COM (2012)0011	EP Position/amendments 2012/0011(COD)	Council Position Doc.15395/14	Comments / compromise suggestions
Proposal for a	Proposal for a	Proposal for a	
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) and Article 114(1) thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) and Article 114(1) thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) ***(…) thereof,***	
Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	
After transmission of the draft legislative act to the national Parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national Parliaments,	
Having regard to the opinion of the European Economic and Social Committee[1],	Having regard to the opinion of the European Economic and Social Committee[1],	Having regard to the opinion of the European Economic and Social Committee[1],	
[1] OJ C , , p. .	[1] OJ C 229, 31.7.2012, p. 90.		

[1] ***OJ C, p. . .***

	After consulting the Committee of the Regions,		
After consulting the European Data Protection Supervisor[2], [2] OJ C , , p.	~~After consulting~~ ***Having regard to the opinion of*** the European Data Protection Supervisor[2] ***[2] OJ C 192, 30.6.2012, p. 7.***	After consulting the European Data Protection Supervisor***[2],***	
Acting in accordance with the ordinary legislative procedure	Acting in accordance with the ordinary legislative procedure***[3]*** ***[3] Position of the European Parliament of 12 March 2014.***	Acting in accordance with the ordinary legislative procedure,	
Whereas:	Whereas:	Whereas:	
(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty lay down that everyone has the right to the protection of personal data concerning him or her.	(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union ('Charter') and Article 16(1) of the Treaty lay down that everyone has the right to the protection of personal data concerning him or her.	(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty lay down that everyone has the right to the protection of personal data concerning him or her.	

[2] OJ C p. .

(2) The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, the strengthening and the convergence of the economies within the internal market, and the well-being of individuals.	(2) The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, the strengthening and the convergence of the economies within the internal market, and the well-being of individuals.	(2) The ~~processing of personal data is designed to serve man; the~~ principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, the strengthening and the convergence of the economies within the internal market, and the well-being of individuals.	
(3) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[3] seeks to harmonise the	(3) Directive 95/46/EC of the European Parliament and of the Council[1] ~~of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[4]~~ seeks to harmonise the	(3) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[5] seeks to harmonise the	

[3] OJ L 281, 23.11.1995, p. 31.
[4] ~~OJ L 281, 23.11.1995, p. 31.~~
[5] OJ L 281, 23.11.1995, p. 31.

protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.	protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States. ***[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).***	protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.	
		(3a) The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought,	

		conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity	
(4) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows. The exchange of data between economic and social, public and private actors across the Union increased. National authorities in the Member States are being called upon by Union law to co-operate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.	(4) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows. The exchange of data between economic and social, public and private actors across the Union increased. National authorities in the Member States are being called upon by Union law to co-operate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.	(4) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows. The exchange of data between ~~economic and social,~~ public and private actors***, including individuals and undertakings*** across the Union ***has*** increased. National authorities in the Member States are being called upon by Union law to co-operate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.	
(5) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly.	(5) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly.	(5) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly.	

Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and requires to further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring an high level of the protection of personal data.	Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and requires to further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring an high level of the protection of personal data.	Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.	
(6) These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance to create the trust that will allow the digital economy to develop across the internal market. Individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced.	(6) These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance to create the trust that will allow the digital economy to develop across the internal market. Individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced.	(6) These developments require ~~building~~ a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance ~~to~~ of ~~create~~ creating the trust that will allow the digital economy to develop across the internal market. Individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced.	

(7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.	(7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.	(7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.	

(8) In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.	(8) In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.	(8) In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. ***Regarding the processing of personal data for compliance with a legal obligation,[6] for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and***	

[6] ***AT, supported by SI, made a proposal for a separate Article 82b which would allow Member States to adopt specific private sector provisions for specific situations (15768/14 DATAPROTECT 176 JAI 908 MI 916 DRS 156 DAPIX 179 FREMP 215 COMIX 623 CODEC 2300). The Presidency thinks that the revised recital 8 read together with Article 1(2a) sufficiently caters for this concern.***

		horizontal law on data protection implementing Directive 95/46/EC Member States have several sector specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules. Within this margin of manoeuvre sector-specific laws that Member States have issued implementing Directive 95/46/EC should be able to be upheld.	
(9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders in the Member States.	(9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders in the Member States.	(9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders in the Member States.	
(10) Article 16(2) of the Treaty mandates the European Parliament and the Council to lay down the rules relating to the protection of	(10) Article 16(2) of the Treaty mandates the European Parliament and the Council to lay down the rules relating to the protection of	(10) Article 16(2) of the Treaty mandates the European Parliament and the Council to lay down the rules relating to the protection of	

individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.	individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.	individuals with regard to the processing of personal data and the rules relating to the free movement of personal data	
(11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations.	(11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union	(11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. ***The proper functioning of the internal market requires that the free movement of personal data within the Union should not be restricted or prohibited for***	

In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.	institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC[1] ~~of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises~~. [1] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	***reasons connected with the protection of individuals with regard to the processing of personal data.*** To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.	
(12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings	(12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings	(12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings	

established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any person. This should also apply where the name of the legal person contains the names of one or more natural persons.	established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any person. This should also apply where the name of the legal person contains the names of one or more natural persons.	established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any person. ~~This should also apply where the name of the legal person contains the names of one or more natural persons.~~	
(13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.	(13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.	(13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.	

	Amendment 1		
(14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, nor does it cover the processing of personal data by the Union institutions, bodies, offices and agencies, which are subject to Regulation (EC) No 45/2001[7], or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.	(14) This Regulation does not This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law~~, nor does it cover the processing of personal data by the Union institutions, bodies, offices and agencies, which are subject to~~**.** Regulation (EC) No 45/2001~~, or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union~~ ***of the European Parliament and of the Council[44][1] should be brought in line with this Regulation and applied in accordance with this Regulation***. [44] [1] ***Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals***	(14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, ***such as activities concerning national security, taking into account Articles 3 to 6 of the Treaty on the Functioning of the European Union*** nor does it cover the processing of personal data by the ~~Union institutions, bodies, offices and agencies, which are subject to Regulation (EC) No 45/2001[8], or the processing of personal data by the~~ Member States when carrying out activities in relation to the common foreign and security policy of the Union.	

[7] ***OJ L 8, 12.1.2001, p. 1.***

[8] ~~OJ L 8, 12.1.2001, p. 1.~~

	with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1***)***.		
		(14a) Regulation (EC) No 45/2001[9] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of this Regulation.	
	Amendment 2		
(15) This Regulation should not apply to processing of personal data by a natural person, which are exclusively personal or domestic, such as correspondence and the holding of addresses, and without any gainful interest and thus without any connection with a professional or commercial activity. The exemption should also not apply to controllers or	(15) This Regulation should not apply to processing of personal data by a natural person, which are exclusively personal***, family-related,*** or domestic, such as correspondence and the holding of addresses ***or a private sale***~~,~~ and ~~without any gainful interest and thus~~ without any connection with a professional or commercial activity. ~~The exemption should also~~	(15) This Regulation should not apply to processing of personal data by a natural person ***in the contects of a***~~, which are exclusively~~ personal or~~ domestic~~***household activity***~~,~~ ~~such as correspondence and the holding of addresses, and without any gainful interest and~~ thus without any connection with a professional or commercial activity. ***Personal and household activities***	

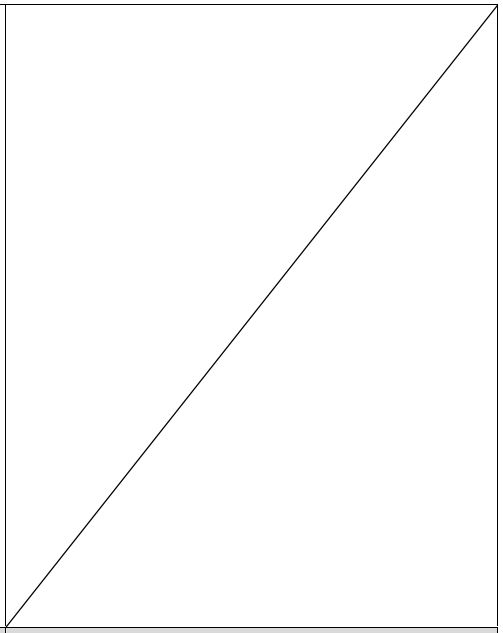
[9] ***OJ L 8, 12.1.2001, p. 1.***

processors which provide the means for processing personal data for such personal or domestic activities.	~~not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.~~ ***However, this Regulation should apply to controllers and processors which provide the means for processing personal data for such personal or domestic activities..***	***include social networking and on-line activity undertaken within the context of such personal and househlod activities. However, this Regulation*** ~~The exemption~~ should ~~also not~~ apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.	
(16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal	(16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the	(16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences ***and, for these purposes, the maintenance of public order,*** or the execution of criminal penalties, and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences	

penalties should be governed by the more specific legal instrument at Union level (Directive XX/YYY).	more specific legal instrument at Union level (Directive ~~XX/YYY~~(Directive 2014/.../EU of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data).	or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive XX/YYY). ***When processing of personal data by (...) private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection and prosecution of criminal offences. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.***	
		(16a) While this Regulation applies also to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation	

		to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including its decision-making. Supervision of such data processing operations may be entrusted to specific bodies within the judicial system of the Member State, which should in particular control compliance with the rules of this Regulation, promote the awareness of the judiciary of their obligations under this Regulation and deal with complaints in relation to such processing.	
(17) This Regulation should be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.	(17) This Regulation should be without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council[1], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.	(17) ***Directive 2000/31/EC does not apply to questions relating to information society services covered by this Regulation. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society***	

	[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 178, 17.7.2000, p. 1).	***services between Member States. Its application should not be affected by this Regulation.***This Regulation should ***therefore*** be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.	
	Amendment 3		
(18) This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation.	(18) This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation. ***Personal data in documents held by a public authority or public body may be disclosed by that authority or body in accordance with Union or Member State law regarding public access to official documents, which reconciles the right to data protection with the right of public access to official documents and constitutes a fair balance of the various interests involved***.	(18) This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation. ***Public access to official documents may be considered as a public interest. Personal data in documents held by a public authority or a public body may be publicly disclosed by this authority or body if the disclosure is provided for by Union law or Member State law to which the public authority or public body is subject. Such laws should reconcile the interest of public access to official documents with the right to the protection of personal data.***	



(19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.	(19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.	(19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.	
	Amendment 4		
(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of the	(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects ~~residing~~ in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services***, irrespective of whether connected to a payment or***	(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects~~, or to the monitoring of the~~	

behaviour of such data subjects.	***not,*** to such data subjects, or to the monitoring ~~of the behaviour~~ of such data subjects. ***In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging the offering of services to data subjects in one or more Member States in the Union.***	~~behaviour of such data subjects~~ ***irrespective of whether connected to a payment or not, which takes place in the Union. In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging doing business with data subjects residing in one or more Member States in the Union. Whereas the mere accessibility of the controller's or an intermediary's website in the Union or of an email address and of other contact details or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, and/or the mentioning of customers or users residing in the Union, may make it apparent that the controller envisages offering goods or***	

		services to such data subjects in the Union.	
	Amendment 5		
(21) In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	(21) In order to determine whether a processing activity can be considered to 'monitor ~~the behaviour~~' ~~of~~ data subjects, it should be ascertained whether individuals are tracked ~~on the internet with~~***, regardless of the origins of the data, or if other data about them are collected, including from public registers and announcements in the Union that are accessible from outside of the Union, including with the intention to use, or potential of subsequent use of*** data processing techniques which consist of applying a 'profile' ~~to an individual~~, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	(21) ***The processing of personal data of data subjects residing in the Union by a controller not established in the Union should also be subject to this Regulation when it is related to the monitoring of their behaviour taking place within the European Union.*** In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of ~~applying a 'profile' to~~ ***profiling*** an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	
(22) Where the national law of a Member State applies by virtue of	(22) Where the national law of a Member State applies by virtue of	(22) Where the national law of a Member State applies by virtue of	

public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.	public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.	public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.	
	Amendment 6		
(23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.	(23) The principles of **data** protection should apply to any information concerning an identified or identifiable **natural** person. To determine whether a person is identifiable, account should be taken of all the means ~~likely~~ reasonably **likely** to be used either by the controller or by any other person to identify **or single out** the individual **directly or indirectly**. **To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.** The principles of	(23) The principles of ***data*** protection should apply to any information concerning an identified or identifiable ***natural*** person. ***Data including pseudonymised data, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person.*** To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual ***directly or indirectly***. ***To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and***	

	data protection should **therefore** not apply to **anonymous** data ~~rendered anonymous in such a way that the data subject is no longer identifiable~~**, which is information that does not relate to an identified or identifiable natural person**. **This Regulation does therefore not concern the processing of such anonymous data, including for statistical and research purposes**.	***the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.*** The principles of data protection should ***therefore*** not apply to ***anonymous information, that is information which does not relate to an identified or identifiable natural person or to*** data rendered anonymous in such a way that the data subject is ***not or*** no longer identifiable. ***This Regulation does therefore not concern the processing of such anonymous information, including for statistical and research purposes.*** ~~***The principles of data protection should not apply to deceased persons, unless information on deceased persons is related to an identified or identifiable natural person.***~~[10]	
		**(*23a) The application of pseudonymisation to personal data can reduce the risks for the data*	

[10] ***The question of the application of the Regulation to deceased persons may need to be revisited in the future.***

		subjects concerned and help controllers and processors meet their data protection obligations. The explicit introduction of 'pseudonymisation' through the articles of this Regulation is thus not intended to preclude any other measures of data protection. ***23b) (…)***	
		(23c) In order to create incentives for applying pseudonymisation when processing personal data, measures of pseudonymisation whilst allowing general analysis should be possible within the same controller when the controller has taken technical and organisational measures necessary to ensure that the provisions of this Regulation are implemented, taking into account the respective data processing and ensuring that additional information for attributing the personal data to a specific data subject is kept separetly. The controller who processes the data shall also refer to authorised persons within the same controller. In such case however the controller shall make	

		sure that the individual(s) performing the pseudonymisation are not referenced in the meta-data[11].	
	Amendment 7		
(24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.	(24) ~~When using online services, individuals may be associated with online~~ ***This Regulation should be applicable to processing involving*** identifiers provided by ~~their~~ devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers ***and Radio Frequency Identification tags, unless those identifiers do not relate to an identified or identifiable natural person***. ~~This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need~~	(24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, ***when*** combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. ~~It follows that i~~Identification numbers, location data, online identifiers or other specific factors as such ~~need~~ ***should*** not ~~necessarily~~ be considered as personal data ~~in all circumstances~~ if they do not identify an individual ***or make an individual identifiable[12].***	

11 ***COM, IE, IT, AT, SE, UK reservation and FR scrutiny reservation on two last sentences.***

12 ***DE reservation. ES, EE and IT also queried as regard the status of so-called identifiers. AT and SI thought the last sentence of the recital should be deleted. UK questioned whether so-called identifiers which were never used to trace back to a data subject should also be considered as personal data and hence subjected to the Regulation. It suggested stating that these can constitute personal data, but this will depend on the context. UK suggests deleting the words 'provided by their devices, applications, tools and protocols, such as Internet***

	~~not necessarily be considered as personal data in all circumstances~~**..**		
	Amendment 8		
(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If	(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action ***that is the result of choice*** by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data~~, including by~~***. Clear affirmative action could include*** ticking a box when visiting an Internet website or ~~by~~ any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence***, mere use of a service*** or inactivity should therefore not constitute consent. Consent should cover all processing	(25) Consent should be given ~~explicitly~~ ***unambiguously*** by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a ***writtent, including[13] electronic, oral*** ~~***or other***~~ statement or***, if required by specific circumstances,*** by ~~a~~***any other*** clear affirmative action by the data subject, ***signifying his or her agreement to*** ~~ensuring that individuals are aware that they give their consent to the processing of~~ personal data ***relating to him or her being processed.***~~,~~ ***This could*** includ~~ingee~~ ~~by~~ ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed	

Protocol addresses or cookie identifiers' and 'received by the servers'. It also suggests deleting 'need not necessarily be considered as personal data in all circumstances ' and replacing it by 'can constitute personal data, but this will depend on the context'. COM referred to the ECJ case law (Scarlett C-70/10) according to which IP addresses should be considered as persona data if they actually could lead to the identification of data subjects. DE queried who would in practice be responsible for such metadata.

[13] ***HU and DE would prefer to distinguish electronic from written statements.***

the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	processing of their personal data. Silence or inactivity should therefore not constitute consent. ***Where it is technically feasible and effective, the data subject's consent to processing may be given by using the appropriate settings of a browser or other application[14]. In such cases it is sufficient that the data subject receives the information needed to give freely specific and informed consent when starting to use the service.*** Consent should cover all processing activities carried out for the same purpose or purposes. ***When the processing has multiple purposes, unambiguous consent should be granted for all of the processing purposes. It is often not possible to fully identify the purpose of data processing for scientific purposes at the time of data collection. Therefore data subjects can give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research[15]. Data subjects should***	

[14] ***PL and AT reservation.***

[15] ***FR and COM scrutiny reservation.***

		have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose and provided that this does not involve disproportionate efforts in view of the protective purpose[16]. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided[17].	
		(25a) Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent	

[16] ***AT, CZ, IE and FR scrutiny reservation; COM reservation.***

[17] ***UK, supported by CZ and IE, proposed adding: 'Where the intention is to store data for an as yet unknown research purpose or as part of a research resource [such as a biobank or cohort], then this should be explained to data subjects, setting out the types of research that may be involved and any wider implications. This interpretation of consent does not affect the need for derogations from the prohibition on processing sensitive categories of data for scientific purposes' .***

		information to be obtained.	
(26) Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of	(26) Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a	(26) Personal data ~~relating to~~ ***concerning*** health should include ~~in particular all~~ data pertaining to the health status of a data subject ***which reveal information relating to the past, current or future physical or mental health of the data subject***[18]; ***including*** information about the registration of the individual for the provision of health services; ~~information about payments or eligibility for healthcare with respect to the individual;~~ a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; ~~any information about the individual collected in the course of the provision of health services to the individual;~~ information derived from the testing or examination of a body part or bodily substance, including ***genetic data and*** biological samples; ~~identification of a person as provider of healthcare to the individual;~~ or any information on ~~e.g.~~ ***for a example*** a	

[18] ***BE proposal.***

its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.	physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.	disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as ~~e.g.~~ ***for example*** from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.	
(27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the	(27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, ~~conditions~~ and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the	(27) The main establishment of a controller in the Union should be ***the place of its central administration in the Union, unless*** ~~determined according to objective criteria and should imply the effective and real exercise of management activities determining~~ the ~~main~~ decisions ~~as to~~ ***on*** the purposes~~, conditions~~ and means of processing ***of personal data are taken in another establishment of the controller in the Union. In this case the latter should be considered as the main establishment.*** ~~through stable arrangements.~~ ***The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real***	

processor should be the place of its central administration in the Union.	processor should be the place of its central administration in the Union.	***exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements.*** This criterion should not depend ***on*** whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no***t*** determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union ***and, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment but the supervisory authority of the processor should***	

		be considered as a concerned supervisory authority and participate to the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered as concerned supervisory authorities when the draft decision concerns only the controller. ***Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered as the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.***	
(28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other	(28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other	(28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other	

undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.	undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.	undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.	
	Amendment 9		
(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. To determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention on the Rights of the Child.	(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. ~~To determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention on the Rights of the Child.~~ ***Where data processing is based on the data subject's consent in relation to the offering of goods or services directly to a child, consent should be given or authorised by the child's parent or legal guardian in cases where the child is below the age of 13. Age-appropriate language should be***	(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data[19]. ~~To determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention on the Rights of the Child.~~ [20] ***This concerns especially the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child[21].***	

[19] ***COM reservation on deletion of the UN Convention on the Rights of the Child reference.***
[20] ***COM reservation on deletion of the reference to the UN Convention on the Rights of the Child.***
[21] ***CZ and AT reservation.***

	used where the intended audience is children. Other grounds of lawful processing such as grounds of public interest should remain applicable, such as for processing in the context of preventive or counselling services offered directly to a child.		
(30) Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to	(30) Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that	(30) Any processing of personal data should be lawful ***and***~~,~~ fair~~.~~ ~~and~~ ***It should be*** transparent ~~in relation to~~ ***for*** the individuals~~ concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means.~~ ***that personal data concerning them are collected,***	

ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.	personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.	***used, consulted or otherwise processed and to which extent the data are processed or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language is used. This concerns in particular the information of the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the individuals concerned and their right to get confirmation and communication of personal data being processed concerning them.*** ***Individuals should be made aware on risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise his or her rights in relation to the processing. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the***	

		collection of the data[22]. The data should be adequate and relevant (…) for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. (…). Personal data should only be processed if the purpose of the processing could not reasonably be fulfilled by other means[23]. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. ~~In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.~~ ***Personal data should be processed in a manner that ensures***	

[22] ***DE suggested inserting the following sentence: 'Data processing for archiving and statistical purposes in the public interest and for scientific or historical purposes is considered compatible and can be conducted on the basis of the original legal basis (e.g. consent), if the data have been initially collected for these purposes'.***

[23] ***UK reservation: this was too burdensome.***

		appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or the use of personal data and the equipment used for the processing.	
	Amendment 10		
(31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.	(31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation. ***In case of a child or a person lacking legal capacity, relevant Union or Member State law should determine the conditions under which consent is given or authorised by that person.***	(31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation***, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract***.	
		(31a) Wherever this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without	

		prejudice to requirements pursuant the constitutional order of the Member State concerned, however such legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it as required by the case law of the Court of Justice of the European Union and the European Court on Human Rights.	
	Amendment 11		
(32) Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.	(32) Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given. ***To comply with the principle of data minimisation, the burden of proof should not be understood as requiring the positive identification of data subjects unless necessary. Similar to civil law terms (e.g. Council***	(32) Where processing is based on the data subject's consent, the controller should ~~have the burden of proving~~ ***be able to demonstrate*** that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and ~~to what~~ ***the*** extent ***to which*** consent is given. ***A declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and its content should***	

	Directive 93/13/EEC[44a1]), data protection policies should be as clear and transparent as possible. They should not contain hidden or disadvantageous clauses. Consent ~~can not~~cannot be given for the processing of personal data of third persons. ***[44a–1] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).***	***not be unusual within the overall context. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended; consent should not be regarded as freely-given if the data subject has no genuine and free choice and is unable to refuse or withdraw consent without detriment.***	
	Amendment 12		
(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment.	(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment. ***This is especially the case if the controller is a public authority that can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given. The use of default options which the data subject is required to***	(33) ~~In order to ensure free~~ ***~~For consent~~,*** ~~it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse~~ ***~~to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended; consent should not be regarded as freely given if the data subject has no genuine and free choice and is unable to refuse~~*** ~~or~~	

	modify to object to the processing, such as pre-ticked boxes, does not express free consent. Consent for the processing of additional personal data that are not necessary for the provision of a service should not be required for using the service. When consent is withdrawn, this may allow the termination or non-execution of a service which is dependent on the data. Where the conclusion of the intended purpose is unclear, the controller should in regular intervals provide the data subject with information about the processing and request a re-affirmation of ~~their~~ his or her consent.	~~withdraw consent without detriment.~~	
	Amendment 13		
(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data	***deleted***	(34) ***In order to safeguard that*** ~~Consent~~ consent ***has been freely-given, consent*** should not provide a valid legal ground for the processing of personal data ***in a specific case***~~,~~ where there is a clear imbalance between the data subject and the controller ***and*** ~~This~~ this ~~is especially the case where the data~~	

are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.		~~subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an~~ imbalance ~~only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and~~ ***makes it unlikely that*** ~~the~~ consent ~~cannot be deemed~~ ***was given*** ~~as~~ freely ~~given, taking into account the interest of the data subject~~***in all circumstance of that specific situation. Consent is presumed not to be freely given, if it does not allow separate consent to be given to different data processing operations despite it is appropriate in the individual case, or if the performance of a contract is made dependent on the consent despite this is not necessary for such performance and the data subject cannot reasonably obtain***	

		equivalent services from another source without consent[24].	
(35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.	(35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.	(35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.	
		(35a) This Regulation provides for general rules on data protection and that in specific cases Member States are also empowered to lay down national rules on data protection. The Regulation does therefore not exclude Member State law that defines the circumstances of specific processing situations, including determining more precisely the conditions under which processing of personal data is lawful. National law may also provide for special processing conditions for specific sectors and for the processing of special categories of data.	

[24] ***COM, DK, IE and FR, SE reservation. CZ thought the wording should be more generic.***

	Amendment 14		
(36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law, or in a Member State law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms. It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association.	(36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law, or in a Member State law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms. ***This should include also collective agreements that could be recognised under national law as having general validity.*** It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association.	(36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a ~~legal~~ basis in Union law, or in ***the national law of*** a Member State ~~law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms~~. It ~~is~~ ***should be*** also for Union or national law to determine ***the purpose of processing.*** ~~whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association~~. ***Furthermore, this basis could specify the general conditions of the Regulation governing the lawfulness of data***	

		processing, determine specifications for determining the controller, the type of data which are subject to the processing, the data subjects concerned, the entities to which the data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. ***It should also be for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or by private law such as a professional association, where grounds of public interest so justify including for health purposes, such as public health and social protection and the management of health care services.***	
(37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life.	(37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life.	(37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life	

		or that of another person. Some types of data processing may serve both important grounds of public interest and the vital interests of the data subject as, for instance when processing is necessary for humanitarian purposes, including for monitoring epidemic and its spread or in situations of humanitarian emergencies, in particular in situations of natural disasters[25].	
	Amendment 15		
(38) The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should	(38) The legitimate interests of ~~a~~ ***the*** controller***, or in case of disclosure, of the third party to whom the data*** ~~***is***~~ ***are*** ***disclosed,*** may provide a legal basis for processing, provided ***that they meet the reasonable expectations of the data subject based on his or her relationship with the controller and*** that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children	(38) The legitimate interests of a controller ***including of a controller to which the data may be disclosed or of a third party*** may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. ~~This would need careful assessment ***including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place.***~~ ***Legitimate interest could exist for***	

[25] CZ, FR, SE and PL thought the entire recital was superfluous.

be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.	deserve specific protection. ***Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, processing limited to pseudonymous data should be presumed to meet the reasonable expectations of the data subject based on his or her relationship with the controller.*** The data subject should have the right to object the processing~~, on grounds relating to their particular situation and~~ free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. ***The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.*** Given that it is for the legislator to provide by law the	***example when there is a relevant and appropriate connection between the data subject and the controller in situations such as the data subject being a client or in the service of the controller[26]. (…) At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place.*** ~~i~~I<u></u>n particular ~~where~~ ***such assessment must take into account whether*** the data subject is a child, given that children deserve specific protection. The data subject should have the right to object ***to*** the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. ~~Given that it is~~	

[26] ***HU scrutiny reservation.***

	legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.	~~for ***Union or national law*** the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the ***exercise*** performance of their tasks***duties***.~~	
		(38a) Controllers that are part of a group of undertakings or institution affiliated to a central bodymay have a legitimate interest to transmit personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country (…) remain unaffected.[27]	
	Amendment 16		
(39) The processing of data to the extent strictly necessary for the purposes of ensuring network and	(39) The processing of data to the extent strictly necessary ***and proportionate*** for the purposes of	(39) The processing of data to the extent strictly necessary for the purposes of ensuring network and	

[27] ***FR reservation.***

information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.	ensuring network and information security, i.e. the ability of a network or an information system to resist~~, at a given level of confidence,~~ accidental events or ~~unlawful or~~ malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by~~, or accessible via,~~ these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. ***This principle also applies to processing***	information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams - – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the ~~concerned~~ data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. ***The processing of personal data strictly necessary for the purposes***	

	of personal data to restrict abusive access to and use of publicly available network or information systems, such as the blacklisting of electronic identifiers.	***of preventing fraud also constitutes a legitimate interest of the data controller concerned. (...) The processing of personal data for direct marketing purposes ~~can~~ may be regarded as carried out for a legitimate interest.***	
	Amendment 17		
	(39a) Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, the prevention or limitation of damages on the side of the data controller should be presumed as carried out for the legitimate interest of the data controller or, in case of disclosure, of the third party to whom the data ~~is~~ are disclosed, and as meeting the reasonable expectations of the data subject based on his or her relationship with the controller. The same principle also applies to the enforcement of legal claims against a data subject, such as debt collection or civil damages and remedies.		

	Amendment 18		
	(39b) Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, the processing of personal data for the purpose of direct marketing for own or similar products and services or for the purpose of postal direct marketing should be presumed as carried out for the legitimate interest of the controller, or in case of disclosure, of the third party to whom the data ~~is~~ are disclosed, and as meeting the reasonable expectations of the data subject based on his or her relationship with the controller if highly visible information on the right to object and on the source of the personal data is given. The processing of business contact details should be generally regarded as carried out for the legitimate interest of the controller, or in case of disclosure, of the third party to whom the data ~~is~~ are disclosed, and as meeting the reasonable expectations of the data subject based on his or her		

	relationship with the controller. The same should apply to the processing of personal data made manifestly public by the data subject.		
	Amendment 19		
(40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes. Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the	***deleted***	(40) The processing of personal data for other purposes ***than the purposes for which the dat have been initially collected*** should be only allowed where the processing is compatible with those purposes for which the data have been initially collected~~, .~~ ~~in~~ In ***such case no separate legal basis is required other than the one which allowed the collection of the data. (…) If*** ~~particular where~~ the processing is necessary for ***the performacne of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union law or Member State law may determine and specify the tasks and purposes for which the further processing shall be regarded as lawful. The further processing (…) for archiving purposes in the public interest, or***	

information of the data subject on those other purposes should be ensured.		***for*** ~~***historical***~~, statistical, ~~***or***~~ scientific ~~***research***~~ or historical purposes ***or in view of future dispute resolution[28] should be considered as compatible lawful processing operations. The legal basis provided by Union or Member State law for the collection and processing of personal data may also provide a legal basis for further processing for other purposes if these purposes are in line with the assigned task and the controller is entitled legally to collect the data for these other purposes[29].*** ***In order to ascertain whether a purpose of further processing is compatible with the purpose for which the data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account any link between those purposes and the purposes of the intended further processing, the context in which the data have***	

[28] ***ES pointed out the text of Article 6 had not been modified regarding dispute resolution.***

[29] ***FR, IT and UK scrutiny reservation.***

		been collected, including the reasonable expectations of the data subject as to their further use, the nature of the personal data, the consequences of the intended further processing for data subjects, and the existence of appropriate safeguards in both the original and intended processing operations. Where the ***intended*** other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes ***and on his or her rights including the right to object,*** should be ensured. ***Indicating possible criminal acts or threats to public security by the controller and transmitting these data to a***	

		competent authority should be regarded as being in the legitimate interest pursued by the controller[30]. However such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy[31].	
	Amendment 20		
(41) Personal data which are, by their nature, particularly sensitive and vulnerable in relation to fundamental rights or privacy, deserve specific protection. Such data should not be processed, unless the data subject gives his explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain	***deleted***	(41) Personal data which are, by their nature, particularly sensitive ~~and vulnerable~~ in relation to fundamental rights ***and freedoms*** ~~or privacy~~, deserve specific protection ***as the context of their processing may create important risks for the fundamental rights and freedoms. These data should also include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the European***	

[30] ***AT, PL and COM reservation.***

[31] ***IE, SE and UK queried the last sentence of recital 40, which was not reflected in the body of the text. DE, supported by CZ, IE, GR and PL, wanted it to be made clear that Article 6 did not hamper direct marketing or credit information services or businesses in general according to GR.***

associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.		***Union of theories which attempt to determine the existence of separate human races.*** Such data should not be processed, unless ***processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation[32] for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly be provided inter alia where*** the data subject gives his ***or her*** explicit consent ~~. However, derogations from this prohibition should be~~	

[32] ***AT scrutiny reservation.***

		~~explicitly provided for~~ ***or*** in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms. ***Special categories of personal data may also be processed where the data have manifestly been made public or voluntarily and at the request of the data subject transferred to the controller for a specific purpose specified by the data subject, where the processing is done in the interest of the data subject.*** ***Member State and Union Law may provide that the general prohibition for processing such special categories of personal data in certain cases may not be lifted by the data subject's explicit consent.***	
	Amendment 21		
(42) Derogating from the prohibition on processing sensitive categories of data should also be	(42) Derogating from the prohibition on processing sensitive categories of data should also be	(42) Derogating from the prohibition on processing sensitive categories of data should also be	

allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific research purposes.	allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, for historical, statistical and scientific research purposes***, or for archive services***.	allowed ~~if done by a~~ ***when provided for in Union or Member State*** law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify***, in particular processing data in the field of employment law, social security and social protection law, including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health or ensuring high standards of quality and safety of health care and services and of medicinal products or medical devices or assessing public policies adopted in the field of health, also by producing quality and activity indicators.*** ~~and in particular~~ ***This may be done*** for health purposes, including public health ~~and social protection~~ and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the	

		health insurance system, or for ***archiving in the public interest or*** historical, statistical and scientific ~~research~~ purposes. ***A derogation should also allow processing of such data where necessary for the establishment, exercise or defence of legal claims, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure.***	
		(42a) Special categories of personal data which deserve higher protection, may only be processed for health-related purposes where necessary to achieve those purposes for the benefit of individuals and society as a whole, in particular in the context of the management of health or social care services and systems including the processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care	

		and cross-border healthcare or health security, monitoring and alert purposes or for archiving, historical, statistical or scientific purposes as well as for studies conducted in the public interest in the area of public health. Therefore this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy (…). Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of individuals. (…)[33].	
		(42b) The processing of special categories personal data (…) may be necessary for reasons of public interest in the areas of public health, without consent of the data	

[33] ***Moved from recital 122.***

		subject. This processing is subject to for suitable and specific measures so as to protect the rights and freedoms of individuals. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies[34].	

[34] ***Moved from recital 123.***

(43) Moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognised religious associations is carried out on grounds of public interest.	(43) Moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognised religious associations is carried out on grounds of public interest.	(43) Moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognised religious associations is carried out on grounds of public interest.	
(44) Where in the course of electoral activities, the operation of the democratic system requires in a Member State that political parties compile data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.	(44) Where in the course of electoral activities, the operation of the democratic system requires in a Member State that political parties compile data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.	(44) Where in the course of electoral activities, the operation of the democratic system requires in a Member State that political parties compile data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.	
	Amendment 22		
(45) If the data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. In case of a request for access, the controller should be	(45) If the data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. In case of a request for access, the controller should be	(45) If the data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation~~. In case of a request for access, the controller should be~~	

entitled to ask the data subject for further information to enable the data controller to locate the personal data which that person seeks.	entitled to ask the data subject for further information to enable the data controller to locate the personal data which that person seeks. ***If it is possible for the data subject to provide such data, controllers should not be able to invoke a lack of information to refuse an access request.***	~~entitled to ask the data subject for further information to enable the data controller to locate the personal data which that person seeks~~***However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights.***	
(46) The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in	(46) The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to ~~them~~ him or her are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in	(46) The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. ***This information could be provided in electronic form, for example, when addressed to the public, through a website.*** This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children	

such a clear and plain language that the child can easily understand.	such a clear and plain language that the child can easily understand.	deserve specific protection, any information and communication, where processing is addressed ~~specifically -~~to a child, should be in such a clear and plain language that the child can easily understand.	
	Amendment 23		
(47) Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to request, free of charge, in particular access to data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons, in case he does not comply with the data subject's request.	(47) Modalities should be provided for facilitating the data subject's exercise of ~~their~~ his or her rights provided by this Regulation, including mechanisms to ~~request~~ ***obtain***, free of charge, in particular access to data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a ~~fixed~~ ***reasonable*** deadline and give reasons, in case he does not comply with the data subject's request.	(47) Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to request, ~~free of charge,-~~ in particular access to data, rectification, erasure and to exercise the right to object. ***Thus the controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means.*** The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons ***where the controller*** ~~, in case he~~ does not ***intend to*** comply with the data subject's request.	

	Amendment 24		
(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.	(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be ***likely*** stored ***for each purpose***, ***if the data are to be transferred to third parties or third countries,*** on the existence ***of measures to object and*** of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data. ***This information should be provided, which can also mean made readily available, to the data subject after the provision of simplified information in the form of standardised icons. This should also mean that personal data are processed in a way that effectively allows the data subject to exercise his or her rights.***	(48) The principles of fair and transparent processing require that the data subject should be informed ~~in particular~~ of the existence of the processing operation and its purposes~~, how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint.~~ ***The controller should provide the data subject with any further information necessary to guarantee fair and transparent processing. Furthermore the data subject should be informed about the existence of profiling, and the consequences of such profiling.*** Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.	

(49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.	(49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.	(49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient. ***Where the origin of the data could not be provided to the data subject because various sources have been used, the information should be provided in a general manner.***	
	Amendment 25		
(50) However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. The latter	(50) However, it is not necessary to impose this obligation where the data subject already ~~disposes of~~ ***knows*** this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. ~~The latter~~	(50) However, it is not necessary to impose this obligation where the data subject already ~~disposes~~ ***possesses*** ~~of~~ this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. The latter	

could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.	~~could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.~~	could be particularly the case where processing is for historical, statistical or scientific ~~research~~ purposes; in this regard, the number of data subjects, the age of the data, and any ~~compensatory measures~~ ***appropriate safeguards*** adopted may be taken into consideration.	
	Amendment 26		
(51) Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and	(51) Any person should have the right of access to data which have been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what ***estimated*** period, which recipients receive the data, what is the ***general*** logic of the data that are undergoing the processing and what might be~~, at least when based on profiling,~~ the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or	(51) ~~Any~~ ***A natural*** person should have the right of access to data which has been collected concerning ~~them~~him or her, and to exercise this right easily ***and at reasonable intervals***, in order to be aware ***of*** and verify the lawfulness of the processing. ***This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.*** Every data subject should therefore have the right to know and obtain communication in particular for what purposes the	

in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.	intellectual property ~~and in particular~~***, such as in relation to*** the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.	data are processed, ***where possible*** for what period, which recipients receive the data, what is the logic ***involved in any automatic*** ~~of the~~ data ~~that are undergoing the~~ processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject. ***Where the controller processes a large quantity of information concerning the data subject, the controller may request that before the information is delivered the data subject specify to which information or to which processing activities the request relates.***	
(52) The controller should use all reasonable measures to verify the identity of a data subject that requests access, in particular in the context of online services and	(52) The controller should use all reasonable measures to verify the identity of a data subject that requests access, in particular in the context of online services and	(52) The controller should use all reasonable measures to verify the identity of a data subject ~~that~~***who*** requests access, in particular in the context of online services and	

online identifiers. A controller should not retain personal data for the unique purpose of being able to react to potential requests.	online identifiers. A controller should not retain personal data for the unique purpose of being able to react to potential requests.	online identifiers. A controller should not retain personal data for the ~~unique~~ ***sole*** purpose of being able to react to potential requests.	
	Amendment 27		
(53) Any person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a	(53) Any person should have the right to have personal data concerning them rectified and a 'right to ~~be forgotten~~ ***erasure***' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. ~~This right is particularly relevant, when the data subject has given their consent as a~~	(53) ~~Any~~ ***A natural*** person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is ~~particularly~~ in particular relevant, when the data subject has given	

child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.	~~child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet.~~ However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them. ***Also, the right to erasure should not apply when the retention of personal data is necessary for the performance of a contract with the data subject, or when there is a legal obligation to retain this data.***	their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary ***for archiving purposes in the public interest,*** for historical, statistical and scientific ~~research~~ purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.	
	Amendment 28		
(54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be	(54) To strengthen the 'right to ~~be forgotten~~ ***erasure***' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public ***without***	(54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be	

obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.	***legal justification*** should be obliged to ~~inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party~~ ***take all necessary steps to have the data erased, including by third parties, without prejudice to the right of the data subject to claim compensation.***	obliged to inform ~~third parties~~ ***the controllers*** which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take ~~all~~ reasonable steps, ***taking into account available technology and the means available to the controller,*** including technical measures, in relation to data for the publication of which the controller is responsible. ~~In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.~~	
	Amendment 29		
	(54a) Data which are contested by the data subject and whose accuracy or inaccuracy cannot be determined should be blocked until the issue is cleared.	***54a) Methods to restrict processing of personal data could include, inter alia, temporarily moving the selected data to another processing system or making the selected data***	

		unavailable to users or temporarily removing published data from a website. In automated filing systems the restriction of processing of personal data should in principle be ensured by technical means; the fact that the processing of personal data is restricted should be indicated in the system in such a way that it is clear that the processing of the personal data is restricted.	
	Amendment 30		
(55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. This should apply where the data subject	(55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. ***Data controllers should be encouraged***	(55) To further strengthen the control over their own data ~~and their right of access, data subjects should have the right,~~ where ***the processing of*** personal data ~~are processed~~ ***is carried out*** by ~~electronic~~ ***automated*** means ~~and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The~~ the data subject should also be allowed to transmit ~~those~~ ***the personal*** data ***concerning him or her***, which ~~they have~~ ***he or she has*** provided ~~, from one automated application, such as~~	

provided the data to the automated processing system, based on their consent or in the performance of a contract.	***to develop interoperable formats that enable data portability.*** This should apply where the data subject provided the data to the automated processing system, based on ~~their~~ his or her consent or in the performance of a contract. ***Providers of information society services should not make the transfer of those data mandatory for the provision of their services.***	~~a social network, into~~ ***to a controller, in a commonly used and machine-readable format to*** another ~~one~~***controller***. This ***right*** should apply where the data subject provided the ***personal*** data ~~to the automated processing system,~~ based on ~~their~~ ***his or her*** consent or in the performance of a contract***. It should not apply where processing is based on another legal ground other than consent or contract. By its very nature this right should not be exercised against controllers processing data in the exercise of their public duties. It should therefore in particular not apply where processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of a official duty vested in the controller.*** ***Where, in a certain set of personal data, more than one data subject is concerned, the right to transmit the data should be without prejudice to the requirements on the lawfulness of the processing of***	

		personal data related to another data subject in accordance with this Regulation. This right should also not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should in particular not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract, to the extent and as long as the data are necessary for the performance of that contract.	
	Amendment 31		
(56) In cases where personal data might lawfully be processed to protect the vital interests of the data subject, or on grounds of public interest, official authority or the legitimate interests of a controller, any data subject should nevertheless be entitled to object to the processing of any data relating to them. The burden of proof should be on the controller to demonstrate that their legitimate interests may override the interests	(56) In cases where personal data might lawfully be processed to protect the vital interests of the data subject, or on grounds of public interest, official authority or the legitimate interests of a controller, any data subject should nevertheless be entitled to object to the processing of any data relating to ~~them~~him or her***, free of charge and in a manner that can be easily and effectively invoked***. The burden of proof should be on the	(56) In cases where personal data might lawfully be processed ~~to protect the vital interests of the data subject, or~~ on grounds of ~~public interest, official authority or~~ the legitimate interests of a controller, any data subject should nevertheless be entitled to object to the processing of any data relating to them. ~~The burden of proof~~ ***It*** should be ~~on~~ ***for*** the controller to demonstrate that their legitimate interests may override the interests	

or the fundamental rights and freedoms of the data subject.	controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.	or the fundamental rights and freedoms of the data subject.	
	Amendment 32		
(57) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing free of charge and in a manner that can be easily and effectively invoked.	(57) Where ~~personal data are processed for the purposes of direct marketing,~~ the data subject ~~should have~~ ***has*** the right to object to ~~such~~ ***the*** processing ~~free of charge and in a manner that can be easily and effectively invoked~~***, the controller should explicitly offer it to the data subject in an intelligible manner and form, using clear and plain language and should clearly distinguish it from other information.***	(57) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing free of charge and in a manner that can be easily and effectively invoked.	
	Amendment 33		
(58) Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance	(58) ***Without prejudice to the lawfulness of the data processing, every*** natural person should have the right ~~not to be subject~~ ***to object*** to ~~a measure which is based on~~ profiling ~~by means of automated processing. However, such measure~~***. Profiling which leads to***	(58) ~~Every natural person~~ ***The data subject*** should have the right not to be subject to a ~~measure~~ ***a decision evaluation personal aspects relating to him or her and taken*** which is based ***soleley*** on ~~profiling by means of~~ automated processing***, which produces legal effects***	

of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.	***measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject*** should ***only*** be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. ~~The~~ In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human ~~intervention~~ ***assessment*** and that such measure should not concern a child. ***Such measures should not lead to discrimination against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity.***	***concerning him or her or significantly affects his or her, like automatic refusal of an on-line credit application or e-recruiting practices without any human intervention. Such processing includes also 'profiling' intended to create or use a profile, that is a set of data characterising a category of individuals to evaluate personal aspects relating to a natural person, in particular to analyse or predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements.*** However, ~~such measure~~ ***decision making based on such processing, including profiling,*** should be allowed when ~~expressly~~ authorised[35] by ***Union or Member State*** law~~, carried out in the course of~~ ***to which the controller is subject, including for fraud and tax evasion[36] monitoring and prevention purposes and to ensure the security and reliability of a service***	

[35] ***BE suggested adding ' or recommended', with regard to e.g. ECB recommendations.***

[36] ***Further to MT suggestion.***

		provided by the controller, or necessary for the entering or performance of a contract ***between the data subject and a controller***, or when the data subject has given his ***or her explicit*** consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention ~~and that such measure should not concern a child~~, ***to express his or her point of view, to get an explanation of the decision reached after such assessment[37] and the right to contest the decision.*** ***Automated decision making and profiling based on special categories of personal data should only be allowed under specific conditions.***	
	Amendment 34		
	(58a) Profiling based solely on the processing of pseudonymous data should be presumed not to significantly affect the interests,		

[37] Further to PL suggestion.

	rights or freedoms of the data subject. Where profiling, whether based on a single source of pseudonymous data or on the aggregation of pseudonymous data from different sources, permits the controller to attribute pseudonymous data to a specific data subject, the processed data should no longer be considered to be pseudonymous.		
		(58a) The creation and the use of a profile, i.e. a set of data characterising a category of individuals that is e applied or intended to be applied to a natural person as such is subject to the (general) rules of this Regulation governing processing of personal data (legal grounds of processing, data protection principles etc.) with specific safeguards (for instance the obligation to conduct an impact assessment in some cases or provisions concerning specific information to be provided to the concerned individual). The European Data Protection Board should have the possibility to issue guidance in this context.	

	Amendment 35		
(59) Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set	(59) Restrictions on specific principles and on the rights of information, ~~access,~~ rectification and erasure or on the right ***of access and*** to ***obtain*** data ~~portability~~, the right to object, ~~measures based on~~ profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other ***specific and well-defined*** public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those	(59) Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, ***the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific***	

out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.	restrictions should be in compliance with requirements set out by the Charter ~~of Fundamental Rights of the European Union and~~ by the European Convention for the Protection of Human Rights and Fundamental Freedoms.	***information related to the political behaviour under former totalitarian state regimes*** or the protection of the data subject or the rights and freedoms of others***, including social protection and public health***. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.	
	Amendment 36		
(60) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure and be obliged to demonstrate the compliance of each processing operation with this Regulation.	(60) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established***, in particular with regard to documentation, data security, impact assessments, the data protection officer and oversight by data protection authorities***. In particular, the controller should ensure and be ~~obliged~~ ***able*** to demonstrate the compliance of each processing	(60) ~~Comprehensive~~ ***The*** responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ~~ensure and~~ be obliged ***to implement appropriate measures and be able*** to demonstrate the compliance of each processing ~~operation~~ ***activities*** with this Regulation. ***These measures should take into account the nature, scope, context and***	

	operation with this Regulation. ***This should be verified by independent internal or external auditors.***	***purposes of the processing and the risk for the rights and freedoms of individuals.***	
		(60a) Such risks, of varying likelihood and severity, may result from data processing which could lead to physical, material or moral damage, in particular where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, [breach of (…) pseudonymity][38], or any other significant economic or social disadvantage; or where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and	

[38] ***The reference to the use of pseudonymous data in Chapter IV will in the future need to be debated in the context of a further debate on pseudonymising personal data.***

		offences or related security measures; where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable individuals, in particular of children, are processed; where processing involves a large amount of personal data and affects a large number of data subjects.	
		(60b) The likelihood and severity of the risk should be determined in function of the nature, scope, context and purposes of the data processing. Risk should be evaluated on an objective assessment, by which it is established whether data processing operations involve a	

		high risk. A high risk is a particular[39] risk of prejudice to the rights and freedoms of individuals.	
		(60c) Guidance for the implementation of appropriate measures, and for demonstrating the compliance by the controller [or processor], especially as regards the identification of the risk related to the processing, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer. The European Data Protection Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk for the rights and freedoms of individuals and indicate what measures may be sufficient in	

[39] ***The use the word 'particular' was questioned by BE, CZ, ES and UK, which thought that this term does not express the seriousness of the risk in case of 'high' risk.***

		such cases to address such risk.	
	Amendment 37		
(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.	(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. ***The principle of data protection by design requires data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. This should also include the responsibility for the products and services used by the controller***	(61) The protection of the rights and freedoms of ~~data subjects~~ ***individuals*** with regard to the processing of personal data require that appropriate technical and organisational measures are taken, ~~both at the time of the design of the processing and at the time of the processing itself,~~ to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. ***Such measures could consist inter alia of minimising the processing of personal data, (…) pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing,***	

	or processor. The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimisation and purpose limitation.	***enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are either based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.***	
	Amendment 38		
(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a	(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a	(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a	

controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.	controller determines the purposes~~,~~ ~~conditions~~ and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller. ***The arrangement between the joint controllers should reflect the joint controllers' effective roles and relationships. The processing of personal data under this Regulation should include the permission for a controller to transmit the data to a joint controller or to a processor for the processing of the data on ~~their~~ his or her behalf.***	controller determines the purposes, ~~conditions~~ and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.	
	Amendment 39		
(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of	(63) Where a controller not established in the Union is processing personal data of data subjects ~~residing~~ in the Union ~~whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour~~, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of	(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring ***of*** their behaviour ***in the Union***, the controller should designate a representative, unless ***the processing it carries outis occasional and unlikely to result***	

protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.	protection, or the ~~controller is a small or medium sized enterprise or~~ ***processing relates to fewer than 5000 data subjects during any consecutive 12-month period and is not carried out on special categories of personal data, or is*** a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.	***in a risk for the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing or*** the controller is ~~established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or~~ a public authority or body~~ or where the controller is only occasionally offering goods or services to such data subjects~~. The representative should act on behalf of the controller and may be addressed by any supervisory authority.~~ ***The representative should be explicitly designated by a written mandate of the controller to act on its behalf with regard to the latter's obligations under this Regulation. The designation of such representative does not affect the responsibility and liability of the controller under this Regulation. Such representative should perform its tasks according to the received mandate from the controller, including to cooperate with the competent supervisory authorities on any action taken in***	

		ensuring compliance with this Regulation. The designated representative should be subjected to enforcement actions in case of non-compliance by the controller.	
		(63a) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. Adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying out of processing by a processor should be governed by a contract or other	

		legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk for the rights and freedoms of the data subject. ***The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission, or which are part of a certification granted in the certification mechanism. After the completion of the processing on behalf of the controller, the processor should return or delete the personal data, unless there is a requirement to store the data under Union or Member State law***	

		to which the processor is subject.	
	Amendment 39		
(64) In order to determine whether a controller is only occasionally offering goods and services to data subjects residing in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is ancillary to those main activities.	(64) In order to determine whether a controller is only occasionally offering goods and services to data subjects ~~residing~~ in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is ancillary to those main activities.	***deleted***	
	Amendment 41		
(65) In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.	(65) In order to ***be able to*** demonstrate compliance with this Regulation, the controller or processor should ~~document each processing operation~~ ***maintain the documentation necessary in order to fulfill the requirements laid down in this Regulation***. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for ~~monitoring those processing operations~~ ***evaluating the***	(65) In order to demonstrate compliance with this Regulation, the controller or processor should ~~document each~~ ***maintain records regarding all categories of*** processing ~~operation~~***activities under its responsibility***. Each controller and processor should be obliged to co-operate with the supervisory authority and make ~~this documentation~~***these records***, on request, available to it, so that it might serve for monitoring those processing operations.	

	compliance with this Regulation. However, equal emphasis and significance should be placed on good practice and compliance and not just the completion of documentation.		
	Amendment 42		
(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.	(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, ~~the Commission should promote~~ technological neutrality, interoperability and innovation ***should be promoted*** and, where appropriate, ~~cooperate~~ ***cooperation*** with third countries ***should be***	(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security ***including confidentiality***, taking into account ***available technology*** ~~the state of the art~~ and the costs of ~~their~~ implementation in relation to the risk~~s~~ and the nature of the personal data to be protected. ~~When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third ***countries***~~***In assessing***	

	encouraged.	***data security risk, consideration should be given to the risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or moral damage.***	
		(66a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to result in a high risk for the rights and freedoms of individuals, the controller [or the processor] should be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of this risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with this Regulation.	

		Where a data protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.	
	Amendment 43		
(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 24 hours. Where this cannot achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the	(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, ~~as soon as the controller becomes aware that such a breach has occurred,~~ the controller should notify the breach to the supervisory authority without undue delay ~~and, where feasible, within 24~~***,which should be presumed to be not later than 72*** hours. ~~Where this cannot achieved within 24 hours~~ ***If applicable***, an explanation of the reasons for the delay should accompany the notification. The	(67) A personal data breach may, if not addressed in an adequate and timely manner, result in ***physical, material or moral damage to individuals such as*** ~~substantial economic~~ loss ***of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, [brreach of pseudonymity], damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or*** ~~and~~ social ~~harm, including identity fraud,~~ ***disadvantage*** to the individual concerned. Therefore, as soon as the controller becomes aware that	

breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches	individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach and formulate ~~as well as~~ recommendations ~~as well as recommendations~~ for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement	~~such~~ a ***personal data*** breach ***which may result in physical, material or moral damage*** has occurred, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within ~~24~~ 72 hours. Where this cannot ***be*** achieved within ~~24~~ 72 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose ***rights and freedoms*** ~~personal data~~ could be ~~adversely~~ ***severely*** affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. ~~A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation.~~ The notification should describe the nature of the personal data breach as well as recommendations ~~as well as recommendations~~ for the individual concerned to mitigate potential adverse effects. Notifications to data subjects	

may justify a longer delay.	appropriate measures against continuing or similar data breaches may justify a longer delay.	should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the ~~chance for data subjects~~ ***need*** to mitigate an immediate risk of ~~harm~~ ***damage*** would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.	
(68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests	(68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in	(68) ~~In order to determine~~ ***It must*** ~~whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should~~ be ascertained whether ~~the controller has implemented and applied~~ ***all*** appropriate technological protection and organisational measures ***have been implemented*** to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject.~~, before a damage to~~	

occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.	particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.	~~personal and economic interests occurs,~~ ***The fact that the notification was made without undue delay should be established*** taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. ***Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.***	
		(68a) The communication of a personal data breach to the data subject should not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data affected by the personal data breach. Such technological protection measures should include those that render the data unintelligible to any person who is not authorised to access it, in particular by encrypting the personal data.	

(69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.	(69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.	(69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.	
(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate	(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation	(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation***s***	

general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.	should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.	should be abolished, and replaced by effective procedures and mechanism which focus instead on those ***types of*** processing operations which are likely to ~~present specific~~***result in a high*** risk~~s~~ to the rights and freedoms of ~~data subjects~~***individuals*** by virtue of their nature, ~~their~~ scope***, context and*** ~~or their~~ purposes. ~~In such~~ Such ~~cases, a data protection impact assessment should be carried out by the controller or processor prior to the~~ ***types of*** processing***, operations may be those*** which ~~should include~~ in particular***, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or wehere they become necessary in the light of the time that has elapsed since the initial processing***[40] ~~the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation~~.	

[40] ***BE was opposed to the temporal reference in the last part of this sentence.***

		(70a) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk, which should include in particular the envisaged measures, safeguards and mechanisms for mitigating that risk and for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.	
(71) This should in particular apply to newly established large scale filing systems, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.	(71) This should in particular apply to newly established large scale filing systems, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.	(71) This should in particular apply to ~~newly established~~ large scale ~~filing systems~~***processing operations***, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects ***and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of***	

		technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk for the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made in cases where data are processed for taking decisions regarding specific individuals following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is	

		likely to result in a high risk for the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data irrespective of the volume or the nature of the data, should not be considered as being on a large scale, if the processing of these data is protected by professional secrecy, such as the processing of personal data from patients or clients by an individual doctor, health care professional, hospital or attorney. In these cases a data protection impact assessment should not be mandatory.	
	Amendment 44		
	(71a) Impact assessments are the essential core of any sustainable data protection framework, making sure that businesses are aware from the outset of all possible consequences of their data processing operations. If		

	impact assessments are thorough, the likelihood of any data breach or privacy-intrusive operation can be fundamentally limited. Data protection impact assessments should consequently have regard to the entire lifecycle management of personal data from collection to processing to deletion, describing in detail the envisaged processing operations, the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure compliance with ~~the~~ this Rregulation.		
	Amendment 45		
	(71b) Controllers should focus on the protection of personal data throughout the entire data lifecycle from collection to processing to deletion by investing from the outset in a sustainable data management framework and by following it up with a comprehensive compliance mechanism.		

(72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.	(72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.	(72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.	
	Amendment 46		
(73) Data protection impact assessments should be carried out by a public authority or public body if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question.	***deleted***	(73) Data protection impact assessments ~~should~~ ***may*** be carried out by a public authority or public body if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question.	

	Amendment 47		
(74) Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.	(74) Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, ***the data protection officer or*** the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. ~~Such~~ ***A*** consultation ***of the supervisory authority*** should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.	(74) Where a data protection impact assessment indicates that ***the*** processing ***would, despite the envisaged safeguards, security measures and mechanisms to mitigate the*** ~~operations involve a high degree of specific~~ risk~~s to the~~ ***result in a high riks to the*** rights and freedoms of ~~data subjects~~***individuals and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation***, ~~such as excluding individuals from their right, or by the use of specific new technologies,~~ the supervisory authority should be consulted, prior to the start of ~~operations~~***processing activities***~~, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative~~	

		~~measure which defines the nature of the processing and lays down appropriate safeguards~~. ***Such high risk is likely to result from certain types of data processing and certain extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the data subject. The supervisory authority should respond to the request for consultation in a defined period. However, the absence of a reaction of the supervisory authority within this period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of this consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue pursuant to Article 33 may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk for the rights and freedoms of***	

		individuals.	
	Amendment 48		
	(74a) Impact assessments can only be of help if controllers make sure that they comply with the promises originally laid down in them. Data controllers should therefore conduct periodic data protection compliance reviews demonstrating that the data processing mechanisms in place comply with assurances made in the data protection impact assessment. It should further demonstrate the ability of the data controller to comply with the autonomous choices of data subjects. In addition, in case the review finds compliance inconsistencies, it should highlight these and present recommendations on how to achieve full compliance.		
		(74a) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the	

		supervisory authority.	
		(74b) A consultation with the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.	
	Amendment 49		
(75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks	(75) Where the processing is carried out in the public sector or where, in the private sector, processing ~~is carried out by a large enterprise~~ ***relates to more than 5000 data subjects within 12 months***, or where its core activities, regardless of the size of the enterprise, involve processing operations ***on sensitive data, or processing operations*** which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. ***When establishing***	(75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person ~~should~~ ***with expert knowledge of data protection law and practices may*** assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an	

independently.	***whether data about a large number of data subjects are processed, archived data that are restricted in such a way that they are not subject to the normal data access and processing operations of the controller and can no longer be changed should not be taken into account.*** Such data protection officers, whether or not an employee of the controller ***and whether or not performing that task full time***, should be in a position to perform their duties and tasks independently ***and enjoy special protection against dismissal. Final responsibility should stay with the management of an organisation. The data protection officer should in particular be consulted prior to the design, procurement, development and setting-up of systems for the automated processing of personal data, in order to ensure the principles of privacy by design and privacy by default.***	employee of the controller, should be in a position to perform their duties and tasks ***in an*** independent~~ly~~ ***manner***.	

	Amendment 50		
	(75a) The data protection officer should have at least the following qualifications: extensive knowledge of the substance and application of data protection law, including technical and organisational measures and procedures; mastery of technical requirements for privacy by design, privacy by default and data security; industry-specific knowledge in accordance with the size of the controller or processor and the sensitivity of the data to be processed; the ability to carry out inspections, consultation, documentation, and log file analysis; and the ability to work with employee representation. The controller should enable the data protection officer to take part in advanced training measures to maintain the specialized knowledge required to perform his or her duties. The designation as a data protection officer does not necessarily require fulltime occupation of the respective employee.		

	Amendment 51		
(76) Associations or other bodies representing categories of controllers should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors.	(76) Associations or other bodies representing categories of controllers should be encouraged***, after consultation of the representatives of the employees,*** to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors. ***Such codes should make compliance with this Regulation easier for industry.***	(76) Associations or other bodies representing categories of controllers ***or processors*** should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors ***and the specific needs of micro, small and medium enterprises. In particular such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of individuals***.	
		(76a) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult with relevant stakeholders, including data subjects where feasible, and have regard to	

		submissions received and views expressed in response to such consultations.	
	Amendment 52		
(77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.	(77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and ***standardised*** marks should be encouraged, allowing data subjects to quickly**,** ***reliably and verifiably*** assess the level of data protection of relevant products and services. ***A "European Data Protection Seal" should be established on the European level to create trust among data subjects, legal certainty for controllers, and at the same time export European data protection standards by allowing non-European companies to more easily enter European markets by being certified***.	(77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.	
(78) Cross-border flows of personal data are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised	(78) Cross-border flows of personal data are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised	(78) Cross-border flows of personal data ***to and from countries outside the Union and international organisations*** are necessary for the expansion of international trade and	

new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined. In any event, transfers to third countries may only be carried out in full compliance with this Regulation.	new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined. In any event, transfers to third countries may only be carried out in full compliance with this Regulation.	international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to ***controllers, processors or other recipients in*** third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined***, to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international co-operation***. ***The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined, including in cases of***	

		onward transfers of personal data from the third country or international organisation to controllers, processors in the same or[41] another third country or international organisation. In any event, transfers to third countries ***and international organisations*** may only be carried out in full compliance with this Regulation. ***A transfer may only take place if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller or processor.***	
	Amendment 53		
(79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects.	(79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects ***ensuring an adequate level of protection for the fundamental rights of citizens***	(79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. ***Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far***	

[41] ***DE scrutiny reservation, in particular about the application of the rules of place of purchase in relation to Article 89a.***

		as such agreements do not affect this Regulation or any other provisions of EU law and include safeguards to protect the rights of the data subjects[42].	
	Amendment 54		
(80) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.	(80) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. ~~In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.~~ ***The Commission may also decide, having given notice and a complete justification to the third country, to revoke such***	(80) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a ~~processing~~ ***specified*** sector***, such as the private sector or one or more specific economic sectors*** within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.	

[42] ***FR requests the second sentence to be inserted in Article 89a. NL asked what was meant with the new text and considered that it was necessary to keep it, but its purpose and meaning should be clarified. DE and UK scrutiny reservation on the new text. EE asked whether if "affect" means that it was not contradictory or something else.***

	a decision.		
(81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards.	(81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards.	(81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of ~~the~~ a third country ***or of a territory or of a specified sector within a third country***, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards ***and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision to a territory or a specified sector in a third country should take into account clear and objective criteria , such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country***.	
		(81a) Apart from the international commitments the third country or international organisation has	

		entered into, the Commission should also take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult with the European Data Protection Board when assessing the level of protection in third countries or international organisations[43].	
		(81b) The Commission should monitor the functioning of decisions on the level of protection in a third country or a territory or	

[43] ***DE, supported by NL, proposed that the list of checks in Article 42(2) should include a new component consisting of the participation of third states or international organisations in international data-protection systems (e.g. APEC and ECOWAS). According to the position of DE, although those systems are still in the early stages of practical implementation, the draft Regulation should make allowance right away for the significance they may gain in future. Point (d) of Article 41(2) requires the systems to be fundamentally suited to ensuring compliance with data protection standards.***

		specified sector within a third country, or an international organisation, including decisions adopted on the basis of Article 25(6) or Article 26 (4) of Directive 95/46/EC. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any pertinent findings to the Committee within the meaning of Regulation (EU) No 182/2011 as established under this Regulation.	
	Amendment 55		
(82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation offers no adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited. In that case, provision should be made for consultations between the Commission and such third countries or international organisations.	(82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation offers no adequate level of data protection. ***Any legislation which provides for extra-territorial access to personal data processed in the Union without authorisation under Union or Member State law should be considered as an indication of a lack of adequacy.*** Consequently the transfer of personal data to that third country	(82) The Commission may ~~equally~~ recognise that a third country, or a territory or a ~~processing~~ ***specified*** sector within a third country, or an international organisation ~~offers~~ no ***longer ensures an*** adequate level of data protection. Consequently the transfer of personal data to that third country ***or international organisation*** should be prohibited, ***unless the requirements of Articles 42 to 44 are fulfilled***. In that case, provision should be made for consultations between the Commission and such third	

	should be prohibited. In that case, provision should be made for consultations between the Commission and such third countries or international organisations.	countries or international organisations. ***The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation***.	
	Amendment 56		
(83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory	(83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority~~, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory~~	(83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or ***ad hoc*** contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by	

authority.	~~authority~~. ***Those appropriate safeguards should uphold a respect of the data subject's rights adequate to intra-EU processing, in particular relating to purpose limitation, right to access, rectification, erasure and to claim compensation. Those safeguards should in particular guarantee the observance of the principles of personal data processing, safeguard the data subject's rights and provide for effective redress mechanisms, ensure the observance of the principles of data protection by design and by default, guarantee the existence of a data protection officer.***	a supervisory authority. ***Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. They should relate in particular to compliance with the general principles relating to personal data processing, the availability of enforceable data subject's rights and of effective legal remedies and the principles of data protection by design and by default. Transfers may be carried out also by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding. The authorisation of the competent supervisory authority should be obtained when the safeguards are adduced in non legally binding administrative arrangements.***	

	Amendment 57		
(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.	(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses ***or supplementary safeguards*** as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted ~~by the Commission or~~ by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. ***The standard data protection clauses adopted by the Commission could cover different situations, namely transfers from controllers established in the ~~European~~ Union to controllers established outside the ~~European~~ Union and from controllers established in the ~~European~~ Union to processors, including sub-processors, established outside the ~~European~~ Union. Controllers and processors***	(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract***, including in a contract between the processor and another processor,*** nor to add other clauses ***or additional safeguards*** as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.	

	should be encouraged to provide even more robust safeguards via additional contractual commitments that supplement standard protection clauses.		
	Amendment 58		
(85) A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.	(85) A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, as long as such corporate rules include ***all*** essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data	(85) A corporate group ***or a group of enterprises engaged in a joint economic activity*** should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings ***or group of enterprises***, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.	
	Amendment 59		
(86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal	(86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal	(86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his ***explicit*** consent, where the transfer is ~~necessary~~ ***occasional*** in relation to	

claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.	claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients***, taking into full account the interests and fundamental rights of the data subject***.	a contract or a legal claim, ***regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers*** where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.	
	Amendment 60		
(87) These derogations should in particular apply to data transfers required and necessary for the	(87) These derogations should in particular apply to data transfers required and necessary for the	(87) These ~~derogations~~ ***rules*** should in particular apply to data transfers required and necessary for ~~the~~	

protection of important grounds of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters, or to competent authorities for the prevention, investigation, detection and prosecution of criminal offences.	protection of important grounds of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters ***or for public health***, or to competent ***public*** authorities for the prevention, investigation, detection and prosecution of criminal offences***, including for the prevention of money laundering and the fight against terrorist financing. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's life, if the data subject is incapable of giving consent. Transferring personal data for such important grounds of public interest should only be used for occasional transfers. In each and every case, a careful assessment of all circumstances of the transfer***	~~protection of~~ important ~~grounds~~ ***reasons*** of public interest, for example in cases of international data ~~transfers~~ ***exchange*** between competition authorities, tax or customs administrations, ***beteween*** financial supervisory authorities, between services competent for social security matters, or ~~to competent authorities~~ for ~~the prevention, investigation, detection and prosecution of criminal offences~~***for public health, for example in case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent.[44] In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the***	

[44] ***FR referred to the situation of a recipient of the transfer who is a medical professional or has adduced provisions ensuring the respect of the data subject's right to privacy and medical confidentiality. PRES considers that this could be further addressed in the context of Chapter IX.***

	should be carried out.	***transfer of specific categories of data to a third country or an international organization. Member States should notify such provisions to the Commission.***	
	Amendment 61		
(88) Transfers which cannot be qualified as frequent or massive, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when they have assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.	(88) ~~Transfers which cannot be qualified as frequent or massive, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when they have assessed all the circumstances surrounding the data transfer.~~ For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.	(88) Transfers which cannot be qualified as ***large scale or*** frequent ~~or massive~~, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when ~~they have~~ ***those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller or the processor has*** assessed all the circumstances surrounding the data transfer. ***The controller or processor should give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced suitable safeguards to protect fundamental rights and freedoms***	

		of natural persons with respect to processing of their personal data. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. ***To assess whether a transfer is large scale or frequent the amount of personal data and number of data subjects should be taken into account and whether the transfer takes place on an occasional or regular basis.***	
	Amendment 62		
(89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.	(89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a ***legally binding*** guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once those data have been transferred***, to the extent that the processing is not massive, not***	(89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.	

	repetitive and not structural. That guarantee should include financial indemnification in cases of loss or unauthorised access or processing of the data and an obligation, regardless of national legislation, to provide full details of all access to the data by public authorities in the third country.		
	Amendment 63		
(90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. . Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the	(90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the	(90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the	

disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act.	disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act. ***In cases where controllers or processors are confronted with conflicting compliance requirements between the jurisdiction of the Union on the one hand, and that of a third country on the other, the Commission should ensure that Union law takes precedence at all times. The Commission should provide guidance and assistance to the controller and processor, and it should seek to resolve the jurisdictional conflict with the third country in question***.	disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. ~~The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act.~~	
(91) When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the	(91) When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the	(91) When personal data moves across borders ***outside the Union*** it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the	

unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts.	unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts.	unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. ***For the purposes of developing international co-operation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with***	

		competent authorities in third countries, based on reciprocity and in compliance with the provisions of this Regulation, including those laid down in Chapter V.	
	Amendment 64		
(92) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.	(92) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. ***An authority shall have adequate financial and personal resources to fully carry out its role, taking into account the size of the population and the amount of personal data processing.***	(92) The establishment of supervisory authorities in Member States, ***empowered to perform their tasks and*** ~~exercising~~ exercise their ~~functions~~ ***powers*** with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.	
		(92a) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subjected to control or monitoring mechanism	

		regarding their financial expenditure. Neither does it imply that supervisory authorities cannot be subjected to judicial review.	
(93) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.	(93) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.	(93) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.	
	Amendment 65		
(94) Each supervisory authority should be provided with the adequate financial and human resources, premises and infrastructure, which is necessary for the effective performance of their tasks, including for the tasks	(94) Each supervisory authority should be provided with the adequate financial and human resources, ***paying particular attention to ensuring adequate technical and legal skills of staff,*** premises and infrastructure, which	(94) Each supervisory authority should be provided with the ~~adequate~~ financial and human resources, premises and infrastructure, which ~~is~~ are necessary for the effective performance of their tasks,	

related to mutual assistance and co-operation with other supervisory authorities throughout the Union.	is necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union.	including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union. ***Each supervisory authority should have a separate annual budget, which may be part of the overall state or national budget.***	
	Amendment 66		
(95) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government of the Member State, and include rules on the personal qualification of the members and the position of those members.	(95) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be ~~either~~ appointed by the parliament or the government of the Member State ***taking due care to minimise the possibility of political interference***, and include rules on the personal qualification of the members***, the avoidance of conflicts of interest*** and the position of those members.	(95) The general conditions for the ***member or*** members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament ***and/***or the government ***or the heade of State*** of the Member State~~, and include rules on the personal qualification of the members and the position of those members~~***or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure. In order to ensure the independence of the supervisory authority, the member or members should refrain from any action incompatible with their***	

		duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not.	
		(95a) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest proceesing affecting data subjects on its territory or processing carried out by a controller or processor not established in the European Union when targeting data subjects residing in its territory. This should include dealing with complaints lodged by a data subject, conducting investigations on the application of the Regulation, promoting public	

		awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.	
(96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should co-operate with each other and the Commission.	(96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should co-operate with each other and the Commission.	(96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, ***this Regulation should oblige and empower*** the supervisory authorities ~~should~~ to co-operate with each other and the Commission***, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation***.	
		(96a) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one	

		Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities tha t are concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority to which scuh complaint has been lodged should also be a concerned supervisory authority. Within its tasks to issue guidelines on any question covering the application	

		of this Regulation, the European Data Protection Board may issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection[45].	
		(96b) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with the provisions of this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the concerned supervisory authorities in the decision-making process. In cases where the decisions is to reject the complaint by the data subject in whole or in part that decision should be adopted by the supervisory authority at which the complaint has been lodged.	

[45] ***DE proposal; CZ and LU scrutiny reservation.***

		(96c) The decision should be agreed jointly by the lead supervisory authority and the concernec supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure the compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.	
	Amendment 67		
(97) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or	(97) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should ~~be competent for monitoring the activities of~~ ***act as the single***	***Moved modified under 96a***	

processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.	***contact point and the lead authority responsible for supervising*** the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.		
		(97) Each supervisory authority not acting as lead supervisory authority should be competent to deal with local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involving only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay on this matter. After being informed, the lead supervisory authority should	

		decide, whether it will deal with the case within the one-stop-shop mechanism or whether the supervisory authority which informed it should deal with the case at local level. When deciding whether it will deal with the case, the lead supervisory authority should take into account, whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it, in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to deal with the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in the one-stop-shop mechanism.	
	Amendment 68		
(98) The competent authority, providing such one-stop shop,	(98) The ~~competent~~ ***lead*** authority, providing such one-stop shop,	(98) The ~~competent~~ ***rules on the lead supervisory*** authority~~,~~	

should be the supervisory authority of the Member State in which the controller or processor has its main establishment.	should be the supervisory authority of the Member State in which the controller or processor has its main establishment ***or its representative***. ***The European Data Protection Board may designate the lead authority through the consistency mechanism in certain cases at the request of a competent authority.***	~~providing such~~ ***and the*** one-stop-shop ***mechanism***, should ***not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases*** ~~be~~ the ***only*** supervisory authority ***competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority*** of the Member State ***where the public authority pro private body is established*** ~~in which the controller or processor has its main establishment~~.	
	Amendment 69		
	(98a) Data subjects whose personal data ~~***is***~~ ***are processed by a data controller or processor in another Member State should be able to complain to the supervisory authority of their choice. The lead data protection authority should coordinate its work with that of the other authorities involved.***		
(99) While this Regulation applies also to the activities of national courts, the competence of the supervisory authorities should	(99) While this Regulation applies also to the activities of national courts, the competence of the supervisory authorities should not	***deleted***	

not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. However, this exemption should be strictly limited to genuine judicial activities in court cases and not apply to other activities where judges might be involved in, in accordance with national law.	cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. However, this exemption should be strictly limited to genuine judicial activities in court cases and not apply to other activities where judges might be involved in, in accordance with national law.		
(100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. Investigative powers of supervisory authorities as regards access to premises should be exercised in conformity with Union law and national law. This concerns in particular the requirement to obtain a prior	(100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. Investigative powers of supervisory authorities as regards access to premises should be exercised in conformity with Union law and national law. This concerns in particular the requirement to obtain a prior	(100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same ~~duties~~ tasks and effective powers, including powers of investigation, ***corrective powers*** ~~legally binding intervention, decisions~~ and sanctions, ***and authorisation and advisory powers,*** particularly in cases of complaints from individuals, ***and without prejudice to the powers of prosecutorial authorities under national law, to bring infringments of this Regulation to the attention of the judicial***	

judicial authorisation.	judicial authorisation.	***authorities*** and***/or*** to engage in legal proceedings. ***Such powers should also include the power to forbid the processing on which the authority is consulted. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in conformity with appropriate procedural safeguards set out in Union law and national law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned.*** ~~Investigative~~ Investigatory powers ~~of supervisory authorities~~ as regards access to premises should	

		be exercised in ~~conformity~~ ***accordance with specific requirements in national procedural law, such as*** ~~with Union law and national law. This concerns in particular~~ the requirement to obtain a prior judicial authorisation. ***Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to national procedural law. The adoption of such legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.***	

	Amendment 70		
(101) Each supervisory authority should hear complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.	(101) Each supervisory authority should hear complaints lodged by any data subject ***or by associations acting in the public interest*** and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject ***or the association*** of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.	(101) ~~Each~~ ***Where the*** supervisory authority ~~should hear~~ ***to which the*** complaint~~s~~ ***has been*** lodged ***is not the lead supervisory authority, the lead supervisory authority should closely co-operate with the supervisory authority to which the complaint has been lodged according to the provisions on co-operation and consistency laid down in this Regulation. In such cases,*** ~~by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The~~***the lead*** supervisory authority should***, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the*** ~~inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another~~ supervisory authority~~, intermediate~~	

		~~information should be given to the data subject~~ ***to which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority***.	
		(101a) The supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of the Regulation should seek an amicable settlement and, if this proves unsuccessful, exercise its full range of powers in cases where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the one Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect	

		or is not likely to substantially affect data subjects in other Member States. This should include specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; or to processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or that has to be assessed taking into account relevant legal obligations under national law.	
(102) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as data subjects.	(102) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as data subjects.	(102) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as ~~data subjects~~***individuals in particular in the educational context***.	
(103) The supervisory authorities should assist each other in	(103) The supervisory authorities should assist each other in	(103) The supervisory authorities should assist each other in	

performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market.	performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market.	performing their ~~duties~~ ***tasks*** and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. ***Where a supervisory authority requesting mutual assistance, in the case of no response of the requested supervisory authority within one month of receiving the request, adopts a provisional measure, such provisional measure should be duly justified and only of a temporary nature.***	
(104) Each supervisory authority should have the right to participate in joint operations between supervisory authorities. The requested supervisory authority should be obliged to respond to the request in a defined time period.	(104) Each supervisory authority should have the right to participate in joint operations between supervisory authorities. The requested supervisory authority should be obliged to respond to the request in a defined time period.	(104) Each supervisory authority should have the right to participate in joint operations between supervisory authorities. The requested supervisory authority should be obliged to respond to the request in a defined time period.	
	Amendment 71		
(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established.	(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established.	(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities ~~themselves and the Commission~~ should be established.	

This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, , or to the monitoring such data subjects, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.	This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, or to the monitoring ***of*** such data subjects, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. ***Furthermore, the data subjects should have the right to obtain consistency, if they deem a measure by a Data Protection Authority of a Member State has not fulfilled this criterion***. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.	This mechanism should in particular apply where a supervisory authority intends to ~~take~~ ***adopt*** a measure ***intended to produce legal effects*** as regards processing operations ~~that are related to the offering of goods or services to data subjects in several Member States, , or to the monitoring such data subjects, or that might~~ ***which*** substantially affect ***a significant number of data subjects in several Member States.*** ~~the free flow of personal data.~~ It should also apply where any ***concerned*** supervisory authority or the Commission[46] requests that ~~the~~ ***such*** matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.	
(106) In application of the consistency mechanism, the European Data Protection Board	(106) In application of the consistency mechanism, the European Data Protection Board	(106) In application of the consistency mechanism, the European Data Protection Board	

[46] ***HU reservation on the reference to the Commission.***

should, within a determined period of time, issue an opinion, if a simple majority of its members so decides or if so requested by any supervisory authority or the Commission.	should, within a determined period of time, issue an opinion, if a simple majority of its members so decides or if so requested by any supervisory authority or the Commission.	should, within a determined period of time, issue an opinion, if a ~~simple~~ majority of its members so decides or if so requested by any ***concerned*** supervisory authority ***concerned*** or the Commission. ***The European Data Protection Board should also be empowered to adopt legally binding decisions in case of disputes between supervisory authorities. For that purposes it should issue, in principle with a two-third majority of its members, legally binding decisions in clearly defined cases where there are conflicting views among supervisory authorities in particular in the cooperation mechanism between the lead supervisory authority and concerned supervisory authorities on the merits of the case, notably whether there is an infringement of this Regulation or not.***	
	Amendment 72		
	(106a) In order to ensure the consistent application of this Regulation, the European Data Protection Board may in		

	individual cases adopt a decision which is binding on the competent supervisory authorities.		
	Amendment 73		
(107) In order to ensure compliance with this Regulation, the Commission may adopt an opinion on this matter, or a decision, requiring the supervisory authority to suspend its draft measure.	***deleted***	***deleted***	
(108) There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.	(108) There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.	(108) There may be an urgent need to act in order to protect the ***rights and freedoms*** ~~interests~~ of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.	
(109) The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision by a supervisory authority.	(109) The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision by a supervisory authority.	(109) The application of this mechanism should be a condition for the ~~legal validity and enforcement of the respective decision~~ ***lawfulness of a measure***	

In other cases of cross-border relevance, mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.	In other cases of cross-border relevance, mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.	***intended to produce legal effects*** by a supervisory authority ***in those cases where its application is mandatory***. In other cases of cross-border relevance, ***the co-operation mechanism between the lead supervisory authority and concerned supervisory authorities should be applied and*** mutual assistance and joint ~~investigations~~ ***operations*** might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.	
	Amendment 74		
(110) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities. The European Data	(110) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. ~~The Commission should participate in its activities.~~ The European Data	(110) ***In order to promote the consistent application of this Regulation,*** ~~At Union level, a~~ ***the*** European Data Protection Board should be set up ***as an independent body of the Union***. ***To fulfil its objectives, the European Data Protection Board should have legal personality. The European Data Protection Board should be represented by its Chair.*** It should replace the Working Party on the Protection of Individuals with	

Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.	Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the ~~Commission~~ ***institutions of the Union*** and promoting co-operation of the supervisory authorities throughout the Union***, including the coordination of joint operations***. The European Data Protection Board should act independently when exercising its tasks. ***The European Data Protection Board should strengthen the dialogue with concerned stakeholders such as data subjects' associations, consumer organisations, data controllers and other relevant stakeholders and experts.***	Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State ***or his or her representative*** ~~and of~~. ~~the~~ The Commission and the European Data Protection Supervisor ~~. The Commission~~ should participate in its activities ***without voting rights***. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission***, in particular on the level of protection in third countries or international organisations,*** and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.	
		(110a) The European Data Protection Board should be assisted by a secretariat provided by the secretariat of the European Data Protection Supervisor. The	

		staff of the secretariat of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation should perform its tasks exclusively under the instructions of, and report to the Chair of the European Data Protection Board. Organisational separation of staff should concern all services needed for the independent functioning of the European Data Protection Board	
	Amendment 75		
(111) Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject.	(111) ~~Every data~~ ***Data*** ~~subject~~ ***subjects*** should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to ~~a~~ ***an effective*** judicial remedy ***in accordance with Article 47 of the Charter*** ~~***of Fundamental Rights***~~ if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of	(111) Every data subject should have the right to lodge a complaint with a supervisory authority***, in particular in the Member State of his or her habitual residence,*** ~~in any Member State~~ and have the right to a***n effective*** judicial remedy ***in accordance with Article 47 of the Charter of Fundamental Rights if the data subject*** ~~if they~~ consider***s*** that ~~their~~ ***his or her*** rights under this Regulation are infringed or where the supervisory authority does not ~~re~~act on a complaint***,***	

	the data subject.	***partially or wholly rejects or dismisses a complaint*** or does not act where such action is necessary to protect the rights of the data subject. ***The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can be completed also electronically, without excluding other means of communication.***	
	Amendment 76		
(112) Any body, organisation or association which aims to protects	(112) Any body, organisation or association which ~~aims to protects~~	(112) ***Where a data subject considers that his or her rights***	

the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.	~~the rights and interests of data subjects in relation to the protection of their data~~ ***acts in the public interest*** and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority ***on behalf of data subjects with their consent*** or exercise the right to a judicial remedy ~~on behalf of~~ ***if mandated by the*** data ~~subjects~~***subject***, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a ~~personal data~~ breach ***of this Regulation*** has occurred.	***under this Regulation are infringed, he or she should have the right to mandate a***~~Any~~ body, organisation or association which aims to protect~~s~~ the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State~~, should have the right~~ to lodge a complaint ***on his or her behalf*** with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects***. Such a body, organisation or association should have the right***~~, or~~ to lodge, independently of a data subject's complaint, an ~~own~~ complaint where it ***has reasons to*** consider~~s~~ that a personal data breach ***referred to in Article 32(1)*** has occurred ***and Article 32(3) does not apply***.	
(113) Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the	(113) Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the	(113) ~~Each~~ ***Any*** natural or legal person ~~should~~ have the right to ***bring a****n action for annulment of decisions of the European Data Protection Board before the Court of Justice of the European Union (the "Court of Justice") under the conditions provided for in Article*	

supervisory authority is established.	supervisory authority is established.	***263 TFEU. As addressees of such decisions, the concerned supervisory authorities who wish to challenge them, have to bring action within two months of their notification to them, in accordance with Article 263 TFEU. Where decisions of the European Data Protection Board are of direct and individual concern to a controller, processor or the complainant, the latter may bring an action for annulment against those decisions and they should do so within two months of their publication on the website of the European Data Protection Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective*** judicial remedy ***before the competent national court*** against a decision~~s~~ of a supervisory authority ***which produces legal effects*** concerning ~~them~~***this person***. ***Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the***	

		dismissal or rejection of complaints[47]. However, this right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established ***and should be conducted in accordance with the national procedural law of that Member State. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it. Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings to the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a***	

[47] ***GR reservation.***

		decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law including this Regulation. ***Furthermore, where a decision of a supervisory authority implementing a decision of the European Data Protection Board is challenged before a national court and the validity of the decision of the European Data Protection Board is at issue, that national court does not have the power to declare the European Data Protection Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as in terpreted by the Court of Justice in the Foto-frost case[48], whenever it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the European Data Protection Board***	

[48] Case C-314/85.

		at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down by Article 263 TFEU.	
		(113a) Where a court seized with a proceeding against a decision of a supervisory authority has reason to believe that proceedings concerning the same processing activities or the same cause of action are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seized should stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if the latter has jurisdiction over the proceedings in question and its law permits the consolidation of	

		such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings.	
	Amendment 77		
(114) In order to strengthen the judicial protection of the data subject in situations where the competent supervisory authority is established in another Member State than the one where the data subject is residing, the data subject may request any body, organisation or association aiming to protect the rights and interests of data subjects in relation to the protection of their data to bring on the data subject's behalf proceedings against that supervisory authority to the competent court in the other Member State.	(114) In order to strengthen the judicial protection of the data subject in situations where the competent supervisory authority is established in another Member State than the one where the data subject is residing, the data subject may ~~request~~ ***mandate*** any body, organisation or association ~~aiming to protect the rights and interests of data subjects in relation to the protection of their data~~ ***acting in the public interest*** to bring ~~on the data subject's behalf~~ proceedings against that supervisory authority to the competent court in the other Member State.	***deleted***	

	Amendment 78		
(115) In situations where the competent supervisory authority established in another Member State does not act or has taken insufficient measures in relation to a complaint, the data subject may request the supervisory authority in the Member State of his or her habitual residence to bring proceedings against that supervisory authority to the competent court in the other Member State. The requested supervisory authority may decide, subject to judicial review, whether it is appropriate to follow the request or not.	(115) In situations where the competent supervisory authority established in another Member State does not act or has taken insufficient measures in relation to a complaint, the data subject may request the supervisory authority in the Member State of his or her habitual residence to bring proceedings against that supervisory authority to the competent court in the other Member State. ***This does not apply to non-EU residents.*** The requested supervisory authority may decide, subject to judicial review, whether it is appropriate to follow the request or not.	***deleted***	
	Amendment 79		
(116) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the	(116) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or***, in case of EU residence,*** where the data subject resides, unless the	(116) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public	

controller is a public authority acting in the exercise of its public powers.	controller is a public authority ***of the Union or a Member State*** acting in the exercise of its public powers.	authority acting in the exercise of its public powers.	
(117) Where there are indications that parallel proceedings are pending before the courts in different Member States, the courts should be obliged to contact each other. The courts should have the possibility to suspend a case where a parallel case is pending in another Member State. Member States should ensure that court actions, in order to be effective, should allow the rapid adoption of measures to remedy or prevent an infringement of this Regulation.	(117) Where there are indications that parallel proceedings are pending before the courts in different Member States, the courts should be obliged to contact each other. The courts should have the possibility to suspend a case where a parallel case is pending in another Member State. Member States should ensure that court actions, in order to be effective, should allow the rapid adoption of measures to remedy or prevent an infringement of this Regulation.	***deleted***	
	Amendment 80		
(118) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where he establishes fault on the part of the data subject	(118) Any damage***, whether pecuniary or not,*** which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability ***only*** if ~~they prove~~ ***he proves*** that ~~they are~~ ***he is*** not responsible for the damage, in particular where he establishes fault on the part of the	(118) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where he establishes fault on the part of the data subject or in case of force majeure. ***The concept***	

or in case of force majeure.	data subject or in case of force majeure.	***of damage should be broadly interpreted in the light of the case law of the Court of Justice of the European Union in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law[49].***	
		(118a) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation No 1215/2012 should not prejudice the application of such specific rules[50].	
		(118b) In order to strengthen the enforcement of the rules of this Regulation, penalties and administrative fines may be imposed for any infringement of the Regulation, in addition to, or	

[49] ***COM scrutiny reservation.***

[50] ***COM and DE scrutiny reservation.***

		instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. The imposition of penalties and administrative fines should be subject to adequate procedural safeguards in conformity with general principles of Union law and the Charter of Fundamental Rights, including effective judicial protection and due process.	
	Amendment 81		
(119) Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties.	(119) Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties. ***The rules on penalties should be subject to appropriate procedural safeguards in conformity with the general principles of Union law and the Charter*** ~~***of Fundamental Rights***~~***, including those concerning the right to an effective judicial***	(119) ***Member States may lay down the rules on criminal sanctions for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of*** ~~Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with~~ this Regulation. ***These criminal sanctions may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal***	

	remedy, due process and the principle of ne bis in idem.	***sanctionsfor infringements of such national rules and of administrative sanctions*** ~~Member States should ensure that the penalties~~ should ~~be effective, proportionate and dissuasive and should take all measures to implement the penalties.~~***not lead to the breach of the principle of ne bis in idem, as interpreted by the Court of Justice.***	
	Amendment 82		
	(119a) In applying penalties, Member States should show full respect for appropriate procedural safeguards, including the right to an effective judicial remedy, due process, and the principle of ne bis in idem.		
(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each	(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each	(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to ***impose*** ~~sanction~~ administrative ~~offences~~***fines***. This Regulation should indicate ~~these~~ offences ~~and~~, the upper limit ***and criteria*** for ***fixing*** the related administrative	

individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.	individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.	fines, which should be ~~fixed~~ ***determined by the competent supervisory authority*** in each individual case***, taking into account all relevant circumstances of*** ~~proportionate to~~ the specific situation, with due regard in particular to the nature, gravity and duration of the breach ***and of its consequences and the measures taken to ensure compliance with the obligations under the Regulation and to prevent or mitigate the consequences of the infringement***. The consistency mechanism may also be used to ***promote a consistent*** ~~cover divergences in the~~ application of administrative sanctions. ***It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other sanctions under the Regulation.***	

	Amendment 83		
(121) The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the	(121) ~~The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption~~ ***Whenever necessary, exemptions or derogations*** from the requirements of certain provisions of this Regulation ***for the processing of personal data should be provided for*** in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter~~of Fundamental Rights of the European Union~~. ~~This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries.~~ Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member	(121) ***Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation.*** The processing of personal data solely for journalistic purposes, or for the purposes of ***academic,*** artistic or literary expression should ***be subject to*** ~~qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union.~~ ***derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data, with the right to freedom of expression and information, as***	

transfer of data to third countries or international organisations, on the independent supervisory authorities and on co-operation and consistency. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as 'journalistic' for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.	States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities**,** ~~and~~ on co-operation and consistency ***and on specific data processing situations***. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom~~,~~ ~~such as journalism,~~ broadly~~.~~ ~~Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these~~ ***to cover all*** activities ~~is~~ ***which aim at*** the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them***, also taking into account technological development***. They should not be limited to media undertakings and	***guaranteed by Article 11 of the Charter of Fundamental Rights of the European Union.*** This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities and on co-operation and consistency. ***In case these exemptions or derogations differ from one Member State to another, the national law of the Member State to which the controller is subject should apply.*** ~~This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In~~	

	may be undertaken for profit-making or for non-profit making purposes.	~~order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as 'journalistic' for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.~~***In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.***	
		(121a) This Regulation allows the principle of public access to official documents to be taken into account when applying the	

		provisions set out in this Regulation. Public access to official documents may be considered as a public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by this authority or body if the disclosure is provided for by Union law or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary derogations from the rules of this regulation. The reference to public authorities and bodies should in this context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information leaves intact and in no way affects the level of protection of individuals	

		with regard to the processing of personal data under the provisions of Union and national law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents access to which is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data[51].	
(122) The processing of personal data concerning health, as a special category of data which deserves higher protection, may often be justified by a number of legitimate reasons for the benefit of individuals and society as a whole, in particular in the context of ensuring continuity of cross-border	(122) The processing of personal data concerning health, as a special category of data which deserves higher protection, may often be justified by a number of legitimate reasons for the benefit of individuals and society as a whole, in particular in the context of ensuring continuity of cross-border	***Moved to recital 42a[52]***	

[51] ***Moved from recital 18.***

[52] ***Moved to recital 42a.***

healthcare. Therefore this Regulation should provide for harmonised conditions for the processing of personal data concerning health, subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals. This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.	healthcare. Therefore this Regulation should provide for harmonised conditions for the processing of personal data concerning health, subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals. This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.		
	Amendment 84		
	(122a) A professional who processes personal data concerning health should receive, if possible, anonymised or pseudonymised data, leaving the knowledge of the identity only to the ~~General~~ general ~~Practitioner~~ practitioner or to the ~~Specialist~~ specialist who has requested such data processing.		

	Amendment 85		
(123) The processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of personal data concerning health for reasons of public interest should not result in personal data being	(123) The processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the ~~Council~~ ***~~44b~~*** Council ***1*** ~~of 16 December 2008 on Community statistics on public health and health and safety at work~~, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. ~~Such processing of personal data concerning health for reasons of public interest should not result in~~	***Moved to recital 42b[53].***	

[53] ***Moved to recital 42b.***

processed for other purposes by third parties such as employers, insurance and banking companies.	~~personal data being processed for other purposes by third parties such as employers, insurance and banking companies.~~ _____ ~~44b~~ 1b ***Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).***		
	Amendment 86		
	123a) The processing of personal data concerning health, as a special category of data, may be necessary for reasons of historical, statistical or scientific research. Therefore this Regulation foresees an exemption from the requirement of consent in cases of research that serves a high public interest.		
	Amendment 87		
(124) The general principles on the protection of individuals with regard to the processing of personal	(124) The general principles on the protection of individuals with regard to the processing of personal	(124) ~~The general principles on the protection of individuals with regard to the processing of personal~~	

data should also be applicable to the employment context. Therefore, in order to regulate the processing of employees' personal data in the employment context, Member States should be able, within the limits of this Regulation, to adopt by law specific rules for the processing of personal data in the employment sector.	data should also be applicable to the employment ***and the social security*** context. ~~Therefore, in order~~ ***Member States should be able*** to regulate the processing of employees' personal data in the employment ***and the processing of personal data in the social security*** context ***in accordance with the rules and minimum standards set out in***~~, Member States should be able, within the limits of~~ this Regulation~~, to adopt by law specific rules for~~***. Where a statutory basis is provided in the Member State in question for the regulation of employment matters by agreement between employee representatives and the management of the undertaking or the controlling undertaking of a group of undertakings (collective agreement) or under Directive 2009/38/EC of the European Parliament and of the*** ~~***Council***~~[44e]***Council***[1]***,*** the processing of personal data in ~~the~~ ***an*** employment~~ sector~~ ***context may also be regulated by such an***	~~data should also be applicable to the employment context. Therefore, in order to regulate the processing of employees' personal data in the employment context, Member States should be able, within the limits of this Regulation, to adopt by law specific rules for the processing of personal data in the employment sector.~~***National law or collective agreements (including 'works agreements')***[54] ***may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace , health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose***	

[54] ***DE proposal.***

	agreement. ***[44e] [1] Directive 2009/38/EC of the European Parliament and of the Council of 6 May 2009 on the establishment of a European Works Council or a procedure in Community-scale undertakings and Community-scale groups of undertakings for the purposes of informing and consulting employees (OJ L 122, 16.5.2009, p. 28).***	***of the termination of the employment relationship.***	
(125) The processing of personal data for the purposes of historical, statistical or scientific research should, in order to be lawful, also respect other relevant legislation such as on clinical trials.	(125) The processing of personal data for the purposes of historical, statistical or scientific research should, in order to be lawful, also respect other relevant legislation such as on clinical trials.	(125) The processing of personal data for the purposes of historical, statistical or scientific ~~research~~ ***purposes and for archiving purposes in the public interest*** should, ***in addition to the general principles and specific rules of this Regulation, in particular as regards the conditions for*** ~~in order to be~~ lawful ***processing***, also ***comply with*** respect other relevant legislation such as on clinical trials.***The further processing of personal data for historical, statistical and scientific purposes and for archiving purposes in the public interest (…) should not be***	

		considered incompatible with the purposes for which the data are initially collected and may be processed for those purposes for a longer period than necessary for that initial purpose (…). Member States should be authorised to provide, under specific conditions and in the presence of appropriate safeguards for data subjects, specifications and derogations to the information requirements and the rights to access, rectification, erasure, to be forgotten, restriction of processing and on the right to data portability and the right to object when processing personal data for historical, statistical or scientific purposes and for archiving purposes (…) The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality	

		and necessity principles.	
	Amendment 88		
	(125a) Personal data may also be processed subsequently by archive services whose main or mandatory task is to collect, conserve, provide information about, exploit and disseminate archives in the public interest. Member State legislation should reconcile the right to the protection of personal data with the rules on archives and on public access to administrative information. Member States should encourage the drafting, in particular by the European Archives Group, of rules to guarantee the confidentiality of data vis-à-vis third parties and the authenticity, integrity and proper conservation of data.		
		Moved to recitals 126c and 126d.[55]	
		(125aa) By coupling information from registries, researchers can obtain new knowledge of great value when it comes to e.g.	

[55] ***Moved to recitals 126c and 126d.***

		widespread diseases as cardiovascular disease, cancer, depression etc. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about long-term impact of a number of social conditions e.g. unemployment, education, and the coupling of this information to other life conditions. Research results obtained on the basis of registries provide solid, high quality knowledge, which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people, and improve the efficiency of social services etc. ***In order to facilitate scientific research, personal data can be processed for scientific purposes subject to appropriate conditions and safeguards set out in Member State or Union law. Hence consent from the data subject should not be necessary for each further***	

		processing for scientific purposes.	
		(125b) The importance of archives for the understanding of the history and culture of Europe" and "that well-kept and accessible archives contribute to the democratic function of our societies', were underlined by Council Resolution of 6 May 2003 on archives in the Member States[56]. Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. ***Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to***	

[56] ***OJ C 113, 13.5.2003, p. 2.***

		provide that personal data may be further processed for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes[57]. ***Codes of conduct may contribute to the proper application of this Regulation, including when personal data are processed for archiving purposes in the public interest by further specifying appropriate safeguards for the rights and freedoms of the data subject[58]. Such codes should be drafted by Member States' official archives or by the European Archives Group. Regarding international transfers of personal data included in archives, these must take place without prejudice of the applying European and national rules for the circulation of cultural goods and national treasures.***	

[57] ***CZ reservation.***

[58] ***CZ, DK, FI, HU, FR, MT, NL, PT, RO, SE, SI and UK scrutiny reservation.***

	Amendment 89		
(126) Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area.	(126) Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area. ***The processing of personal data for historical, statistical and scientific research purposes should not result in personal data being processed for other purposes, unless with the consent of the data subject or on the basis of Union or Member State law.***	(126) ***Where personal data are processed for*** ~~Scientific~~ scientific ~~research for the~~ purposes, ~~of~~ this Regulation should ***also apply to that processing. For the purposes of this Regulation, processing of personal data for scientific purposes should*** include fundamental research, applied research, ~~and~~ privately funded research[59] and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area***. Scientific purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific purposes specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific purposes. If the result of***	

[59] ***AT and SE scrutiny reservation.***

		scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures[60].	
		(126a) Where personal data are processed for historical purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.	
		(126b) For the purpose of consenting to the participation in scientific research activities in clinical trials (…) the relevant provisions of Regulation (EU) No. 536/2014 of the European Parliament and of the Council should apply.	
		(126c) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union law or	

[60] ***CZ, DK, FI, FR, HU, MT, NL, PT, SE, SI and UK scrutiny reservation.***

		Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for guaranteeing statistical confidentiality.	
		(126d) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in conformity with the statistical principles as set out in Article 338(2) of the Treaty of the Functioning of the European Union, while national statistics should also comply with national law. ***Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No***	

		1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities[61] provides further specifications on statistical confidentiality for European statistics.	
(127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy.	(127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy.	(127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. ***This is without prejudice to***	

[61] ***OJ L 87, 31.3.2009, p. 164–173.***

		existing Member State obligations to adopt professional secrecy where required by Union law.	
	Amendment 90		
(128) This Regulation respects and does not prejudice the status under national law of churches and religious associations or communities in the Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union. As a consequence, where a church in a Member State applies, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, these existing rules should continue to apply if they are brought in line with this Regulation. Such churches and religious associations should be required to provide for the establishment of a completely independent supervisory authority.	(128) This Regulation respects and does not prejudice the status under national law of churches and religious associations or communities in the Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union. As a consequence, where a church in a Member State applies, at the time of entry into force of this Regulation, ~~comprehensive~~ ***adequate*** rules relating to the protection of individuals with regard to the processing of personal data, these existing rules should continue to apply if they are brought in line with this Regulation ***and recognised as compliant***. ~~Such churches and religious associations should be required to provide for the establishment of a completely independent supervisory authority.~~ .	(128) This Regulation respects and does not prejudice the status under ***existing constitutional*** ~~national~~ law of churches and religious associations or communities in the Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union. ~~As a consequence, where a church in a Member State applies, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, these existing rules should continue to apply if they are brought in line with this Regulation. Such churches and religious associations should be required to provide for the establishment of a completely independent supervisory authority.~~	

	Amendment 91		
(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements	(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of ~~lawfulness of processing~~; specifying ~~the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access~~ ***conditions of icon-based mode for provision of information***; the right to ~~be forgotten and to~~ erasure; ~~measures~~	(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the	

in relation to the responsibility of the controller and to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical	~~based on profiling; criteria and requirements in relation to the responsibility of the controller and to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer;~~ ***declaring that*** codes of conduct ***are in line with this Regulation***; criteria and requirements for certification mechanisms; ***the adequate level of protection afforded by a third country or an international organisation;*** criteria and requirements for transfers by way of binding corporate rules;	responsibility of the controller and to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific ~~research~~ purposes. It is of	

and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Councill.	~~transfer derogations;~~ administrative sanctions; processing for health purposes~~;~~ ***and*** processing in the employment context ~~and processing for historical, statistical and scientific research purposes~~. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, ***in particular with the European Data Protection Board***. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and ***to the*** Council..	particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Councill.	
	Amendment 92		
(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for	(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms ***for specific methods to obtain verifiable consent*** in relation to the processing of personal data of a child; standard ~~procedures and~~	(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for	

the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in	forms for ~~exercising the rights of~~ ***the communication to the*** data subjects ***on the*** ~~***exercice***~~ ***exercise*** ***of their*** rights; standard forms for the information to the data subject; standard forms ~~and procedures~~ in relation to the right of access ***including for communicating the personal data to the data subject***; ~~the right to data portability;~~ standard forms in relation to ~~the responsibility of the controller to data protection by design and by default and to~~ the documentation ***to be kept by the controller and the processor***; ~~specific requirements for the security of processing;~~ the standard ~~format and the procedures~~ ***form*** for the notification of a personal data breach to the supervisory authority and ~~the communication of a personal data breach to the data subject~~ ***for documenting a personal data breach***; ~~standards and procedures for a data protection impact assessment;~~ forms ~~and procedures~~ for prior ~~authorisation and prior~~ consultation~~; technical standards and mechanisms for certification; the adequate level of protection~~	the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in	

accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers45. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.	~~afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism~~ ***and information to the supervisory authority***. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the ~~Council[45]~~ Council ~~of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[1].~~ In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises. ~~45~~ 1 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general	accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[62]. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.	

[62] ***Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, OJ L 55, 28.2.2011, p. 13.***

	principles concerning mechanisms for control by ~~the~~ Member States of the Commission's exercise of implementing powers ***(***OJ L 55, 28.2.2011, p. 13***)***.		
	Amendment 93		
(131)The examination procedure should be used for the adoption of specifying standard forms in relation to the consent of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access;, the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures	(131) The examination procedure should be used for the adoption of specifying standard forms ~~in relation to the~~ ***: for specific methods to obtain verifiable*** consent ***in relation to the processing of personal data*** of a child; ~~standard procedures and forms~~ for ~~exercising the~~ ***the communication to the data subjects on the ~~exercice~~ exercise of their*** rights~~of data subjects~~; ~~standard forms~~ for the information to the data subject; ~~standard forms and procedures~~ in relation to the right of access ***including for communicating the personal data to the data subject***; ~~the right to data portability;~~ ~~standard forms~~ in relation to the ~~responsibility of~~ ***documentation to be kept by*** the controller ~~to data protection by design and by default and to the~~	(131) The examination procedure should be used for the adoption of specifying standard forms in relation to the consent of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access;~~,~~ the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures	

for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism, given that those acts are of general scope.	~~documentation~~ ***and the processor***; ~~specific requirements for the security of processing; the standard format and the procedures~~ for the notification of a personal data breach to the supervisory authority and ~~the communication of~~ ***for documenting*** a personal data breach ~~to the data subject~~; ~~standards and procedures for a data protection impact assessment; forms and procedures~~ for prior ~~authorisation and prior~~ consultation~~; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism~~, ***and information to the supervisory authority,*** given that those acts are of general scope.	for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism, given that those acts are of general scope.	
	Amendment 94		
(132) The Commission should	***Deleted***	(132) The Commission should	

adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a processing sector within that third country or an international organisation which does not ensure an adequate level of protection and relating to matters communicated by supervisory authorities under the consistency mechanism, imperative grounds of urgency so require.		adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a processing sector within that third country or an international organisation which does not ensure an adequate level of protection and relating to matters communicated by supervisory authorities under the consistency mechanism, imperative grounds of urgency so require.	
(133) Since the objectives of this Regulation, namely to ensure an equivalent level of protection of individuals and the free flow of data throughout the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order	(133) Since the objectives of this Regulation, namely to ensure an equivalent level of protection of individuals and the free flow of data throughout the Union, cannot be sufficiently achieved by the Member States ~~and~~ but can ~~therefore~~rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order	(133) Since the objectives of this Regulation, namely to ensure an equivalent level of protection of individuals and the free flow of data throughout the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to	

to achieve that objective.	to achieve that objective.	achieve that objective.	
	Amendment 95		
(134) Directive 95/46/EC should be repealed by this Regulation. However, Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC should remain in force.	(134) Directive 95/46/EC should be repealed by this Regulation. However, Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC should remain in force. ***Commission decisions and authorisations by supervisory authorities relating to transfers of personal data to third countries pursuant to Article 41(8) should remain in force for a transition period of five years after the entry into force of this Regulation unless amended, replaced or repealed by the Commission before the end of this period.***	(134) Directive 95/46/EC should be repealed by this Regulation. However, Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC should remain in force.	
(135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of	(135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council[1], including the obligations	(135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of	

individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly~~.~~	on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly. [1] Directive 2202/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.07.2002, P.37)	individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly.	
(136) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation,	(136) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen ***acquis*** to the extent that it applies to the processing of personal data by authorities involved in the implementation of that ***acquis***, within the meaning of ~~as provided for by~~ the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association ~~of those two States~~ with	***deleted***	

application and development of the Schengen acquis[46]. _____ [46] OJ L 176, 10.7.1999, p. 36.	the implementation, application and development of the Schengen acquis[46~~1~~]. _____ [46~~-1~~] OJ L 176, 10.7.1999, p. 36.		
(137) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis[47]. _____ [47] OJ L 53, 27.2.2008, p. 52	(137) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen ***acquis*** to the extent that it applies to the processing of personal data by authorities involved in the implementation of that ***acquis***, within the meaning of ~~as provided for by~~ the Agreement between the European Union, the European Community and the Swiss Confederation ~~concerning~~ on ~~the association of~~ the Swiss Confederation's association with the implementation, application and development of the Schengen ***acquis***[47~~1~~]. _____ [47~~1~~] OJ L 53, 27.2.2008, p. 52	***deleted***	
(138) As regards Liechtenstein, this Regulation constitutes a	(138) As regards Liechtenstein, this Regulation constitutes a	***deleted***[63]	

[63] ***Recitals 136, 137 and 138 were deleted as this proposal is not Schengen relevant. COM scrutiny reservation on these deletions.***

development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis[48]. _____ [48] OJ L 160 of 18.6.2011, p. 19	development of provisions of the Schengen ***acquis*** to the extent that it applies to the processing of personal data by authorities involved in the implementation of that ***acquis***, within the meaning of ~~as provided for by~~ the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen ***acquis***[~~48~~1]. _____ [~~48~~1] OJ L 160 of 18.6.2011, p. 19		
(139) In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its	(139) In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its	***deleted***[64]	

[64] ***Former recital 139 was moved up to recital 3a so as to emphasise the importance of the fundamental rights dimension of data protection in connection with other fundamental rights.***

function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity.business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity.	function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter~~ of Fundamental Rights of the European Union~~ as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity~~.business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity~~ HAVE ADOPTED THIS REGULATION.		

CHAPTER I GENERAL PROVISIONS	CHAPTER I GENERAL PROVISIONS	CHAPTER I GENERAL PROVISIONS	CHAPTER I GENERAL PROVISIONS
Article 1	***Article 1***	***Article 1***	
Subject matter and objectives	***Subject matter and objectives***	***Subject matter and objectives***	
1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.	1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data		
2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.	2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.		
		2a. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to the processing of personal data for compliance with a legal obligation or for the performance of a task	

		carried out in the public interest or in the exercise of official authority vested in the controller or for other specific processing situations as provided for in Article 6(1)(c) and (e) by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX[65].	
3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.	3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.	3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data[66].	

65 ***AT, CZ, HU, SI and SK reservation; these delegations were in favour of a minimum harmonisation clause for the public sector. LU reservation: this offers too much leeway.***

66 ***DK, FR, NL, SI scrutiny reservation.***

Article 2	***Article 2***	***Article 2***	
Material scope	***Material scope***	***Material scope***	
	Amendment 96		
1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	1. This Regulation applies to the processing of personal data wholly or partly by automated means, ***irrespective of the method of processing,*** and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system[67].	
2.This Regulation does not apply to the processing of personal data:	2. This Regulation ~~does not~~ apply to the processing of personal data:	2.This Regulation does not apply to the processing of personal data:	
(a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;	(a) in the course of an activity which falls outside the scope of Union law~~, in particular concerning national security~~;	(a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;	
(b) by the Union institutions, bodies, offices and agencies;	***deleted***	***deleted***	
(c) by the Member States when	(c) by the Member States when	(c) by the Member States when	

67 ***HU objected to the fact that data processing operations not covered by this phrase would be excluded from the scope of the Regulation and thought this was not compatible with the stated aim of a set of comprehensive EU data protection rules. HU therefore proposed to replace the second part by the following wording 'irrespective of the means by which personal data are processed'.***

carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;	carrying out activities which fall within the scope of Chapter 2 ***of Title V*** of the Treaty on European Union;	carrying out activities which fall within the scope of Chapter 2 ***of Title V*** the Treaty on European Union;	
(d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity;	(d) by a natural person ~~without any gainful interest~~ in the course of ~~its own~~ ***an*** exclusively personal or household activity***. This exemption shall also apply to a publication of personal data where it can be reasonably expected that ~~it~~ they will be only accessed by a limited number of persons;***	(d) by a natural person ~~without any gainful interest~~ in the course of ~~its own exclusively~~ ***a*** personal or household activity;	
(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.	(e) by competent ***public*** authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.	(e) by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences ***and, for these purposes[68], safeguarding of public security[69]***, or the execution of criminal penalties.	
3. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of	3. This Regulation shall ~~be without~~ prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary	***deleted***	

68 ***BE reservation on the terms 'for these purposes'.***

69 ***This change in wording will need to be discussed, but the Presidency has suggested this change in order to align the text to the suggested text in the Data Protection Directive for police and judicial cooperation.***

intermediary service providers in Articles 12 to 15 of that Directive.	service providers in ~~Articles 12~~ to 15 of that ~~Directive~~.		
Article 3	***Article 3***	***Article 3***	
Territorial scope	***Territorial scope***	***Territorial scope***	
	Amendment 97		
1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.	1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union***, whether the processing takes place in the Union or not***.	1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.	
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:	2. This Regulation applies to the processing of personal data of data subjects ~~residing~~ in the Union by a controller ***or processor*** not established in the Union, where the processing activities are related to:	2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:	
(a) the offering of goods or services to such data subjects in the Union; or	(a) the offering of goods or services***, irrespective of whether a payment of the data subject is required,*** to such data subjects in the Union; or	(a) the offering of goods or services***, irrespective of whether a payment of the data subject is required,*** to such data subjects in the Union; or	
(b) the monitoring of their behaviour.	(b) the monitoring of ~~their behaviour~~ ***such data subjects***.	(b) the monitoring of their behaviour ***as far as their behaviour***	

		takes place within the European Union[70].	
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.	3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.	3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.	
Article 4	***Article 4***	***Article 4***	
Definitions	***Definitions***	***Definitions***	
	Amendment 98		
For the purposes of this Regulation:	For the purposes of this Regulation:	For the purposes of this Regulation:	
(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors	***deleted***	(1) ***'personal data' means any information relating*** ~~'data subject' means~~ ***or identifiable natural person ('data subject'); an identifiable*** ~~an identified natural person or a natural~~ person who can be identified, directly or indirectly, ~~by means reasonably likely to be used by the controller or by any other natural or legal person,~~ in	

[70] ***UK reservation.***

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;		particular by reference to ***an identifier[71] such as a name,*** an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;	
(2) 'personal data' means any information relating to a data subject;	(2) 'personal data' means any information relating to ~~a~~ ***an identified or identifiable natural person (***'data subject'**)**; ***an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person;***	***deleted***	
	(2a) 'pseudonymous data' means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such		

[71] ***UK is concerned that, together with recital 24, this will lead to risk-averse approach that this is always personal data.***

	additional information is kept separately and subject to technical and organisational measures to ensure non-attribution;		
	(2b) 'encrypted data' means personal data, which through technological protection measures is rendered unintelligible to any person who is not authorised to access ~~it~~them;		
(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;	(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;	(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination~~,~~ or erasure ~~or destruction~~[72];	
	(3a) 'profiling' means any form of automated processing of personal		

[72] ***DE, FR and NL regretted that the blocking of data was not included in the list of data processing operations as this was a means especially useful in the public sector. COM indicated that the right to have the processing restricted in certain cases was provided for in Article 17(4) (restriction of data processing), even though the terminology 'blocking' was not used there. DE and FR thought the definition of Article 4(3) (erasure) should be linked to Article 17.***

	data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour;		
		(3a) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future[73];	
		(3b) 'pseudonymisation' means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person (…)[74].	

[73] ***RO scrutiny reservation.***

[74] ***DE, supported by UK, proposed reinserting the following reference 'or can be attributed to such person only with the investment of a disproportionate amount of time, expense and manpower'.***

(4) filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;	(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;	(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis[75];	
(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes~~, conditions~~ and means of the processing of personal data; where the purposes~~, conditions~~ and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes~~, conditions~~ and means of the processing of personal data; where the purposes~~,~~ ~~conditions~~ and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	
(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller[76];	

[75] ***DE, FR SI, SK and UK scrutiny reservation. DE and SI thought this was completely outdated concept. COM explained that the definition had been taken over from Directive 95/46/EC and is related to the technical neutrality of the Regulation, as expressed in Article 2(1).***

[76] ***DE, DK, FR, LU and NL requested the inclusion of a definition of third party.***

(7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;	(7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;	(7)'recipient' means a natural or legal person, public authority, agency or any other body ***other than the data subject, the data controller or the data processor*** to which the personal data are disclosed;[77] ***however regulatory bodies and authorities which may receive personal data in the exercise of their official functions shall not be regarded as recipients[78];***	
	(7a) 'third party' means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;		
(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of	(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of	(8) 'the data subject's consent' means any freely given specific~~,~~ ***and*** informed ~~and explicit~~[79]	

[77] ***PT reservation. DE, FR, LU, NL, SI and SE regretted the deletion from the 1995 Data Protection Directive of the reference to third party disclosure and pleaded in favour of its reinstatement. COM argued that this reference was superfluous and that its deletion did not make a substantial difference.***

[78] ***DE, ES, NL and UK scrutiny reservation on latter part of definition. ES, NL and UK thought it could be deleted.***

[79] ***COM, CY, FR, GR, HU, IT, PL and RO reservation on the deletion of 'explicit'.***

his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	
(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	(9) 'personal data breach' means ~~a breach of security leading to~~ the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed[80];	
(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;	(10) 'genetic data' means all ***personal*** data~~, of whatever type, concerning~~ ***relating to*** the ***genetic*** characteristics of an individual which ~~are~~ ***have been*** inherited or acquired ~~during early prenatal development~~ ***as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal,***	(10) 'genetic data' means all ***personal*** data~~, of whatever type, concerning~~ ***relating to the genetic*** characteristics of an individual ~~which are inherited or acquired during early prenatal development~~ ***that have been inherited or acquired, resulting from an analysis of a biological sample from the individual in question***[81];	

[80] ***COM, supported by LU, explained that it sought to have a similar rule as in the E-Privacy Directive, which should be extended to all types of data processing. DE scrutiny reservation questioned the very broad scope of the duty of notifying data breaches, which so far under German law was limited to sensitive cases. NL, LV and PT concurred with DE and thought this could lead to over-notification. In the meantime the scope of Articles 31 and 32 has been limited.***

[81] ***AT, CY, FR, IT, NL and SE scrutiny reservation. Several delegations (CH, CY, DE and SE) expressed their surprise regarding the breadth of this definition, which would also cover data about a person's physical appearance. DE thought the definition should differentiate between various types of genetic data. AT scrutiny reservation. The definition is now explained in the recital 25a.***

	desoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained;		
(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;	(11) 'biometric data' means any ***personal*** data relating to the physical, physiological or behavioural characteristics of an individual which allow ~~their~~ his or her unique identification, such as facial images, or dactyloscopic data;	(11) 'biometric data' means any ***personal*** data ***resulting from specific technical processing*** relating to the physical, physiological or behavioural characteristics of an individual which allow***s or confirms the***[82] ~~their~~ unique identification ***of that individual***, such as facial images, or dactyloscopic data[83];	
(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;	(12) 'data concerning health' means any ~~information~~ ***personal data*** which relate to the physical or mental health of an individual, or to the provision of health services to the individual;	(12) 'data concerning health' means ***data related*** ~~any information which relates~~ to the physical or mental health of an individual, ***which reaveal information about his or her health status***[84] ~~or to the provision of health services to the individual~~;	

[82] ***ES preferred 'allows'; SI suggested 'allows or confirms'***

[83] ***NL, SE and AT scrutiny reservation. SI did not understand why genetic data were not included in the definition of biometric data. FR queried the meaning of 'behavioural characteristics of an individual which allow their unique identification'. CH is of the opinion that the term 'biometric data' is too broadly defined.***

[84] ***CZ, DE, DK, EE, FR and SI expressed their surprise regarding the breadth of this definition. AT, BE, DE, NL and SI scrutiny reservation. COM scrutiny reservation.***

		(12a) 'profiling' means a form of automated processing of personal data intended to (…) use a profile to evaluate personal aspects relating to a natural person, in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements[85];	
		(12b) 'profile' means a set of data characterising a category of individuals that is intended to be applied to a natural person;	
(13) 'main establishment' means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main	(13) 'main establishment' means ~~as regards the controller,~~ the place of ~~its~~ establishment ***of the undertaking or group of undertakings*** in the Union***, whether controller or processor,*** where the main decisions as to the purposes~~, conditions~~ and means of the processing of personal data are taken~~.; if no decisions as to the~~	(13) 'main establishment' means[86] **-** as regards ~~the~~ ***a*** controller ***with establishments in more than one Member State***, the place of its ~~establishment~~ ***central administration*** in the Union ~~where~~ ***unless*** the ~~main~~ decisions ~~as to~~ ***on*** the purposes~~, conditions~~ and means of the processing of personal data	

[85] ***BE, RO and SE scrutiny reservation. BE, FR, LU, SI and RO would prefer reverting to the Council of Europe definition. COM reservation.***

[86] ***AT remarked that, in view technological developments, it was very difficult to pinpoint the place of processing and , supported by ES, HU, PL, expressed a preference for a formal criterion, which referred to the incorporation of the controller. AT pointed out that such criterion would avoid the situation that, depending on the processing activity concerned, there would be a different main establishment and consequently a different lead DPA.***

establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;	~~purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union~~ ***The following objective criteria may be considered among others: the location of the controller or processor's headquarters; the location of the entity within a group of undertakings which is best placed in terms of management functions and administrative responsibilities to deal with and enforce the rules as set out in this Regulation; the location where effective and real management activities are exercised determining the data processing through stable arrangements;***	are taken ***in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in this case the establishment having taken such decisions shall be considered as the main establishment***[87]***.*** ~~If no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place.~~ ~~-~~ ~~As~~ as regards ~~the~~ a processor ***with establishments in more than one Member State***, ~~'main establishment' means~~ the place of its central administration in the Union***, and, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context***	

[87] ***BE reservation.***

		of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation; ***- Where the controller exercises also activities as a processor, (…) the main establishment of the controller shall be considered as the main establishment for the supervision of processing activities;*** ***- Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking shall be considered as the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking;***	
(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other	(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, ~~acts and may be addressed by any supervisory authority and other~~	(14) 'representative' means any natural or legal person established in the Union who, ~~explicitly~~ designated by the controller ***in writing pursuant to Article 25, represents*** ~~acts and may be~~	

bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;	~~bodies in the Union instead of~~ ***represents*** the controller, with regard to the obligations of the controller under this Regulation;	~~addressed by any supervisory authority and other bodies in the Union instead of~~ the controller, with regard to the obligations of the controller under this Regulation;	
(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;	(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;	(15) 'enterprise' means any ***natural or legal person*** ~~entity~~ engaged in an economic activity, irrespective of its legal form, ~~thus~~ including~~, in particular, natural and legal persons,~~ partnerships or associations regularly engaged in an economic activity;	
(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;	(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;	(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings[88];	
(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or	(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or	(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or	

[88] ***DE scrutiny reservation. UK scrutiny reservation on all definitions in paragraphs 10 to 16.***

more third countries within a group of undertakings;	more third countries within a group of undertakings;	more third countries within a group of undertakings[89] ***or group of enterprises engaged in a joint economic activity***;	
(18) 'child' means any person below the age of 18 years;	(18) 'child' means any person below the age of 18 years;	***deleted***[90]	
(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46.	(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46.	(19) 'supervisory authority' means a***n independent*** public authority which is established by a Member State ~~in accordance with~~ ***pursuant to*** Article 46.	
		19a) 'concerned supervisory authority means - ***a supervisory authority which is concerned by the processing, because:*** ***a) the controller or processor is established on the territory of the Member State of that supervisory authority;*** ***b) data subjects residing in this***	

[89] ***DE queried whether BCRs could also cover intra-EU data transfers. COM indicated that there was no need for BCRs in the case of intra-EU transfers, but that controllers were free to apply BCRs also in those cases.***

[90] ***COM scrutiny reservation on the deletion of the definition of a child.***

		Member State are substantially[91] affected or likely to be substantially affected by the processing; or ***c) the underlying complaint has been lodged to that supervisory authority.*** ***(19b) "transnational processing of personal data" means either:*** ***a) processing which takes place in the context of the activities of establishments in more than one Member State of a controller or a processor in the Union and the controller or processor is established in more than one Member State; or*** ***b) processing which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect[92] data subjects in more than one***	

[91] *IE and UK would prefer the term 'materially'.*

[92] *Several Member States thought that this should be clarified in recital: CZ, FI, HU, SE.*

		Member State. ***(19c) "relevant and reasoned objection" means :*** ***an objection as to whether there is an infringement of this Regulation or not, or, as the case may be, whether the envisaged action in relation to the controller or processor is in conformity with the Regulation. The objection shall clearly demonstrate[93] the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects[94] and where applicable, the free flow of personal data.***	
		(20) 'Information Society service' means any service as defined by Article 1 (2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the	

[93] ***BE thought that this was a threshold too high.***

[94] ***IE thought that also risks to the controller should be covered.***

		provision of information in the field of technical standards and regulations and of rules on Information Society services[95] [96] [97]***.***	
		(21) 'international organisation' means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries[98]***;***	

[95] ***OJ L 204, 21.7.1998, p. 37–48.***

[96] ***UK suggests adding a definition of 'competent authority' corresponding to that of the future Data Protection Directive.***

[97] ***BE, DE, FR and RO suggest adding a definition of 'transfer' ('communication or availability of the data to one or several recipients'). RO suggests adding 'transfers of personal data to third countries or international organizations is a transmission of personal data object of processing or designated to be processed after transfer which ensure an adequate level of protection, whereas the adequacy of the level of protection afforded by a third country or international organization must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations'.***

[98] ***NL queried whether MOUs would also be covered by this definition; FI queried whether Interpol would be covered. CZ, DK, LV, SI, SE and UK pleaded in favour of its deletion.***

CHAPTER II PRINCIPLES	CHAPTER II PRINCIPLES	CHAPTER II PRINCIPLES	
Article 5	***Article 5***	***Article 5***	
Principles relating to personal data processing	***Principles relating to personal data processing***	***Principles relating to personal data processing***	
	Amendment 99		
Personal data must be:	1. Personal data ~~must~~***shall*** be:	Personal data must be:	
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;	(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ***(lawfulness, fairness and transparency)***;	(a) processed lawfully, fairly and in a transparent manner in relation to the data subject[99];	
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;	(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes ***(purpose limitation)***;	(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; ***further processing of personal data for archiving purposes in the public interest or scientific, statistical[100] or historical purposes***	

[99] ***DE proposed adding "and non-discriminatory" and "taking into account the benefit of data processing within a free, open and social society". This was viewed critically by several delegations (CZ, ES, IE, IT, PL).***

[100] ***FR thought Chapter III should contain specific rules for protecting personal data processed for statistical purposes; DE and PL thought statistical purposes should also be qualified by the public interest filter. DE, supported by SI, suggested adding: "if the data have initially been collected for these purposes".***

		shall in accordance with Article 83 not be considered incompatible with the initial purposes[101];	
(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;	(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data ***(data minimisation)***;	(c) adequate, relevant, and ***not excessive*** ~~limited to the minimum necessary~~ in relation to the purposes for which they are processed[102]; ~~they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;~~	
(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	(d) accurate and***, where necessary,*** kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***(accuracy).***	(d) accurate and***, where necessary,*** kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	
(e) kept in a form which permits identification of data subjects for no longer than is	(e) kept in a form which permits ***direct or indirect*** identification of data subjects for no longer than is	(e) kept in a form which permits identification of data subjects for no longer than is necessary for the	

[101] ***Referring to Article 6(2), DE and RO queried whether this phrase implied that a change of the purpose of processing was always lawful in case of scientific processing, also in the absence of consent by the data subject. BE queried whether the concept of compatible purposes was still a useful one. HU and ES scrutiny reservations on reference to Article 83. FR thought that health data could be processed only in the public interest or with the consent of the data subject.***

[102] ***COM reservation on the deletion of the data minimisation principle. AT, CY, DE, EE, FR, HU, IT, PL, FI and SI preferred to return to the initial COM wording, stating 'limited to the minimum necessary'. DE, supported by PL, also suggested adding: "they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data". DK and UK were opposed to any further amendments to this point.***

necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;	necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research ***or for archive*** purposes in accordance with the rules and conditions of ~~Article~~ Articles 83 ***and 83a*** and if a periodic review is carried out to assess the necessity to continue the storage, ***and if appropriate technical and organizational measures are put in place to limit access to the data only for these purposes (storage minimisation)***;	purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for ***archiving purposes in the public interest, or*** scientific, ~~historical,~~ statistical, ~~or scientific research~~ ***or historical*** purposes in accordance with ~~the rules and conditions of~~ Article 83 ~~and if a periodic review is carried out to assess the necessity to continue the storage~~***subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of data subject***[103]***;***	
	(ea) processed in a way that effectively allows the data subject to exercise his or her rights (effectiveness);		
	(eb) processed in a way that protects against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational		

[103] ***IE proposal so as to cover all the safeguards required under the Regulation, including those in Chapter IV.***

	measures (integrity);		
		(ee) processed in a manner that ensures appropriate security (…) of the personal data.	
(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.	(f) processed under the responsibility and liability of the controller, who shall ensure and ***be able to*** demonstrate ~~for each processing operation~~ the compliance with the provisions of this Regulation ***(accountability)***.	***deleted***[104]	
		2. The controller shall be responsible for compliance with paragraph 1[105]***.***	
Article 6	***Article 6***	***Article 6***	
Lawfulness of processing	***Lawfulness of processing***	***Lawfulness of processing***[106]	
	Amendment 100		
1. Processing of personal data shall be lawful only if and to the extent that at least one of the	1. Processing of personal data shall be lawful only if and to the extent that at least one of the following	1. Processing of personal data shall be lawful only if and to the extent that at least one of the following	

[104] ***AT wondered whether a principle of digital autonomy should be added here.***

[105] ***It was previously proposed to add 'also in case of personal data being processed on its behalf by a processor', but further to suggestion from LU and FR, this rule on liability may be dealt with in the context of Chapter VIII.***

[106] ***DE, AT, PT, SI, SE and SK scrutiny reservation.***

following applies:	applies:	applies:	
(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;	(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;	(a) the data subject has given ***unambiguous***[107] consent to the processing of their personal data for one or more specific purposes[108];	
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	
(d) processing is necessary in order to protect the vital interests of the data subject;	(d) processing is necessary in order to protect the vital interests of the data subject;	(d) processing is necessary in order to protect the vital interests of the data subject ***or of another person***;	
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	
(f) processing is necessary for	(f) processing is necessary for the	(f) processing is necessary for the	

[107] ***FR, PL and COM reservation in relation to the deletion of 'explicit' in the definition of 'consent'; UK thought that the addition of 'unambiguous' was unjustified.***

[108] ***RO scrutiny reservation.***

the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.	purposes of the legitimate interests pursued by ***the*** controller ***or***, ***in case of disclosure, by the third party to whom the data ~~is~~ are disclosed, and which meet the reasonable expectations of the data subject based on his or her relationship with the controller***, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data~~, in particular where the data subject is a child~~. This shall not apply to processing carried out by public authorities in the performance of their tasks.	purposes of the legitimate interests[109] pursued by ~~a~~ ***the*** controller ***or by a third party***[110], except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. ~~***[***This ***subparagraph*** shall not apply to processing carried out by public authorities in the performance ***exercise*** of their tasks***public duties]***~~[111] [112].	
2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.	2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.	2. Processing of personal data which is necessary for ***archiving*** ~~the~~ purposes ***in the public interest, or*** ~~of~~***for*** historical, statistical or scientific ~~research~~ ***purposes*** shall be lawful subject ***also*** to the conditions and safeguards referred	

[109] ***FR scrutiny reservation.***

[110] ***Reinstated at the request of BG, CZ, DE, ES, HU, IT, NL, SE, SK and UK. COM, IE, FR and PL reservation on this reinstatement.***

[111] ***Deleted at the request of BE, CZ, DK, IE, MT, SE, SI, SK, PT and UK. COM, AT, CY, DE, FI, FR, GR and IT wanted to maintain the last sentence. COM reservation against deletion of the last sentence, stressing that processing by public authorities in the exercise of their public duties should rely on the grounds in point c) and e).***

[112] ***DK and FR regretted there was no longer a reference to purposes set out in Article 9(2) and thought that the link between Article 6 and 9 needed to be clarified.***

		to in Article 83.	
3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:	3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:	3. The basis ~~of~~ for the processing referred to in points (c) and (e) of paragraph 1 must be ~~provided for~~established in ***accordance with***:	
(a) Union law, or	(a) Union law, or	(a) Union law, or	
(b) the law of the Member State to which the controller is subject.	(b) the law of the Member State to which the controller is subject.	(b) ***national*** ~~the~~ law of the Member State to which the controller is subject[113].	
		The purpose of the processing shall be determined in this legal basis or as regards the processing referred to in point (e) of paragraph 1, be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. ***This legal basis may contain specific provisions to adapt the application of rules of this***	

[113] ***It was pointed out that the text of Article 6 may have an adverse effect on the collection of personal data under administrative, criminal and civil law collections by third country public authorities, in that Article 6 provides that processing for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest may only take place to the extent established in accordance with Union or Member State law. Compliance with the administrative, regulatory, civil and criminal law requirements of a third country incumbent on controllers that engage in commercial or other regulated activities with respect to third countries, or voluntary reporting of violations of law to, or cooperation with, third country administrative, regulatory, civil and criminal law enforcement authorities appear not be allowed under the current draft of Article 6 . The Presidency thinks this point will have to be examined in the future, notably in the context of Chapter I.***

		Regulation, inter alia the general conditions governing the lawfulness of data processing by the controller, the type of data which are subject to the processing, the data subjects concerned; the entities to, and the purposes for which the data may be disclosed; the purpose limitation; storage periods and processing operations and processing procedures, including measures to ensure lawful and fair processing, including for other specific processing situations as provided for in Chapter IX.	
		3a. In order to ascertain whether a purpose of further processing is compatible with the one for which the data are initially collected, the controller shall take into account, unless the data subject has given consent [114], inter alia[115]:	
		(a) any link between the purposes for which the data have been collected and the purposes of	

[114] ***DK, IT and PT scrutiny reservation; IT deemed this irrelevant to compatibility test.***

[115] ***DK, FI, NL, RO, SI and SE stressed the list should not be exhaustive.***

		the intended further processing;	
		(b) the context in which the data have been collected;	
		(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9;	
		(d) the possible consequences of the intended further processing for data subjects;	
		(e) the existence of appropriate safeguards[116].	
The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.	The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued. ***Within the limits of this Regulation, the law of the Member State may provide details of the lawfulness of processing, particularly as regards data***	***deleted***	

[116] ***DE, SK and PL reservation: safeguards as such do not make further processing compatible. FR queried to which processing this criterion related: the initial or further processing. DE and UK pleaded for the deletion of paragraph 3a.***

	controllers, the purpose of processing and purpose limitation, the nature of the data and the data subjects, processing measures and procedures, recipients, and the duration of storage.		
4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.	***deleted***	4. Where the purpose of further processing is ~~not~~ ***in***compatible with the one for which the personal data have been collected ***by the same controller***, the **further** processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1[117] [118]. ~~This shall in particular apply to any change of terms and general conditions of a contract.~~ ***Further processing by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject***[119]***.***	

[117] ***ES, AT and PL reservation; DE, HU scrutiny reservation. FR suggested adding 'if the process concerns the data mentioned in Articles 8 and 9'.***

[118] ***HU, supported by CY, FR, AT and SK, thought that a duty for the data controller to inform the data subject of a change of legal basis should be added here. The Presidency refers to the changes proposed in ADD 1 to 17072/3/14 REV 3.***

[119] ***COM reservation; BE, AT, FI, HU, IT and PL scrutiny reservation: (some of) these delegations would have liked to delete this last sentence; DE wanted to limit the second sentence to private controllers.***

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.	***deleted***	***deleted***	
Article 7	***Article 7***	***Article 7***	
Conditions for consent	***Conditions for consent***	***Conditions for consent***	
	Amendment 101		
1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.	1. ***Where processing is based on consent,*** ~~The~~***the*** controller shall bear the burden of proof for the data subject's consent to the processing of ~~their~~ his or her personal data for specified purposes.	1. ***Where Article 6(1)(a) applies*** the controller shall ~~bear the burden of proof for the data subject's~~ ***be able to demonstrate that unambiguous***[120] consent ~~to the processing of their personal data for specified purposes~~ ***was given by the data subject***.	

[120] ***COM reservation related to the deletion of 'explicit' in the definition of consent.***

		1a. Where article 9(2)(a) applies, the controller shall be able to demonstrate that explicit consent was given by the data subject.	
2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.	2. If the data subject's consent is given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented ***clearly*** distinguishable in its appearance from this other matter. ***Provisions on the data subject's consent which are partly in violation of this Regulation are fully void.***	2. If the data subject's consent is to be given in the context of a written declaration which also concerns ~~an~~other matter<u>s</u>, the ~~requirement to give~~***request for*** consent must be presented ***in a manner which is clearly*** distinguishable ~~in its appearance~~ from th~~is~~<u>e</u> other matter<u>s</u>***, in an intelligible and easily accessible form, using clear and plain language***.	
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.	3. ***Notwithstanding other legal grounds for processing,*** ~~The~~ ***the*** data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. ***It shall be as easy to withdraw consent as to give it. The data subject shall be informed***	3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal***. Prior to giving consent, the data subject shall be informed thereof***[121]***.***	

[121] ***IE reservation. The Presidency concurs with SE that the last sentence belongs rather in Article 14. To that end the Presidency has made some suggestions set out in ADD 1 to 17072/3/14 REV 3.***

	by the controller if withdrawal of consent may result in the termination of the services provided or of the relationship with the controller.		
4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.	4. Consent shall ~~not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller~~ ***be purpose-limited and shall lose its validity when the purpose ceases to exist or as soon as the processing of personal data is no longer necessary for carrying out the purpose for which they were originally collected. The execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1), point (b)***.	***deleted***	
Article 8	***Article 8***	***Article 8***	
Processing of personal data of a child	~~***Processing of personal data of a child***~~	***Conditions applicable to child's consent in relation to***	

		information society services [122]	
	Amendment 102		
1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.	1. For the purposes of this Regulation, in relation to the offering of ~~information society~~ ***goods or*** services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or ~~custodian~~***legal guardian***. The controller shall make reasonable efforts to ~~obtain verifiable~~ ***verify such*** consent, taking into consideration available technology ***without causing otherwise unnecessary processing of personal data***.	1. ~~For the purposes of this Regulation~~***Where Article 6 (1)(a) applies***, in relation to the offering of information society services directly to a child[123], the processing of personal data of a child ~~below the age of 13 years~~[124] shall only be lawful if and to the extent that ***such*** consent is given or authorised by the ***holder of parental responsibility over the*** child~~'s parent~~ or ~~custodian~~***is given by the child in circumstances where it is treated as valid by Union or Member State law***.	
		(1a) The controller shall make reasonable efforts to ~~obtain verifiable~~ ***verify in such cases that***	

[122] ***CZ, DE, AT, SE, SI, PT and UK scrutiny reservation. CZ and SI would prefer to see this Article deleted. NO proposes including a general provision stating that personal data relating to children cannot be processed in an irresponsible manner contrary to the child's best interest. Such a provision would give the supervisory authorities a possibility to intervene if for example adults publish personal data about children on the Internet in a manner which may prove to be problematic for the child. DE, supported by NO, opined this article could have been integrated into Article 7***

[123] ***Several delegations (DE, HU, ES, FR, SE, SK, PT) disagreed with the restriction of the scope and thought the phrase 'in relation to the offering of information society services directly to a child' should be deleted.***

[124] ***COM reservation on the deletion of a harmonised age threshold.***

		consent ***is given or authorised by the holder of parental responsibility over the child***, taking into consideration available technology.	
	1a. Information provided to children, parents and legal guardians in order to express consent, including about the controller's collection and use of personal data, should be given in a clear language appropriate to the intended audience.		
2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.	2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.	2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child[125].	
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable	3. The ~~Commission~~ ***European Data Protection Board*** shall be ~~empowered to adopt delegated acts in accordance with Article 86 for the purpose~~ ***entrusted with the task*** of ~~further specifying the criteria and~~	3. ***[***The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable	

[125] ***DE, supported by SE, queried whether a Member State could adopt/maintain more stringent contract law. SI thought the reference should be worded more broadly to 'civil law', thus encompassing also personality rights.***

consent referred to in paragraph 1. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.	~~requirements~~ ***issuing guidelines, recommendations and best practices*** for the methods ~~to obtain verifiable~~ ***of verifying*** consent referred to in paragraph 1***, in accordance with Article 66***. ~~In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.~~	consent referred to in paragraph 1[126]]. ~~In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.~~	
4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	~~4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)]~~[127]~~.~~	
Article 9	***Article 9***	***Article 9***	
	Amendment 103		
Processing of special categories of personal data	~~**Processing of special**~~ ***Special categories of*** ~~**personal**~~ ***data***	***Processing of special categories of personal data***[128]	

[126] ***DE, ES, FR, SE and UK suggested deleting this paragraph. CZ suggested adding "and for identifying that a service is offered directly to a child". DE, supported by BE and FR, suggested giving the EDPB the power to issue guidelines in this regard.***

[127] ~~***LU reservation. ES, FR, SE and UK suggested deleting paragraphs 3 and 4.***~~

[128] ***COM, DK, SE and AT scrutiny reservation. SK thought the inclusion of biometric data should be considered.***

1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.	1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or ***philosophical*** beliefs, ***sexual orientation or gender identity,*** trade-union membership ***and activities***, and the processing of genetic ***or biometric*** data or data concerning health or sex life~~or~~***, administrative sanctions, judgments,*** criminal ***or suspected offences,*** convictions or related security measures shall be prohibited.	1. The processing of personal data, revealing ~~race~~ ***racial*** or ethnic origin, political opinions, religio~~n~~us or ***philosophical*** beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life ~~or criminal convictions or related security measures~~ shall be prohibited.	
2. Paragraph 1 shall not apply where:	2. Paragraph 1 shall not apply~~where~~ ***if one of the following applies:***	2. Paragraph 1 shall not apply ***if one of the following applies:***	
(a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or	(a) the data subject has given consent to the processing of those personal data ***for one or more specified purposes***, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or	(a) the data subject has given ***explicit*** consent to the processing of those personal data, ~~subject to the conditions laid down in Articles 7 and 8,~~ except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or	
	(aa) processing is necessary for the performance or execution of a		

	contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;		
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or	(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law ***or collective agreements*** providing for adequate safeguards ***for the fundamental rights and the interests of the data subject such as right to non-discrimination, subject to the conditions and safeguards referred to in Article 82***; or	(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller ***or of the data subject*** in the field of employment ***and social security and social protection*** law in so far as it is authorised by Union law or Member State law ***or a collective agreement pursuant to Member State law*** providing for adequate safeguards; or	
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or	(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or	(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or	
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-	(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a	(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a	

seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or	political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or	political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or	
(e) the processing relates to personal data which are manifestly made public by the data subject; or	(e) the processing relates to personal data which are manifestly made public by the data subject; or	(e) the processing relates to personal data which are manifestly made public by the data subject; or	
(f) processing is necessary for the establishment, exercise or defence of legal claims; or	(f) processing is necessary for the establishment, exercise or defence of legal claims; or	(f) processing is necessary for the establishment, exercise or defence of legal claims ***or whenever courts are acting in their judicial capacity***; or	
(g) processing is necessary for the performance of a task carried out in the public interest, on the basis of Union law, or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests;	(g) processing is necessary for the performance of a task carried out ~~in the~~ ***for reasons of high*** public interest, on the basis of Union law, or Member State law which shall ***be proportionate to the aim pursued, respect the essence of the right to data protection and*** provide for	(g) processing is necessary for ~~the performance of a task carried out in the~~[129] ***reasons of*** public interest, on the basis of Union law, or Member State law which shall provide for suitable ***and specific*** measures to safeguard the data subject's	

[129] ***AT, PL and COM reservation on deletion of 'important'; DK suggested adding 'in the public interest vested in the controller'.***

or	suitable measures to safeguard the ***fundamental rights and the*** ~~data subject's legitimate~~ interests ***of the data subject***; or	legitimate interests; or	
(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or	(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or	(h) processing[130] ~~of data concerning health~~ is necessary for ~~health purposes~~ ***the purposes of preventive or occupational medicine[131], for the assessment of the working capacity of the employee[132], medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or Member State law[133] or pursuant to contract with a health professional[134]*** and subject to the conditions and safeguards referred to in ~~Article 81~~***paragraph 4[135]***; or	

[130] ***HU suggested reinstating "of health data" here and in point (hb).***

[131] ***AT would like to see this deleted; BE pointed out this type of medicine practice is not (entirely) regulated by law under Belgian law and therefore the requirement of paragraph 4 is not met.***

[132] ***PL and AT would like to see this deleted.***

[133] ***COM, IE, PL scrutiny reservation.***

[134] ***FR and PL reservation.***

[135] ***AT, DE and ES scrutiny reservation. DE and ES queried what happened in cases where obtaining consent was not possible (e.g. in case of contagious diseases; persons who were physically or mentally not able to provide consent); NL thought this should be further clarified in recital 42. BE queried what happened in the case of processing of health data by insurance companies. COM explained that this was covered by Article 9(2) (a), but SI was not convinced thereof.***

		(ha) (…);	
		(hb) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union law or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject data; or	
(i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or	(i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or	(i) processing is necessary for ***archiving purposes in the public interest or*** historical, statistical or scientific ~~research~~ purposes ***and*** subject to the conditions and safeguards ***laid down in Union or Member State law, including those*** referred to in Article 83***.***	
	(ia) processing is necessary for archive services subject to the conditions and safeguards referred to in Article 83a; or		

(j) processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority.	(j) processing of data relating to ***administrative sanctions, judgments,*** criminal ***offences,*** convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards~~.~~ ~~A complete~~ ***for the fundamental rights and the interests of the data subject***. ***Any*** register of criminal convictions shall be kept only under the control of official authority.	***deleted***[136]	
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the	3. The ~~Commission~~ ***European Data Protection Board*** shall be ~~empowered to adopt delegated acts in accordance with Article 86 for the purpose~~***entrusted with the task*** of ~~further specifying the criteria,~~	***deleted***[137]	

[136] ***Deleted at the request of AT, COM, EE, ES, FR, HU, IT, LU, MT, PL, PT, RO and SK. DE and FI wanted to reintroduce the paragraph.***

[137] ***COM reservation on the deletion of paragraph 3 on delegated acts.***

processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2.	~~conditions and appropriate safeguards~~ ***issuing guidelines, recommendations and best practices*** for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2***, in accordance with Article 66***.		
		4. Personal data referred to in paragraph 1 may on the basis of Union or Member State law be processed for the purposes referred to in points (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Umion or Member State law or rules established by national competent bodies.	
		5. Member States may maintain or introduce more specific provisions with regard to genetic data or health data. This includes the	

		possibility for Member States to introduce further conditions for the processing of these data[138].	
		Article 9a	
		Processing of data relating to criminal convitions and offences[139]	
		Processing of data relating to criminal convictions and offences or related security measures based on Article 6(1) may only be carried out either under the control of official authority or when the processing is authorised by Union law or Member State law providing for adequate safeguards for the rights and freedoms of data subjects. A complete register of criminal convictions may be kept only under the control of official authority[140].	

138 ***COM scrutiny reservation.***

139 ***DE and HU would prefer to see these data treated as sensitive data in the sense of Article 9(1). EE and UK are strongly opposed thereto.***

140 ***SI, SK reservation on last sentence.***

Article 10	***Article 10***	***Article 10***	
Processing not allowing identification	***Processing not allowing identification***	***Processing not ~~allowing~~ requiring identification***	
	Amendment 104		
If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.	***1.*** If the data processed by a controller do not permit the controller ***or processor*** to ***directly or indirectly*** identify a natural person, ***or consist only of pseudonymous data,*** the controller shall not ~~be obliged to~~ ***process or*** acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.	If the ~~data processed by~~ ***purposes for which a*** controller ***processes personal data*** do not ~~permit~~ ***or do no longer require the identification of a data subject by*** the controller~~ to identify a natural person~~, the controller shall not be obliged to ***maintain or*** acquire additional information ***nor to engage in additional processing*** in order to identify the data subject for the sole purpose of complying with ~~any provision of~~ this Regulation[141].	
	2. Where the data controller is unable to comply with a provision of this Regulation because of paragraph 1, the controller shall not be obliged to comply with that particular provision of this Regulation. Where as a consequence the data controller is	***2. Where, in such cases the controller is not in a position to identify the data subject, articles 15, 16, 17, 17a, 17b and 18 do not apply except where the data subject, for the purpose of exercising his or her rights under these articles, provides additional***	

[141] ***AT, DE, HU, PL scrutiny reservation and UK and FR and COM reservation.***

	unable to comply with a request of the data subject, it shall inform the data subject accordingly.	***information enabling his or her identification[142].***	
	Article 10 a (new)		
	Amendment 105		
	General principles for the rights of the data subject ~~rights~~		
	1. The basis of data protection is clear and unambiguous rights for the data subject which shall be respected by the data controller. The provisions of this Regulation aim to strengthen, clarify, guarantee and where appropriate, codify these rights.		
	2. Such rights include, inter alia, the provision of clear and easily understandable information regarding the processing of the data subject's ~~his or her~~ personal data, the right of access, rectification and erasure of ~~their~~ his or her data, the right to obtain data, the right to object to		

[142] ***DK, RO, SE and SI scrutiny reservation; COM and FR reservation; FR wanted to add in the end of the paragraph "In any case, the data subject should only have to provide the minimum additional information necessary in order to be able to exercise his or her rights which can never be denied by the controller.***

	profiling, the right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as the right to compensation and damages resulting from an unlawful processing operation. Such rights shall in general be exercised free of charge. The data controller shall respond to requests from the data subject within a reasonable period of time.		

CHAPTER III RIGHTS OF THE DATA SUBJECT	CHAPTER III RIGHTS OF THE DATA SUBJECT	CHAPTER III RIGHTS OF THE DATA SUBJECT[143]	
SECTION 1 TRANSPARENCY AND MODALITIES	**SECTION 1 TRANSPARENCY AND MODALITIES**	**SECTION 1 TRANSPARENCY AND MODALITIES**	
Article 11	***Article 11***	***Article 11***	
Transparent information and communication	***Transparent information and communication***	***Transparent information and communication***	
	Amendment 106		
1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.	1. The controller shall have ***concise,*** transparent***, clear*** and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights	***deleted***	
2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form,	2.The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and	***deleted***	

[143] ***General scrutiny reservation by UK on the articles in this Chapter.***

using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.	plain language, ~~adapted to the data subject,~~ in particular for any information addressed specifically to a child.		
Article 12	***Article 12***	***Article 12***	
Procedures and mechanisms for exercising the rights of the data subject	***Procedures and mechanisms for exercising the rights of the data subject***	~~**Procedures and mechanisms**~~ **Transparent information, communication and modalities for exercising the rights of the data subject**[144]	
	Amendment 107		
1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be	1. ~~The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19.~~ Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically ***where***	1. The controller shall ~~establish procedures for providing the~~ ***take appropriate measured to providay any*** information referred to in Article 14 and ***14a*** ~~for the exercise of the rights of data subjects referred to in Article 13~~ and ***any communication under*** Articles 15 to 19 ***and 32 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language***[145]***. The information shall be provided in***	

144 ***DE, SE, SI and FI scrutiny reservation.***

145 ***COM reservation on deletion.***

made electronically.	***possible***.	***writing, or where appropriate, electronically or by other means.*** . ~~The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.~~	
		1a. The controller shall facilitate the exercise of data subject rights under Articles 15 to 19[146]***.***	
2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a	2. The controller shall inform the data subject without ***undue*** delay and, at the latest within ~~one month~~ ***40 calendar days*** of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a	2. The controller shall ***provide the*** inform***ation referred to in Articles 14a and 15 and information on action taken on a rquest under Articles 16 to 19 to*** the data subject without ***undue*** delay and, at the latest within one month of receipt of the request[147]~~;~~ ~~whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information~~.	

[146] ***SI and UK thought this paragraph should be deleted.***

[147] ***UK pleaded in favour of deleting the one-month period. BG and PT thought it more simple to revert to the requirement of 'without excessive delay' under the 1995 Data Protection Directive.***

reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.	reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing ***and, where possible, the controller may provide remote access to a secure system which would provide the data subject with direct access to ~~their~~ his or her personal data***. Where the data subject makes the request in electronic form, the information shall be provided in electronic form ***where possible***, unless otherwise requested by the data subject.	This period may be ~~prolonged~~ ***extended*** for a further ***two*** month***s when necessary, taking into account the complexity of the request and th enumber of the requests.***~~, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing.~~ Where ***the extended period applies,*** the data subject ~~makes the request in electronic form, the information~~ shall be ~~provided in electronic form, unless otherwise requested by the data subject~~***informed within one month of receipt of the request of the reasons for the delay***.	
3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.	3. If the controller ~~refuses to~~ ***does not*** take action at the request of the data subject, the controller shall inform the data subject of the reasons for the ~~refusal~~***inaction*** and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.	3. If the controller ~~refuses to~~***does not*** take action on the request of the data subject, the controller shall inform the data subject ***without delay and at the latest within one month of receipt of the request*** of the reasons for ~~the refusal~~***not taking action*** and on the ~~possibilities~~ ***possibility*** of	

		lodging a complaint to ~~the~~ ***a*** supervisory authority~~ and seeking a judicial remedy~~.	
4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.	4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a ***reasonable*** fee ***taking into account the administrative costs*** for providing the information or taking the action requested~~, or the controller may not take the action requested~~. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.	4. ~~The i~~***I***nformation ~~and the actions taken on requests referred to in paragraph 1~~***provided under Articles 14 and 14a and any communication under Articles 16 to 19 and 32*** shall be ***provided*** free of charge. Where requests ***from a data subject*** are[148] manifestly ***unfounded or*** excessive, in particular because of their repetitive character, the controller may ~~charge a fee for providing the information or taking the action requested, or the controller may not take the action requested~~***refuse to act on***[149] ***the request***. In that case, the controller shall bear the burden of ~~proving~~ ***demonstrating*** the manifestly ***unfounded or*** excessive character of the request[150].	
		4a. Without prejudice to Article 10, where the controller has	

148 ***PL thought the criterion of 'manifestly excessive' required further clarification, e.g. through an additional recital. COM reservation on deletion.***

149 ***NL scrutiny reservation: avoid that this gives the impression that public authority cannot refuse to consider request by citizen.***

150 ***IT scrutiny reservation.***

		reasonable doubts concerning the identity of the individual making the request referred to in Articles 15 to 19, the controller may request the provision of additional information necessary to confirm the identity of the data subject.	
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.	***deleted***	***deleted***	
6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	

Article 13	***Article 13***	***Article 13***	
	Amendment 108		
Rights in relation to recipients	***~~Rights in relation to recipients~~ Notification requirement in the event of rectification and erasure***	***Rights in relation to recipients***	
The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.	The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been ~~disclosed~~ ***transferred***, unless this proves impossible or involves a disproportionate effort. ***The controller shall inform the data subject about those recipients if the data subject requests this.***	***deleted***	
	Article 13 a (new)		
	Amendment 109		
	Standardised information policies		
	1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with the following particulars before providing information pursuant to Article 14:		

	(a) whether personal data are collected beyond the minimum necessary for each specific purpose of the processing;		
	(b) whether personal data are retained beyond the minimum necessary for each specific purpose of the processing;		
	(c) whether personal data are processed for purposes other than the purposes for which they were collected;		
	(d) whether personal data are disseminated to commercial third parties;		
	(e) whether personal data are sold or rented out;		
	(f) whether personal data are retained in encrypted form.		
	2. The particulars referred to in paragraph 1 shall be presented pursuant to Annex to this Regulation in an aligned tabular format, using text and symbols, in the following three columns:		

	(a) the first column depicts graphical forms symbolising those particulars;		
	(b) the second column contains essential information describing those particulars;		
	(c) the third column depicts graphical forms indicating whether a specific particular is met.		
	3. The information referred to in paragraphs 1 and 2 shall be presented in an easily visible and clearly legible way and shall appear in a language easily understood by the consumers of the Member States to whom the information is provided. Where the particulars are presented electronically, they shall be machine readable.		
	4. Additional particulars shall not be provided. Detailed explanations or further remarks regarding the particulars referred to in paragraph 1 may be provided together with the other information requirements pursuant to Article 14.		

	5. The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86 for the purpose of further specifying the particulars referred to in paragraph 1 and their presentation as referred to in paragraph 2 and in the Annex to this Regulation.		

SECTION 2	SECTION 2	SECTION 2	
INFORMATION AND ACCESS TO DATA	**INFORMATION AND ACCESS TO DATA**	**INFORMATION AND ACCESS TO DATA**	
Article 14	***Article 14***	***Article 14***	
Information to the data subject	***Information to the data subject***	***Information to be provided where the data are collected from the data subject***	
	Amendment 110		
1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:	1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information, ***after the particulars pursuant to Article 13a have been provided***:	1[151]. Where personal data relating to a data subject are collected ***from the data subject***, the controller shall***, at the time when personal data are obtained,*** provide the data subject with ~~at least~~ the following information:	
(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;	(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer**;**	(a) the identity and the contact details of the controller and, if any, of the controller's representative***; the controller may also include the contact details*** and of the data protection officer**,**	

[151] ***HU thought the legal basis of the processing should be included in the list.***

		if any;	
(b) the purposes of the processing for which the personal data are intended, ***including the contract terms and general conditions where the processing is based on point (b) of Article 6(1)*** and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);	(b) the purposes of the processing for which the personal data are intended, ***as well as information regarding the security of the processing of personal data,*** including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and ~~the legitimate interests pursued by the controller where the processing is based on~~ **,** ***where applicable, information on how they implement and meet the requirements of*** point (f) of Article 6(1);	(b) the purposes of the processing for which the personal data are intended~~, ***including the contract terms and general conditions where the processing is based on point (b) of Article 6(1)*** and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1)~~;	
		1a. In addition to the information referred to in paragraph 1, the controller shall[152] provide the data subject with such further information [153]necessary to ensure fair and transparent processing in respect of the data subject[154], having	

[152] ***DE, EE, and PL asked to insert "on request". DE, DK, NL and UK doubted whether the redraft would allow for a sufficient risk-based approach and warned against excessive administrative burdens/compliance costs. DK and UK in particular referred to the difficulty for controllers in assessing what is required under para. 1a in order to ensure fair and transparent processing. DE, EE and PL pleaded for making the obligation to provide this information contingent upon a request thereto as the controller might otherwise take a risk-averse approach and provide all the information under Article 14(1a), also in cases where not required. UK thought that many of the aspects set out in paragraph 1a of Article 14 (and paragraph 2 of Article 14a) could be left to guidance under Article 39.***

[153] ***CZ suggested adding the word 'obviously'.***

[154] ***FR scrutiny reservation.***

		regard to the specific circumstances and context in which the personal data are processed[155]:	
(c) the period for which the personal data will be stored;	(c) the period for which the personal data will be stored***, or if this is not possible, the criteria used to determine this period***;	***deleted***	
		(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller;	
		(~~f~~c) the recipients or categories of recipients of the personal data[156];	
		(~~g~~d) where applicable, that the controller intends to transfer ***personal data*** to a ***recipient in a*** third country or international organisation~~ and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission~~;	

[155] ***COM reservation on deletion of the words 'such as'.***

[156] ***AT and DE thought that this concept was too vague (does it e.g. encompass employees of the data controller?).***

(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;	(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject**,** ~~or~~ to object to the processing of such personal data***, or to obtain data***;	(~~d~~e) the existence of the right to request from the controller access to and rectification or erasure of the personal data ***or restriction of processing of personal data*** concerning the data subject ~~or~~ ***and*** to object to the processing of such personal data[157];	
(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;	(e) the right to lodge a complaint ~~to~~ with the supervisory authority and the contact details of the supervisory authority;	(e~~f~~) the right to lodge a complaint to ~~the~~ ***a*** supervisory authority ~~and the contact details of the supervisory authority~~;	
(f) the recipients or categories of recipients of the personal data;	(f) the recipients or categories of recipients of the personal data;	***moved under (c)***	
(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;	(g) where applicable, that the controller's intends to transfer ***the data*** to a third country or international organisation and ~~on the level of protection afforded by that third country or international organisation by reference to~~ ***the existence or absence of*** an adequacy decision by the Commission***, or in case of transfers referred to in Article 42~~, Article~~or 43~~, or point (h) of Article 44(1)~~, reference to the***	***moved under (d) modified***	

[157] ***The reference to direct marketing was deleted in view of comments by DK, FR, IT and SE.***

	appropriate safeguards and the means to obtain a copy of them;		
		(g) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as the possible consequences of failure to provide such data[158]; and	
	(ga) where applicable, information about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the data subject;		
	(gb) meaningful information about the logic involved in any automated processing;		
		(h) the existence of automated decision making including - profiling referred to in Article 20(1) and (3) and information concerning (…) the processing , as well as the significance and the envisaged consequences of	

158 ***CZ, DE, ES and NL reservation.***

		such processing for the data subject.[159]	
(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.	(h) any further information ***which is*** necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected ***or processed, in particular the existence of certain processing activities and operations for which a personal data impact assessment has indicated that there may be a high risk;***	***deleted***	
	(ha) where applicable, information whether personal data ~~was~~ were provided to public authorities during the last consecutive 12-month period.		
2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences	2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is ~~obligatory~~ ***mandatory*** or ~~voluntary~~***optional***, as well as the	***deleted***[160]	

[159] ***SE scrutiny reservation.***

[160] ***HU reservation on the deletion of this paragraph.***

of failure to provide such data.	possible consequences of failure to provide such data.		
	2a. In deciding on further information which is necessary to make the processing fair under point (h) of paragraph 1, controllers shall have regard to any relevant guidance under Article ~~38~~34.		
3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.	3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the ***specific*** personal data originate. ***If personal data originate from publicly available sources, a general indication may be given.***	***deleted***	
4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:	4. The controller shall ~~provide~~ the information referred to in paragraphs 1, 2 ~~and~~ 3:	***deleted***	
(a) at the time when the personal data are obtained from the data subject; or	(a) at the time when the personal data are obtained from the data subject ***or without undue delay where the above is not feasible***; or	***deleted***	
	(aa) ~~on~~ at the request ~~by~~ of a body, organization or association referred		

	to in Article 73;		
(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.	(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a ~~disclosure~~ ***transfer*** to another recipient is envisaged, and at the latest ~~when the data are first disclosed.~~***at the time of the first transfer, or, if the data are to be used for communication with the data subject concerned, at the latest at the time of the first communication to that data subject; or***	***deleted***	
	(ba) only on request where the data are processed by a small or micro enterprise which processes personal data only as an ancillary activity.		
5. Paragraphs 1 to 4 shall not apply, where:	5. Paragraphs 1 to 4 shall not apply, where:	5. Paragraphs 1 to 4***1a*** shall not apply~~,~~ where ***and insofar as the data subject already has the information.***	
(a) the data subject has already the information referred to in	(a) the data subject ~~has~~ already the information referred to in paragraphs	***merged with above 5.***	

paragraphs 1, 2 and 3; or	1, 2 and 3; or		
(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or	(b) the data ***are processed for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Articles 81 and 83,*** are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort ***and the controller has published the information for anyone to retrieve***; or	***deleted***	
(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or	(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law ***to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests, considering the risks represented by the processing and the nature of the personal data***; or	***deleted***	
(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance	(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of ~~others~~ ***other natural persons***, as defined in Union law or Member State law in	***deleted***	

with Article 21.	accordance with Article 21***;***		
	(da) the data are processed in the exercise of his profession by, or are entrusted or become known to, a person who is subject to an obligation of professional secrecy regulated by Union or Member State law or to a statutory obligation of secrecy, unless the data is collected directly from the data subject.		
6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.	6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's ***rights or*** legitimate interests.	***deleted***	
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the	***deleted***	***deleted***	

conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.			
8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	
		Article 14 a	
		Information to be provided where the data have not been obtained from the data subject[161]	
		1[162]***. Where personal data have not been obtained from the data subject, the controller shall***	

[161] ***DE, EE, ES, NL (§§1+2),AT, PT scrutiny reservation.***

[162] ***HU thought the legal basis of the processing should be included in the list.***

		provide the data subject with the following information:	
		(a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller may also include the contact details of the data protection officer, if any;	
		(b) the purposes of the processing for which the personal data are intended.	
		2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with such further information necessary to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances and context[163] in which the personal data are processed:	
		(a) the categories of personal data concerned;	
		(b) (…)	

[163] ***ES, IT and FR doubts on the addition of the words 'and context'.***

		(c) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller;	
		(d) the recipients or categories of recipients of the personal data;	
		(e) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject and to object to the processing of such personal data;	
		(f) the right to lodge a complaint to <u>a</u> supervisory authority;	
		(g) the origin of the personal data, unless the data originate from publicly accessible sources[164];	
		(h) the existence of automated decision making including profiling referred to in Article 20(1) and (3) and	

[164] ***COM and AT scrutiny reservation.***

		information concerning the processing, as well as the significance and the envisaged consequences of such processing for the data subject.[165]	
		3. The controller shall provide the information referred to in paragraphs 1 and 2[166]***:***	
		(a) within a reasonable period after obtaining the data, having regard to the specific circumstances in which the data are processed, or	
		(b) if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed.	
		4. Paragraphs 1 to 3 shall not apply where and insofar as:	
		(a) the data subject already has the information; or	
		(b) the provision of such information proves impossible or	

[165] ***PL asks for the deletion of the reference to 'logic'.***

[166] ***BE proposed to add: 'possibly through an easily accessible contact person where the data subject concerned can consult his data'. This is already covered by the modified recital 46.***

		would involve a disproportionate effort or is likely to render impossible or to seriously impair the achievement of the purposes of the processing[167]; in such cases the controller shall take appropriate measures to protect the data subject's legitimate interests[168]; or	
		(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests[169]; or	
		(d) where the data originate from publicly available sources[170]; or	
		(e) where the data must remain confidential in accordance with a legal provision in Union or Member State law or	

167 ***COM scrutiny reservation.***

168 ***Several delegations (DE, DK, FI, PL, SK, and LT) thought that in this Regulation (contrary to the 1995 Directive) the text should be specified so as to clarify both the concepts of 'appropriate measures' and of 'legitimate interests'. According to the Commission, this should be done through delegated acts under Article 15(7). DE warned that a dangerous situation might ensue if these delegated acts were not enacted in due time.***

169 ***UK thought the requirement of a legal obligation was enough and no further appropriate measures should be required.***

170 ***COM, IT and FR reservation on this exception. ES thought this concept required further clarification. DE and SE emphasised the importance of this exception.***

		because of the overriding legitimate interests of another person[171].	
		4. Paragraphs 1 to 3 shall not apply where and insofar as:	
		(a) the data subject already has the information; or	
		(b) the provision of such information proves impossible or would involve a disproportionate effort or is likely to render impossible or to seriously impair the achievement of the purposes of the processing[172]; in such cases the controller shall take appropriate measures to protect the data subject's legitimate interests[173]; or	
		(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which	

[171] ***COM and AT reservation on (d) and (e). UK referred to the existence of case law regarding privilege (confidentiality). BE thought the reference to the overriding interests of another person was too broad.***

[172] ***COM scrutiny reservation.***

[173] ***Several delegations (DE, DK, FI, PL, SK, and LT) thought that in this Regulation (contrary to the 1995 Directive) the text should be specified so as to clarify both the concepts of 'appropriate measures' and of 'legitimate interests'. According to the Commission, this should be done through delegated acts under Article 15(7). DE warned that a dangerous situation might ensue if these delegated acts were not enacted in due time.***

		provides appropriate measures to protect the data subject's legitimate interests[174]; or	
		(d) where the data originate from publicly available sources[175]; or	
		(e) where the data must remain confidential in accordance with a legal provision in Union or Member State law or because of the overriding legitimate interests of another person[176].	
Article 15	***Article 15***	***Article 15***	
	Amendment 111		
Right of access for the data subject	Right ~~of~~ ***to*** access ***and to obtain data*** for the data subject	***Right of access for the data subject[177]***	
1. The data subject shall have the right to obtain from the	1. ~~The~~***Subject to Article 12(4), the*** data subject shall have the right to	1. The data subject shall have the right to obtain from the controller	

[174] ***UK thought the requirement of a legal obligation was enough and no further appropriate measures should be required.***

[175] ***COM, IT and FR reservation on this exception. ES thought this concept required further clarification. DE and SE emphasised the importance of this exception.***

[176] ***COM and AT reservation on (d) and (e). UK referred to the existence of case law regarding privilege (confidentiality). BE thought the reference to the overriding interests of another person was too broad.***

[177] ***DE, FI and SE scrutiny reservation. DE, LU and UK expressed concerns on overlaps between Articles 14 and 15.***

controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:	obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed~~. Where such personal data are being processed,~~ ***and, in clear and plain language,*** ~~the controller shall provide~~ the following information:	at ***reasonable intervals and free of charge***[178] ~~any time, on request,~~ confirmation as to whether or not personal data ~~relating to the data subject~~ ***concerning him or her*** are being processed ***and*** ~~. W~~where such personal data are being processed~~, the controller shall provide~~***access to the data and*** the following information:	
(a) the purposes of the processing;	(a) the purposes of the processing ***for each category of personal data;***	(a) the purposes of the processing;	
(b) the categories of personal data concerned;	(b) the categories of personal data concerned;	***deleted***	
(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;	(c) the recipients ~~or categories of recipients~~ to whom the personal data are to be or have been disclosed, ~~in particular~~ ***including*** to recipients in third countries;	(c) the recipients or categories of recipients to whom the personal data ~~are to be or~~ have been ***or will be*** disclosed, in particular to recipients in third countries[179];	
(d) the period for which the personal data will be stored;	(d) the period for which the personal data will be stored***, or if this is not possible, the criteria used to determine this period***;	(d) ***where possible,*** the ***envisaged***[180] period for which the personal data will be stored;	

178 ***DE, ES, HU, IT and PL reservation on the possibility to charge a fee. DE, LV and SE thought that free access once a year should be guaranteed.***

179 ***UK reservation on the reference to recipients in third countries. IT thought the concept of recipient should be clarified, inter alia by clearly excluding employees of the controller.***

180 ***ES and UK proposed adding 'where possible'; FR reservation on 'where possible ' and 'envisaged'; FR emphasised the need of providing an exception to archives.***

(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;	(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;	(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;	
(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;	(f) the right to lodge a complaint ~~to~~ with the supervisory authority and the contact details of the supervisory authority;	(f) the right to lodge a complaint to ***a*** supervisory authority[181] [182]***;***	
(g) communication of the personal data undergoing processing and of any available information as to their source;	***deleted***	***(g) where*** ~~communication of~~ the personal data ~~undergoing processing and of~~ ***are not collected from the data subject,*** any available information as to their source[183]	
(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.	(h) the significance and envisaged consequences of such processing~~, at least in the case of measures referred to in Article 20.~~***;***	(h) ***in the case of automated decision making including profiling referred to in Article 20(1) and (3), knowledge of the logic involved***[184] ***in any automated data processing as well as*** the significance and envisaged consequences of such	

[181] ***DE thought it was too onerous to repeat this for every data subject and pointed to difficulties in ascertaining the competent DPA in its federal structure.***

[182] ***IT suggestion to delete subparagraphs (e) and (f) as under Article 14 this information should already be communicated to the data subject at the moment of the collection of the data.***

[183] ***SK scrutiny reservation: subparagraph (g) should be clarified.***

[184] PL reservation on the reference to 'logic': the underlying algorithm should not be disclosed. DE reservation on reference to decisions.

		processing~~, at least in the case of measures referred to in Article 20~~[185].	
	(ha) meaningful information about the logic involved in any automated processing;		
	(hb) without prejudice to Article 21, in the event of disclosure of personal data to a public authority as a result of a public authority request, confirmation of the fact that such a request has been made.		
		1a. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 42 relating to the transfer[186].	
		1b. On request and without an excessive charge, the controller shall provide a copy of the personal data undergoing processing to the data subject.	

[185] ***NL scrutiny reservation. CZ and FR likewise harboured doubts on its exact scope.***

[186] ***FR and UK scrutiny reservation on links with Chapter V***

2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.	2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in ***an*** electronic ~~form~~ ***and structured format***, unless otherwise requested by the data subject. ***Without prejudice to Article 10, the controller shall take all reasonable steps to verify that the person requesting access to the data is the data subject.***	***2. Where personal data supplied by the data subject are processed by automated means and in a structured and commonly used format, the controller shall, on request and without an excessive charge, provide a copy of the data concerning the data subject in that format to the data subject[187].***	
	2a. Where the data subject has provided the personal data where the personal data are processed by electronic means, the data subject shall have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal	***2a. The right to obtain a copy referred to in paragraphs 1b and 2 shall not apply where such copy cannot be provided without disclosing personal data of other data subjects [188]***	

[187] ***COM, ES and FR reservation: they thought this was too narrowly drafted. DE, supported by UK, referred to the danger that data pertaining to a third party might be contained in such electronic copy. DE scrutiny reservation on relation to paragraph 1.***

[188] ***DE, supported by UK, referred to the danger that data pertaining to a third party might be contained in such electronic copy.***

	data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject.		
	2b. This Article shall be without prejudice to the obligation to delete data when no longer necessary under point (e) of Article 5(1).		
	2c. There shall be no right of access in accordance with paragraphs 1 and 2 when data within the meaning of point (da) of Article 14(5) are concerned, except if the data subject is empowered to lift the secrecy in question and acts accordingly.		
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.	***deleted***	***deleted***	
4. The Commission may specify standard forms and	***deleted***	***deleted***	

procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).			

SECTION 3 RECTIFICATION AND ERASURE	SECTION 3 RECTIFICATION AND ERASURE	SECTION 3 RECTIFICATION AND ERASURE	
Article 16	***Article 16***	***Article 16***	
Right to rectification	***Right to rectification***	***Right to rectification***	
The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.	The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.	The data subject shall have the right[189] to obtain from the controller the rectification of personal data ~~relating to them~~ ***concerning him or her*** which are inaccurate. ***Having regard the purposes for which data were processed,*** ~~The~~ the data subject shall have the right to obtain completion of incomplete personal data, including by ~~way~~ ***means*** of ~~supplementing~~ ***providing*** a ~~corrective~~ ***supplementary*** statement.	

[189] ***UK suggested to insert the qualification ' where reasonably practicable' UK also suggested inserting the qualification 'where necessary'.***

Article 17	*Article 17*	*Article 17*	
	Amendment 112		
Right to be forgotten and to erasure	***Right to ~~be forgotten and to~~ erasure***	***Right to be forgotten and to erasure***[190]	
1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:	1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to him or her and the abstention from further dissemination of such data, ~~especially in relation to personal data which are made available by the data subject while he or she was a child,~~ ***and to obtain from third parties the erasure of any links to, or copy or replication of, those data*** where one	1. The ~~data subject shall have the right to obtain from the~~ controller ***shall have the obligation to erase*** ~~the erasure of~~ personal data ~~relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by~~ ***without undue delay and*** the data subject ~~while he or she was a child,~~ ***shall have the***	

[190] ***DE, EE, PT, SE, SI, FI and UK scrutiny reservation. EE, FR, NL, RO and SE reservation on the applicability to the public sector. Whereas some Member States have welcomed the proposal to introduce a right to be forgotten (AT, EE, FR, IE); other delegations were more sceptical as to the feasibility of introducing a right which would go beyond the right to obtain from the controller the erasure of one's own personal data (DE, DK, ES). The difficulties flowing from the household exception (UK), to apply such right to personal data posted on social media were highlighted (BE, DE, FR), but also the impossibility to apply such right to 'paper/offline' data was stressed (EE, LU, SI). Some delegations (DE, ES) also pointed to the possible externalities of such right when applied with fraudulent intent (e.g. when applying it to the financial sector). Several delegations referred to the challenge to make data subjects active in an online environment behave responsibly (DE, LU and UK) and queried whether the creation of such a right would not be counterproductive to the realisation of this challenge, by creating unreasonable expectations as to the possibilities of erasing data (DK, LU and UK). Some delegations thought that the right to be forgotten was rather an element of the right to privacy than part of data protection and should be balanced against the right to remember and access to information sources as part of the freedom of expression (DE, ES, LU, NL, SI, PT and UK). It was pointed out that the possibility for Member States to restrict the right to be forgotten under Article 21 where it interferes with the freedom of expression is not sufficient to allay all concerns in that regard as it would be difficult for controllers to make complex determinations about the balance with the freedom of expression, especially in view of the stiff sanctions provided in Article 79 (UK). In general several delegations (CZ, DE, FR) stressed the need for further examining the relationship between the right to be forgotten and other data protection rights. The Commission emphasised that its proposal was in no way meant to be a limitation of the freedom of expression. The inherent problems in enforcing such right in a globalised world outside the EU were cited as well as the possible consequences for the competitive position of EU companies linked thereto (BE, AT, LV, LU, NL, SE and SI).***

	of the following grounds applies:	***right to obtain the erasure of personal data without undue delay*** where one of the following grounds applies:	
(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;	(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;	(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or ***point (a) of Article 9(2) and*** ~~when the storage period consented to has expired, and where~~ there is no other legal ground for the processing of the data;	
(c) the data subject objects to the processing of personal data pursuant to Article 19;	(c) the data subject objects to the processing of personal data pursuant to Article 19;	(c) the data subject objects to the processing of personal data pursuant to Article 19***(1) and there are no overriding legitimate grounds for the processing or the data subject objects to the processing of personal data pursuant to Article 19(2)*** ;	
	(ca) a court or regulatory authority based in the Union has ruled as final and absolute that the data		

	concerned must be erased;		
(d) the processing of the data does not comply with this Regulation for other reasons.	(d) the ~~processing of the~~ data ~~does not comply with this Regulation for other reasons~~ ***~~has~~ have been unlawfully processed***.	***(d) the*** ~~processing of the~~ ***data*** ~~does not comply with this Regulation for other reasons~~ ***have been unlawfully processed[191];***	
		(e) the data have to be erased for compliance with a legal obligation to which the controller is subject[192] [193].	
	1a. The application of paragraph 1 shall be dependent upon the ability of the controller to verify that the person requesting the erasure is the data subject.		
2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to	2. Where the controller referred to in paragraph 1 has made the personal data public ***without a justification based on Article 6(1)***, it shall take all reasonable steps~~, including technical~~	***deleted***	

191 ***UK scrutiny reservation: this was overly broad.***

192 ***RO scrutiny reservation.***

193 ***DE pointed to the difficulties in determining who is the controller in respect of data who are copied/made available by other controllers (e.g. a search engine) than the initial controller (e.g. a newspaper). AT opined that the exercise of the right to be forgotten would have take place in a gradual approach, first against the initial controller and subsequently against the 'secondary' controllers. ES referred to the problem of initial controllers that have disappeared and thought that in such cases the right to be forgotten could immediately be exercised against the 'secondary controllers' ES suggested adding in paragraph 2: 'Where the controller who permitted access to the personal data has disappeared, ceased to exist or cannot be contacted by the data subject for other reasons, the data subject shall have the right to have other data controllers delete any link to copies or replications thereof'. The Commission, however, replied that the right to be forgotten could not be exercised against journals exercising freedom of expression. According to the Commission, the indexation of personal data by search engines is a processing activity not protected by the freedom of expression.***

data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.	~~measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication~~ ***to have the data erased, including by third parties, without prejudice to Article 77. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties.***		
		2a. Where the controller[194] has made the personal data public[195] and is obliged pursuant to paragraph 1 to erase the data, the controller, taking account of	

[194] ***BE, DE and SI queried whether this also covered controllers (e.g. a search engine) other than the initial controller (e.g. a newspaper).***

[195] ***ES prefers referring to 'expressly or tacitly allowing third parties access to'. IE thought it would be more realistic to oblige controllers to erase personal data which are under their control, or reasonably accessible to them in the ordinary course of business, i.e. within the control of those with whom they have contractual and business relations. BE, supported by IE and LU, also remarked that the E-Commerce Directive should be taken into account (e.g. through a reference in a recital) and asked whether this proposed liability did not violate the exemption for information society services provided in that Directive (Article 12 of Directive 2000/31/EC of 8 June 2000), but COM replied there was no contradiction. LU pointed to a risk of obliging controllers in an online context to monitor all data traffic, which would be contrary to the principle of data minimization and in breach with the prohibition in Article 15 of the E-Commerce Directive to monitor transmitted information.***

		available technology and the cost of implementation[196], shall take reasonable steps[197], including technical measures, to inform controllers[198] which are processing the data, that a data subject requests them to erase any links to, or copy or replication of that personal data[199].	
3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:	3. The controller ***and, where applicable, the third party*** shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:	3. ~~The controller shall carry out the erasure without delay, except~~ ***Paragraphs 1 and 2a shall not apply[200]*** to the extent that ~~the retention~~ ***processing*** of the personal data is necessary:	

196 ***Further to NL suggestion. This may hopefully also accommodate the DE concern that the reference to available technology could be read as implying an obligation to always use the latest technology;***

197 ***LU queried why the reference to all reasonable steps had not been inserted in paragraph 1 as well and SE, supported by DK, suggested clarifying it in a recital. COM replied that paragraph 1 expressed a results obligation whereas paragraph 2 was only an obligation to use one's best efforts. ES thought the term should rather be 'proportionate steps'. DE, ES and BG questioned the scope of this term. ES queried whether there was a duty on controllers to act proactively with a view to possible exercise of the right to be forgotten. DE warned against the 'chilling effect' such obligation might have on the exercise of the freedom of expression.***

198 ***BE, supported by ES and FR, suggested referring to 'known' controllers (or third parties).***

199 ***BE and ES queried whether this was also possible for the offline world and BE suggested to clearly distinguish the obligations of controllers between the online and offline world. Several Member States (CZ, DE, LU, NL, PL, PT, SE and SI) had doubts on the enforceability of this rule.***

200 ***DE queried whether these exceptions also applied to the abstention from further dissemination of personal data. AT and DE pointed out that Article 6 contained an absolute obligation to erase data in the cases listed in that article and considered that it was therefore illogical to provide for exception in this paragraph.***

(a) for exercising the right of freedom of expression in accordance with Article 80;	(a) for exercising the right of freedom of expression in accordance with Article 80;	(a) for exercising the right of freedom of expression in accordance with Article 80[201];	
		(b) for compliance with a legal obligation to process the personal data by Union or Member State law to which the controller is subject[202]or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[203];	
(b) for reasons of public interest in the area of public health in accordance with Article 81;	(b) for reasons of public interest in the area of public health in accordance with Article 81;	(~~b~~c) for reasons of public interest in the area of public health in accordance with Article 81[204];	
(c) for historical, statistical and scientific research purposes in accordance with Article 83;	(c) for historical, statistical and scientific research purposes in accordance with Article 83;	(~~c~~d) for ***archiving purposes in the public interest or for*** historical, statistical and scientific ~~research~~ purposes in accordance with Article 83;	

201 ***DE and EE asked why this exception had not been extended to individuals using their own freedom of expression (e.g. an individual blogger).***

202 ***In general DE thought it was a strange legal construct to lay down exceptions to EU obligations by reference to national law. DK and SI were also critical in this regard. UK thought there should be an exception for creditworthiness and credit scoring, which is needed to facilitate responsible lending, as well as for judicial proceedings. IT suggested inserting a reference to Article 21 (1).***

203 ***AT scrutiny reservation.***

204 ***DK queried whether this exception implied that a doctor could refuse to erase a patient's personal data notwithstanding an explicit request to that end from the latter. ES and DE indicated that this related to the more general question of how to resolve differences of view between the data subject and the data controller, especially in cases where the interests of third parties were at stake. PL asked what was the relation to Article 21.***

(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;	(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the right to the protection of personal data and be proportionate to the legitimate aim pursued;	***deleted***	
(e) in the cases referred to in paragraph 4.	(e) in the cases referred to in paragraph 4.	***deleted***	
		(g) for the establishment, exercise or defence of legal claims.	
4. Instead of erasure, the controller shall restrict processing of personal data where:	4. Instead of erasure, the controller shall restrict processing of personal data ***in such a way that it is not subject to the normal data access and processing operations and ~~can not~~cannot be changed anymore,*** where:	***deleted***	
(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;	(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;	***deleted***	
(b) the controller no longer	(b) the controller no longer needs the	***deleted***	

needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;	personal data for the accomplishment of its task but they have to be maintained for purposes of proof;		
(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;	(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;	***deleted***	
	(ca) a court or regulatory authority based in the Union has ruled as final and absolute than the processing that the data concerned must be restricted;		
(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).	(d) the data subject requests to transmit the personal data into another automated processing system in accordance with ***paragraphs 2a of*** Article ~~18(2).~~***15;***	***deleted***	
	(da) the particular type of storage technology does not allow for erasure and has been installed before the entry into force of this Regulation.		
5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or	5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data	***deleted***	

with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.	subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.		
6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.	6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.	***deleted***	
7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.	***deleted***	***deleted***	
8. Where the erasure is carried out, the controller shall not otherwise process such personal data.	8. Where the erasure is carried out, the controller shall not otherwise process such personal data.	***deleted***	
	8a. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.		
9. The Commission shall be empowered to adopt delegated acts	9. The Commission shall be empowered to adopt***, after***	***deleted***	

in accordance with Article 86 for the purpose of further specifying:	***requesting an opinion of the European Data Protection Board,*** delegated acts in accordance with Article 86 for the purpose of further specifying:		
(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;	(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;	***deleted***	
(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;	(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;	***deleted***	
(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.	(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.	***deleted***	
		Article 17a	
		Right to restriction of processing	
		1. The data subject shall have the right to obtain from the controller the restriction of the processing of personal data where:	

		(a) the accuracy of the data is contested by the data subject, for a period enabling the controller to verify the accuracy of the data[205];	
		(b) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or	
		(c) he or she has objected to processing pursuant to Article 19(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.	
		2. deleted	
		3. Where processing of personal data has been restricted under paragraph 1, such data may, with the exception of storage, only be processed with the data subject's consent or for	

[205] ***FR scrutiny reservation: FR thought the cases in which this could apply, should be specified.***

		the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest[206].	
		4. A data subject who obtained the restriction of processing pursuant to paragraph 1 (…) shall be informed by the controller before the restriction of processing is lifted[207].	
		Article 17b	
		Notification obligation regarding rectification, erasure or restriction[208]	
		The controller shall communicate any rectification, erasure or restriction of	

206 ***DE , ES and SI asked who was to define the concept of public interest. DE reservation.***

207 ***DE, PT, SI and IT thought that this paragraph should be a general obligation regarding processing, not limited to the exercise of the right to be forgotten. DK likewise thought the first sentence should be moved to Article 22.***

208 ***Whilst several delegations agreed with this proposed draft and were of the opinion that it added nothing new to the existing obligations under the 1995 Directive, some delegations (DE, PL, SK and NL) pointed to the possibly far-reaching impact in view of the data multiplication since 1995, which made it necessary to clearly specify the exact obligations flowing from this proposed article. Thus, DE was opposed to a general obligation to log all the disclosures to recipients. DE also pointed out that the obligation should exclude cases where legitimate interests of the data subject would be harmed by a further communication to the recipients, that is not the case if the recipient would for the first time learn negative information about the data subject in which he has no justified interest. BE and ES asked that the concept of a 'disproportionate effort' be clarified in a recital.***

		processing carried out in accordance with Articles 16, 17(1) and 17a to each recipient[209] to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.	
Article 18	***Article 18***	***Article 18***	
	Amendment 113		
Right to data portability	***Right to data portability***	***Right to data portability[210]***	
1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format	***deleted***	***deleted***	

209 ***BE, supported by ES and FR, suggested referring to 'known' recipients.***

210 ***UK reservation: while it supports the concept of data portability in principle, the UK considers it not within scope of data protection, but in consumer or competition law. Several other delegations (DK, DE, FR, IE, NL, PL and SE) also wondered whether this was not rather a rule of competition law and/or intellectual property law or how it related to these fields of law. Therefore the UK thinks this article should be deleted. NL and CZ thought its scope should be limited to social media. DE, DK and UK pointed to the risks for the competitive positions of companies if they were to be obliged to apply this rule unqualifiedly and referred to/raises serious issues about intellectual property and commercial confidentiality for all controllers. DE, FI, SE and UK also underscored the considerable administrative burdens this article would imply. DE and FR referred to services, such as health services where the exercise of the right to data portability might endanger on-going research or the continuity of the service. Reference was also made to an increased risk of fraud as it may be used to fraudulently obtain the data of innocent data subjects (UK). DE, ES, FR, HU, IE and PL were in principle supportive of this right. SK thought that the article was unenforceable and DE referred to the difficulty/impossibility to apply this right in 'multi-data subject' cases where a single 'copy' would contain data from several data subjects, who might not necessarily agree or even be known or could not be contacted. BE, CZ and RO thought that the exclusion of the public sector should be mentioned not only in recital 55, but also here (ES was opposed thereto).***

which is commonly used and allows for further use by the data subject.			
2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.	***deleted***	2. ~~Where t~~The data subject ~~has provided~~ ***shall have the right to transmit*** the personal data[211] **concerning him or her which he or she has provided to a controller** ~~and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, in~~to another ~~one, in an electronic format which is~~ ***controller in a*** commonly used[212] ***and***[213] ***machine-readable format***~~,~~ without hindrance from the controller~~ from whom the personal data are withdrawn~~ ***to which the data have been provided to, where***.	

[211] ***PL suggested to specify that this pertained to personal data in their non-aggregated or non-modified form. DE also queried about the scope of this right, in particular whether it could extend to data generated by the controller or data posted by third persons.***

[212] ***DE and FI queried whether this meant the scope was restricted to currently used formats (excluding future developments) and whether it implied an obligation for controllers to use one of these commonly used formats.***

[213] ***PT thought 'and' should be deleted.***

		(a) the processing is based on consent or on a contract pursuant to points (a) and	
		(b) of Article 6 (2) or point (a) of Article 9 (2); and	
		(b) the processing is carried out by automated means[214].	
		2a. The exercise of this right shall be without prejudice to Article 17.	
		2aa. The right referred to in paragraph 2 shall be without prejudice to intellectual property rights in relation to the processing of the those personal data[215].	
3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be	***deleted***	**2.** The Commission may specify ~~the electronic format referred to in paragraph 1 and~~ the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those	

[214] ***BE, DE, ES, IE, FI and FR these delegations thought emphasis should be put on the right to withdraw data, also with a view to creating an added value as compared to the right to obtain a copy of personal data. VY and HU also thought the obligation of the controller should be emphasised.***

[215] ***ES thought there should be an exception in case disproportionate efforts would be required.***

adopted in accordance with the examination procedure referred to in Article 87(2).		implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)[216].	

[216] ***FR, HU, SE and UK reservation: this would better set out in the Regulation itself.***

SECTION 4 **RIGHT TO OBJECT AND PROFILING**	**SECTION 4** **RIGHT TO OBJECT AND PROFILING**	**SECTION 4** **RIGHT TO OBJECT AND PROFILING**	
Article 19	***Article 19***	***Article 19***	
Right to object	***Right to object***	***Right to object***[217]	
	Amendment 114		
1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.	1. The data subject shall have the right to object~~, on grounds relating to their particular situation,~~ at any time to the processing of personal data which is based on points (d)~~,~~ ***and*** (e) ~~and (f)~~ of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject**.**	1. The data subject shall have the right to object, on ***reasoned***[218] grounds relating to ~~their~~ ***his or her*** particular situation, at any time to the processing of personal data ***concerning him or her*** which is based on points ~~(d), (e) and~~ (f) of Article 6(1) [219]***; the personal data shall no longer be processed***~~,~~ unless the controller demonstrates ~~compelling~~ legitimate grounds for the processing which override the	

[217] ***DE, ES, EE, AT, SI, SK and UK scrutiny reservation.***

[218] **COM reservation.**

[219] **The reference to point (e) of Article 6(1) was deleted in view of the objections by BE, CZ, DE, DK, FR and HU. COM reservation on deletion. UK, supported by DE, queried whether the right to object would still apply in a case where different grounds for processing applied simultaneously, some of which are not listed in Article 6. ES and LU queried why Article 6(1) (c) was not listed here.**

		interests or ~~fundamental~~ rights and freedoms of the data subject[220].	
		1a. Where an objection is upheld pursuant to paragraph 1, the controller shall no longer[221] process the personal data concerned except for the establishment, exercise or defence of legal claims[222].	
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other	2. Where ***the processing of*** personal data ~~are processed for direct marketing purposes~~ ***is based on point (f) of Article 6(1)***, the data subject shall have, ***at any time and without any further justification,*** the right to object free of charge ***in general or for any particular purpose*** to the processing of his or her personal data ~~for such marketing~~.	2. Where personal data are processed for direct marketing[223] purposes, the data subject shall have the right to object ~~free of charge~~ ***at any time*** to the processing of ~~their~~ personal data ***concerning him or her*** for such marketing. This right shall be explicitly ~~offered to~~ ***brought to the attention of*** the data subject ~~in~~	

[220] ***SE scrutiny reservation: SE and NL queried the need to put the burden of proof on the controller regarding the existence of compelling legitimate grounds. DE and FI queried the need for new criteria, other than those from the 1995 Directive. COM stressed that the link with the 'particular situation' was made in order to avoid whimsical objections. CZ also stated that this risked making processing of data an exceptional situation due to the heavy burden of proof. NL and SE queried whether the right would also allow objecting to any processing by third parties.***

[221] ***ES proposed to reformulate the last part of this paragraph as follows: 'shall inform the data subject of the compelling legitimate reasons applicable as referred to in paragraph 1 above, or otherwise shall no longer use or otherwise process the personal data concerned'.***

[222] ***UK proposed adding ' for demonstrating compliance with the obligations imposed under this instrument'. This might also cover the concern raised by DE that a controller should still be able to process data for the execution of a contract if the data were obtained further to a contractual legal basis. CZ, DK, EE, IT, SE and UK have likewise emphasised the need for allowing to demonstrate compliance. CZ and SK also referred to the possibility of further processing on other grounds.***

[223] **FR and UK under lined the need to have clarity regarding the exact content of this concept, possibly through a definition of direct marketing. DE asked which cases were covered exactly.**

information.	~~This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.~~	~~an intelligible manner~~ and shall be ~~clearly distinguishable~~ ***presented clearly and separately*** from ***any*** other information[224].	
	2a. The right referred to in paragraph 2 shall be explicitly offered to the data subject in an intelligible manner and form, using clear and plain language, in particular if addressed specifically to a child, and shall be clearly distinguishable from other information.	***2a. Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.***	
	2b. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the right to object may be exercised by automated means using a technical standard which allows the data subject to clearly express his or her wishes.		

[224] ***At the request of several delegations (FR, LT, PT), COM confirmed that this paragraph was not meant to create an opt-in system and that the E-Privacy Directive would remain unaffected. DE feels there is a need to clarify the relationship between Article 19(2) on the one hand and Article 6(1)(f) and Article 6(4) on the other. It can be concluded from the right to object that direct marketing without consent is possible on the basis of a weighing of interests. On the other hand, Article 6(1)(f) no longer refers to the interests of third parties and Article 6(4) also no longer refers to Article 6(1)(f) in regard to data processing which changes the original purpose. DE is therefore of the opinion that this also needs to be clarified in view of online advertising and Directive 2002/58/EC and Article 89 of the Proposal for a Regulation.***

3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.	3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned ***for the purposes determined in the objection***.	***deleted***	
Article 20	***Article 20***	***Article 20***	
	Amendment 115		
Measures based on profiling	~~***Measures based on profiling***~~***Profiling***	~~***Measures based on p***~~***P***~~***rofiling***~~	
1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.	1. ***Without prejudice to the provisions in Article 6,*** ~~Every~~ ***every*** natural person shall have the right ***to object*** ~~not~~ to ~~be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour~~ ***profiling in***	1. ~~Every natural person~~ ***The data subject*** shall have the right not to be subject to a ~~measure which produces legal effects concerning this natural person or significantly affects this natural person, and which~~ ***decision evaluating personal aspects relating to him or her, which*** is based solely on automated processing, ~~intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal~~	

	accordance with Article 19. The data subject shall be informed about the right to object to profiling in a highly visible manner.	~~preferences, reliability or behaviour~~***including profiling, and produces legal effects concerning him or her or significantly***[225] ***affects him or her***.	
		1a. A data subject may be subject to a decision] referred to in paragraph 1 only if it	
		(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller [226]***; or***	
		(b) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's legitimate interests; or	
		(c) is based on the data subject's explicit consent.	
		1b. In cases referred to in paragraph 1a) the data controller	

[225] ***DE and PL wondered whether automated data processing was the right criterion for selecting high risk data processing operations and provided some examples of automated data processing operation which it did not consider as high risk. DE and ES pointed out that there are also cases of automated data processing which actually were aimed at increasing the level of data protection (e.g. in case of children that are automatically excluded from certain advertising).***

[226] ***NL had proposed to use the wording 'and arrangements allowing him to put his point of view, inspired by Article 15 of Directive 95/46. BE suggested adding this for each case referred in paragraph 2.***

		shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, such as the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision[227]:	
2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:	2. Subject to the other provisions of this Regulation, a person may be subjected to ~~a measure of the kind referred to in paragraph 1~~ ***profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject*** only if the processing:	***deleted***	
(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the	(a) is ~~carried out in the course of~~ ***necessary for*** the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied ~~or where~~**,** ***provided that*** suitable measures to safeguard the data subject's legitimate interests have	***deleted***	

[227] ***NL had proposed to use the wording 'and arrangements allowing him to put his point of view, inspired by Article 15 of Directive 95/46.***

right to obtain human intervention; or	been adduced~~, such as the right to obtain human intervention~~; or		
(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or	(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests;	***deleted***	
(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.	(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.	***deleted***	
3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.	***3.*** ~~Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person~~***Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement effective protection against possible discrimination***	3. ~~Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person~~ ***Decisions referred to in paragraph 1a*** shall not be based solely on the special categories of personal data referred to in Article 9***(1), unless points (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's legitimate interests[228] are in place.***	

[228] ***BE, FR, IT, PL, PT, AT, SE and UK reservation FR and AT reservation on the compatibility with the E-Privacy Directive. BE would prefer to reinstate the term 'solely based', but FR and DE had previously pointed out that 'not … solely' could empty this prohibition of its meaning by allowing sensitive data to be profiled together with other non-sensitive personal data. DE would prefer to insert a reference to a the use of pseudonymous data.***

	resulting from profiling. Profiling shall not be based solely on the special categories of personal data referred to in Article 9.		
4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.	***deleted***	***deleted***	
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.	***5.*** ~~The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for~~ ***Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an***	***deleted***	

	assessment. The suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2 ***shall include the right to obtain human assessment and an explanation of the decision reached after such assessment.***		
	5a. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1) for further specifying the criteria and conditions for profiling pursuant to paragraph 2.		

SECTION 5 RESTRICTIONS	SECTION 5 RESTRICTIONS	SECTION 5 RESTRICTIONS	
Article 21	***Article 21***	***Article 21***	
Restrictions	***Restrictions***	***Restrictions***[229]	
	Amendment 116		
1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:	1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights ~~provided for~~ in ~~points (a) to (e) of Article 5 and~~ Articles 11 to ~~20~~***19*** and Article 32, when such a restriction ~~constitutes~~ ***meets a clearly defined objective of public interest, respects the essence of the right to protection of personal data, is proportionate to the legitimate aim pursued and respects the fundamental rights and interests of the data subject and is*** a necessary and proportionate measure in a	1. Union or Member State law to ***which the data controller or processor is subject*** may restrict by way of a legislative measure the scope of the obligations and rights provided for in ~~points (a) to (e) of Article 5 and~~ Articles ~~11~~ 12 to 20 and Article 32, ***as well as Article 5***[230] ***in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 20,***when such a restriction constitutes a necessary and proportionate measure in a democratic society to	

[229] ***SI and UK scrutiny reservation. SE and UK wondered why paragraph 2 of Article 13 of the 1995 Data Protection Directive had not been copied here. DE, supported by DK, HU, RO, PT and SI, stated that para. 1 should not only permit restrictions of the rights of data subjects but also their extension. For example, Article 20(2)(b) requires that Member States lay down 'suitable measures to safeguard the data subject's legitimate interests', which, when they take on the form of extended rights of access to information as provided for under German law in the case of profiling to asses creditworthiness (credit scoring), go beyond the Proposal for a Regulation.***

[230] ***AT reservation.***

	democratic society to safeguard:	safeguard:	
		(aa) national security;	
		(ab) defence;	
(a) public security;	(a) public security;	(a) public security;	
(b) the prevention, investigation, detection and prosecution of criminal offences;	(b) the prevention, investigation, detection and prosecution of criminal offences;	(b) the prevention, investigation, detection and prosecution of criminal offences ***and for these purposes, safeguarding public security[231], or the execution of criminal penalties***;	
(c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;	(c) ~~other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and~~ taxation matters ~~and the protection of market stability and integrity~~;	(c) other ***important objectives of general*** public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters***, public health and social security,*** and the protection of market stability and integrity;	
		(ca) the protection of judicial independence and judicial proceedings;	

[231] ***The wording of points (b), and possibly also point (a), will have to be discussed again in the future in the light of the discussions on the relevant wording of the text of the Data Protection Directive for police and judicial cooperation.***

(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;	(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;	(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;	
(e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d);	(e) a monitoring, inspection or regulatory function ~~connected, even occasionally, with~~ ***in the framework of*** the exercise of ~~official~~ ***a competent public*** authority in cases referred to in (a), (b), (c) and (d);	(e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (aa), (ab), (a) (b), (c) and (d);	
(f) the protection of the data subject or the rights and freedoms of others.	(f) the protection of the data subject or the rights and freedoms of others.	(f) the protection of the data subject or the rights and freedoms of others~~.~~;	
		(g) ***the enforcement of civil law claims***.	
2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller.	2. In particular, any legislative measure referred to in paragraph 1 ***must be necessary and proportionate in a democratic society and*** shall contain specific provisions at least as to~~ the objectives to be pursued by the processing and the determination of the controller.~~***:*** ***(a) the objectives to be pursued by the processing;***	2. ~~In particular, a~~Any legislative measure referred to in paragraph 1 shall contain specific provisions at least***, where relevant,*** as to the ~~objectives to be pursued by the processing and the determination~~ ***purposes of the processing or categories of processing, the categories of personal data, the scope of the restrictions introduced, the specification***of the controller ***or categories of***	

	(b) the determination of the controller; ***(c) the specific purposes and means of processing;*** ***(d) the safeguards to prevent abuse or unlawful access or transfer;*** ***(e) the right of data subjects to be informed about the restriction.***	***controllers, the storage periods and the applicable safeguards taking into account of the nature, scope and purposes of the processing or categories of processing and the risks for the rights and freedoms of data subjects***.	
	2a. Legislative measures referred to in paragraph 1 shall neither permit nor oblige private controllers to retain data additional to those strictly necessary for the original purpose.		

CHAPTER IV CONTROLLER AND PROCESSOR	CHAPTER IV CONTROLLER AND PROCESSOR	CHAPTER IV CONTROLLER AND PROCESSOR[232]	
SECTION 1 GENERAL OBLIGATIONS	**SECTION 1 GENERAL OBLIGATIONS**	**SECTION 1 GENERAL OBLIGATIONS**	
Article 22	***Article 22***	***Article 22***	
	Amendment 117		
Responsibility of the controller	***Responsibility and accountability of the controller***	***~~Responsibility~~ Obligations of the controller***	
1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.	1. The controller shall adopt ***appropriate*** policies and implement appropriate ***an demonstrable technical and organisational*** measures to ensure and be able to demonstrate ***in a transparent manner*** that the processing of personal data is performed in compliance with this Regulation, ***having regard to the state of the art, the nature of personal data processing, the context, scope and purposes of processing, the risks***	1. ***Taking into account the nature, scope context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals,*** ~~The~~ the controller shall ~~adopt policies and~~ implement appropriate measures ~~to ensure~~ and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.	

[232] ***SI and UK scrutiny reservation on the entire chapter. BE, DE, NL and UK have not been not convinced by the figures provided by COM according to which the reduction of administrative burdens doing away with the general notification obligation on controllers, outbalanced any additional administrative burdens and compliance costs flowing from the proposed Regulation.***

	for the rights and freedoms of the data subjects and the type of the organisation, both at the time of the determination of the means for processing and at the time of the processing itself.		
	1a. Having regard to the state of the art and the cost of implementation, the controller shall take all reasonable steps to implement compliance policies and procedures that persistently respect the autonomous choices of data subjects. These compliance policies shall be reviewed at least every two years and updated where necessary.		
2. The measures provided for in paragraph 1 shall in particular include:	***deleted***	***deleted***	
(a) keeping the documentation pursuant to Article 28;	***deleted***	***deleted***	
(b) implementing the data security requirements laid down in Article 30;	***deleted***	***deleted***	
(c) performing a data protection impact assessment pursuant to	***deleted***	***deleted***	

Article 33;			
(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);	***deleted***	***deleted***	
(e) designating a data protection officer pursuant to Article 35(1).	***deleted***	***deleted***	
		2a. Where proportionate in relation to the processing activities[233], the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.	
		2b. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the obligations of the controller.	
3. The controller shall implement mechanisms to ensure	3. The controller shall ~~implement mechanisms to ensure the~~	***deleted***	

[233] ***HU, RO and PL thought this wording allowed too much leeway to controllers. AT thought that in particular for the respects to time limits and the reference to the proportionality was problematic.***

the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.	~~verification of the~~***be able to demonstrate the adequacy and*** effectiveness of the measures referred to in paragraphs 1 and 2. ~~If proportionate, this verification shall be carried out by independent internal or external auditors~~ ***Any regular general reports of the activities of the controller, such as the obligatory reports by publicly traded companies, shall contain a summary description of the policies and measures referred to in paragraph 1.***		
	3a. The controller shall have the right to transmit personal data inside the Union within the group of undertakings the controller is part of, where such processing is necessary for legitimate internal administrative purposes between connected business areas of the group of undertakings and an adequate level of data protection as well as the interests of the data subjects are safeguarded by internal data protection provisions or equivalent codes of conduct as referred to in Article 38.		

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.	***deleted***	***deleted***	
Article 23	***Article 23***	***Article 23***	
Data protection by design and by default	***Data protection by design and by default***	***Data protection by design and by default***	
	Amendment 118		
1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and	1. Having regard to the state of the art ~~and the cost of implementation~~, ***current technical knowledge, international best practices and the risks represented by the data processing,*** the controller ***and the processor, if any,*** shall, both at the time of the determination of the	1. Having regard to ***available technology*** ~~the state of the art~~ and the cost of implementation ***and taking account of the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for rights and freedoms of***	

organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	***purposes and*** means for processing and at the time of the processing itself, implement appropriate ***and proportionate*** technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject***, in particular with regard to the principles laid down in Article 5. Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when developing those measures and procedures***.	***individuals posed by the processing,*** the controller~~s~~ shall~~,~~ ~~both at the time of the determination of the means for processing and at the time of the processing itself,~~ implement ~~appropriate~~ technical and organisational measures ***appropriate to the processing activity being carried out and its objectives, [including minimisation and pseudonymisation[234]],*** ~~and procedures~~ in such a way that the processing will meet the requirements of this Regulation and ~~ensure~~ ***protect*** ~~the protection of~~ the rights of ~~the~~ data subject~~s~~.	

[234] ***DE thought that, in view of Article 5(c), the principle of data economy and avoidance, as well as anonymisation and pseudonymisation should be listed as key options for implementation. This debate will however need to take place in the context of a debate on pseudonymising personal data.***

	1a. In order to foster its widespread implementation in different economic sectors, data protection by design shall be a prerequisite for public procurement tenders according to Directive 2004/18/EC of the European Parliament and of the Council[48a1] as well as according to Directive 2004/17/EC of the European Parliament and of the Council[48b2] (Utilities Directive). ***[48a1] Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts (OJ L 134, 30.4.2004, p. 114).*** ***[48b2] Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sector (OJ L 134, 30.4.2004, p.1)***		

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.	2. The controller shall ~~implement mechanisms for ensuring~~ ***ensure*** that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected ~~or~~**,** retained ***or disseminated*** beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals ***and that data subjects are able to control the distribution of their personal data***.	2. The controller shall implement ~~mechanisms~~ ***appropriate measures*** for ensuring that, by default, only ~~those~~ personal data ~~are processed~~ which are necessary[235] for each specific purpose of the processing ~~and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of~~ ***are processed; this applies to*** the amount of ~~the~~ data ***collected, the extent of their processing,*** ~~and~~ the ~~time~~ ***period*** of their storage ***and their accessibility***. ***Where the purpose of the processing is not intended to provide the public with information*** ~~In particular~~, those mechanisms shall ensure that by default personal data are not made accessible ***without human intervention*** to an indefinite number of individuals.	
		2a. An approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the	

[235] ***CZ would prefer "not excessive". This term may be changed again in the future in the context of the debate on the wording of Article 5(1)(c).***

		requirements set out in paragraphs 1 and 2.	
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.	***deleted***	***deleted***	
4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	

Article 24	***Article 24***	***Article 24***	
Joint controllers	***Joint controllers***	***Joint controllers***[236]	
	Amendment 119		
Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.	Where ~~a controller determines~~ ***several controllers jointly determine*** the purposes~~, conditions~~ and means of the processing of personal data ~~jointly with others~~, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. ***The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. In case of unclarity of the responsibility, the controllers shall***	***1.*** Where ***two or more*** ~~a~~ controller<u>s</u> determine~~s~~ the purposes~~, conditions~~ and means of the processing of personal data ~~jointly with others,~~ the<u>y</u> ***are*** joint controllers<u>.</u> ***They*** shall ***in a transparent manner*** determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the ~~procedures and mechanisms for~~ exercising ***of*** the rights of the data subject ***and their respective duties to provide the information referred to in Articles 14 and 14a***, by means of an arrangement between them ***unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The***	

[236] ***SI reservation; it warned against potential legal conflicts on the allocation of the liability and SI therefore thought this article should be further revisited in the context of the future debate on Chapter VIII. FR also thought the allocation of liability between the controller and the processor is very vague and CZ expressed doubts about the enforceability of this provision in the private sector outside arrangements within a group of undertakings and thought it should contain a safeguard against outsourcing of responsibility.***

	be jointly and severally liable.	***arrangement shall designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights***.	
		2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the (…) controllers.	
		3. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. Paragraph 2 does not apply where the data subject has been informed in a transparent and unequivocal manner which of the joint controllers is responsible, unless such arrangement other than one determined by Union or Member State law is unfair with regard to his or her rights (…)	

Article 25	*Article 25*	*Article 25*	
Representatives of controllers not established in the Union	***Representatives of controllers not established in the Union***	***Representatives of controllers not established in the Union***	
	Amendment 120		
1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.	1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.	1. ~~In the situation referred to in~~ ***Where*** Article 3(2) ***applies***, the controller shall designate ***in writing*** a representative in the Union.	
2. This obligation shall not apply to:	2. This obligation shall not apply to:	2. This obligation shall not apply to:	
(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or	(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or	***deleted***	
(b) an enterprise employing fewer than 250 persons; or	(b) ~~an enterprise employing fewer than 250 persons~~***a controller processing personal data which relates to less than 5000 data subjects during any consecutive 12-month period*** ~~***are***~~ ***and not processing special categories of personal data as referred to in***	(b) ~~an enterprise employing fewer than 250~~ ***persons processing which is occasional***[237] ***and unlikely to result in a (…) risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the***	

[237] ***HU, SE and UK reservation.***

	Article 9(1), location data or data on children or employees in large-scale filing systems; or	***processing;*** or	
(c) a public authority or body; or	(c) a public authority or body; or	(c) a public authority or body; or	
(d) a controller offering only occasionally goods or services to data subjects residing in the Union.	(d) a controller ~~offering~~ only occasionally ***offering*** goods or services to data subjects ~~residing~~ in the Union***, unless the processing of personal data concerns special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large-scale filing systems***.	***deleted***	
3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.	3. The representative shall be established in one of those Member States where ~~the data subjects whose personal data are processed in relation to~~ the offering of goods or services to ~~them~~***the data subjects***, or ~~whose behaviour is monitored, reside~~ ***the monitoring of them***, ***takes place***.	3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.	
		3a. The representative shall be mandated by the controller to be addressed in addition to or instead of the controller by, in particular,	

		supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation.	
4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	
Article 26	***Article 26***	***Article 26***	
Processor	***Processor***	***Processor***	
	Amendment 121		
1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights	1. Where ~~a~~ processing ~~operation~~ is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of	1. ~~Where a processing operation is to be carried out on behalf of a controller,~~ [238] ~~the~~ The controller shall ~~choose~~ ***use only*** ~~a~~ processors providing sufficient guarantees to implement appropriate technical and organisational measures ~~and procedures~~ in such a way that the processing will meet the requirements of this Regulation ~~and~~	

[238] ***The Presidency suggest completing Article 5(2) with the words "also in case of personal data being processed on its behalf by a processor". This may also need further discussion in the context of the future debate on liability in the context of Chapter VIII.***

of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.	the data subject, in particular in respect of the technical security measures and organisational measures governing the processing to be carried out and shall ensure compliance with those measures.	~~ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures~~.	
		1a. The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes[239].	
2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:	2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller***. The controller and the processor shall be free to determine respective roles and tasks with respect to the requirements of this Regulation, and shall provide that*** ~~and stipulating in particular that~~ the	2. The carrying out of processing by a processor shall be governed by a contract or ~~other~~ a legal act ***under Union or Member State law binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of***	

[239] ***LU and FI were concerned that this might constitute an undue interference with contractual freedom.***

	processor shall:	***data subjects, the rights of*** ~~binding the processor to~~ the controller and stipulating in particular that the processor shall:	
(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;	(a) ~~act~~ ***process personal data*** only on instructions from the controller, ~~in particular, where the transfer of the personal data used is prohibited~~***, unless otherwise required by Union law or Member State law***;	(a) ***process the personal data*** ~~act~~ only on instructions from the controller, ~~in particular, where the transfer of the personal data used is prohibited~~***unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest***;	
(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;	(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;	***deleted***	
(c) take all required measures pursuant to Article 30;	(c) take all required measures pursuant to Article 30;	(c) take all required measures pursuant to Article 30;	
(d) enlist another processor only with the prior permission of the controller;	(d) ~~enlist~~ ***determine the conditions for enlisting*** another processor only with the prior permission of the controller***, unless otherwise***	(d) ***respect the conditions for*** enlist***ing*** another processor ~~only with the prior permission~~ ***such as a requirement of specific prior***	

	determined;	***permission*** of the controller;	
(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the ~~necessary~~ ***appropriate and relevant*** technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	(e) ~~insofar as this is possible given~~ **taking into account** the nature of the processing, ***assist*** ~~create in agreement with~~ the controller ~~the necessary technical and organisational requirements for the fulfilment of the controller's obligation to~~ ***in*** respond***ing*** to requests for exercising the data subject's rights laid down in Chapter III;	
(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;	(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34***, taking into account the nature of processing and the information available to the processor***;	(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;	
(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;	(g) ~~hand over~~ ***return*** all results to the controller after the end of the processing***,*** ~~and~~ not process the personal data otherwise ***and delete existing copies unless Union or Member State law requires storage of the data;***	(g) ~~hand over all results to~~ ***return or delete, at the choice of*** the controller ~~after the end of the processing and not process~~ the personal data ~~otherwise~~***upon the termination of the provision of data processing services specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the***	

		processor is subject;	
(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.	(h) make available to the controller ~~and the supervisory authority~~ all information necessary to ~~control~~ ***demonstrate*** compliance with the obligations laid down in this Article ***and allow on-site inspections;***	(h) make available to the controller ~~and the supervisory authority~~ all information necessary to ~~control~~ ***demonstrate*** compliance with the obligations laid down in this Article ***and allow for and contribute to audits conducted by the controller***.	
		The processor shall immediately inform the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions.	
		2a. Where a processor enlists another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law[240], in	

[240] ***HU suggested qualifying this reference to EU or MS law by adding 'binding that other processor to the initial processor'.***

		particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.	
		2aa. Adherence of the processor to an approved code of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39[241] may be used as an element to demonstrate sufficient guarantees referred to in paragraphs 1 and 2a.	
		2ab. Without prejudice to an individual contract between the controller and the processor, the	

[241] ***FR reservation; SK suggested specifying that where the other processor fails to fulfil its data protection obligations under such contract or other legal act, the processor shall remain fully liable to the controller for the performance of the other processor's obligation. By authorising the processor to subcontract itself and not obliging the sub-processor to have a contractual relationship with the controller, it should ensure enough legal certainty for the controller in terms of liability. The principle of liability of the main processor for any breaches of sub-processor is provided in clause 11 of Model clause 2010/87 and BCR processor and is therefore the current standard. It also suggested deleting the reference to Article 2aa.***

		contract or the other legal act referred to in paragraphs 2 and 2a may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a.	
		2b. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the examination procedure referred to in Article 87(2) [242]***.***	
		2c. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the consistency mechanism referred to in Article 57.	
3. The controller and the processor shall document in writing the controller's instructions and the	3. The controller and the processor shall document in writing the controller's instructions and the	3. ~~The controller and the processor shall document in writing the controller's instructions and the~~	

[242] ***PL was worried about a scenario in which the Commission would not act. CY and FR were opposed to conferring this role to COM (FR could possibly accept it for the EDPB).***

processor's obligations referred to in paragraph 2.	processor's obligations referred to in paragraph 2.	~~processor's obligations referred to in paragraph 2~~ ***The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing, including in an electronic form***.	
	3a. The sufficient guarantees referred to in paragraph 1 may be demonstrated by adherence to codes of conduct or certification mechanisms pursuant to Articles 38 or 39 of this Regulation.		
4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.	4. If a processor processes personal data other than as instructed by the controller ***or becomes the determining party in relation to the purposes and means of data processing***, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.	***deleted***	
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the	***deleted***	***deleted***[243]	

[243] ***COM reservation on deletion.***

responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.			
Article 27	***Article 27***	***Article 27***	
Processing under the authority of the controller and processor	***Processing under the authority of the controller and processor***	***Processing under the authority of the controller and processor***	
The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.	The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.	***deleted***	
Article 28	***Article 28***	***Article 28***	
Documentation	***Documentation***	***Records of categories of personal data processing activities***[244]	
	Amendment 122		
1. Each controller and	1. Each controller and processor	1. Each controller ~~and processor~~	

[244] ***AT scrutiny reservation.***

processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.	~~and, if any, the controller's representative,~~ shall maintain ***regularly updated*** documentation ~~of all processing operations under its responsibility~~ ***necessary to fulfill the requirements laid down in this Regulation***.	and, if any, the controller's representative, shall maintain ***a record*** ~~documentation~~ of all ***categories of personal data*** processing ~~operations~~ ***activities*** under its responsibility. ~~The documentation~~ ***This record*** shall contain ~~at least~~ the following information:	
2. The documentation shall contain at least the following information:	2. ~~The~~ ***In addition, each controller and processor shall maintain*** documentation ~~shall contain at least~~ ***of*** the following information:	***Merged with 1. above and slightly modified***	
(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;	(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;	(a) the name and contact details of the controller~~, or~~***and*** any joint controller~~ or processor~~, ~~and of the~~***control'er's*** representative ***and data protection officer***, if any;	
(b) the name and contact details of the data protection officer, if any;	(b) the name and contact details of the data protection officer, if any;	***deleted***	
(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);	***deleted***	(c) the purposes of the processing, including the legitimate interest~~s pursued by the controller where~~***when*** the processing is based on ~~point (f) of~~ Article 6(1)(f);	

(d) a description of categories of data subjects and of the categories of personal data relating to them;	***deleted***	(d) a description of categories of data subjects and of the categories of personal data relating to them;	
(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;	(e) the ~~recipients or categories of recipients of the personal data, including~~ ***name and contact details of*** the controllers to whom personal data are disclosed ~~for the legitimate interest pursued by them~~***, if any***;	(e) the ~~recipients or~~ categories of recipients ~~of~~ ***to whom*** the personal data~~, including the controllers to whom personal data are~~***have been or will be*** disclosed~~ for the legitimate interest pursued by them~~ ***in particular recipients in third countries***;	
(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;	***deleted***	(f) where applicable, ***the categories of*** transfers of ***personal*** data to a third country or an international organisation~~, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards~~;	
(g) a general indication of the time limits for erasure of the different categories of data;	***deleted***	(g) ***where possible, the envisaged*** ~~a general indication of the~~ time limits for erasure of the different categories of data;	
(h) the description of the	***deleted***	(h) ***where possible, a general***	

mechanisms referred to in Article 22(3).		***description of the technical and organisational security measures*** ~~the description of the mechanisms~~ referred to in Article ~~22~~30(~~3~~1).	
		2a. Each processor shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing:	
		(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the controller's representative, if any;	
		(b) the name and contact details of the data protection officer, if any;	
		(c) the categories of processing carried out on behalf of each controller;	
		(d) where applicable, the categories of transfers of personal data to a third country or an international organisation;	

		(e) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).	
		3a. The records referred to in paragraphs 1 and 2a shall be in writing, including in an electronic or other non-legible form which is capable of being converted into a legible form.	
3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.	***deleted***	3. ***On request,*** ~~The~~ the controller and the processor and, if any, the controller's representative, shall make the ~~documentation~~ ***record*** available~~, on request,~~ to the supervisory authority.	
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:	***deleted***	4. The obligations referred to in paragraphs 1 and 2***a*** shall not apply to~~ the following controllers and processors~~:	
(a) a natural person processing personal data without a commercial interest; or	***deleted***	(a) ~~a natural person processing personal data without a commercial interest~~; or	
(b) an enterprise or an organisation employing fewer than 250 persons that is processing	***deleted***	(b) an enterprise or an organisation employing fewer than 250 persons ~~that is~~ ***unless the***	

personal data only as an activity ancillary to its main activities.		processing ~~personal data only as an activity ancillary to its main activities~~***it carries out is likely to result in a high risk for the rights and freedoms of data subject such as discrimination, identity theft or fraud, [breach of pseudonymity,] financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage for the data subjects, taking into account the nature, scope, context and purposes of the processing; or***	
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.	***deleted***	***deleted***	
6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing	***deleted***	***deleted***	

acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).			
Article 29	***Article 29***	***Article 29***	
Co-operation with the supervisory authority	***Co-operation with the supervisory authority***	***Co-operation with the supervisory authority***	
	Amendment 123		
1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.	1. The controller and***, if any,*** the processor and~~, if any,~~ the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.	***deleted***	
2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken	2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken	***deleted***	

and the results achieved, in response to the remarks of the supervisory authority.	and the results achieved, in response to the remarks of the supervisory authority.		

SECTION 2 DATA SECURITY	SECTION 2 DATA SECURITY	SECTION 2 DATA SECURITY	
Article 30	***Article 30***	***Article 30***	
Security of processing	***Security of processing***	***Security of processing***	
	Amendment 124		
1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.	1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing ~~and the nature of the personal data to be protected~~, ***taking into account the results of a data protection impact assessment pursuant to Article 33,*** having regard to the state of the art and the costs of their implementation.	1. ***Having regard to available technology and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of individuals,*** ~~The~~ the controller and the processor shall implement appropriate technical and organisational measures***[, including pseudonymisation of personal data]*** to ensure a level of security appropriate to the risk~~s represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation~~.	
	1a. Having regard to the state of the art and the cost of	***1a. In assessing the appropriate level of security account shall be***	

	implementation, such a security policy shall include:	***taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.***	
	(a) the ability to ensure that the integrity of the personal data is validated;		
	(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;		
	(c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident that impacts the availability, integrity and confidentiality of information systems and services;		
	(d) in the case of sensitive personal data processing according to Articles 8 and 9, additional security measures to ensure situational awareness of risks and the ability		

	to take preventive, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to the data;		
	(e) a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness.		
2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.	2. The ~~controller and the processor shall, following an evaluation of the risks, take the~~ measures referred to in paragraph 1 ~~to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.~~ ***shall at least:***	***deleted***	
	(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;		
		2a. Adherence to approved codes of conduct pursuant to Article 38	

		or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraph 1.	
	(b) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and		
		2b. The controller and processor shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	
	(c) ensure the implementation of a security policy with respect to the processing of personal data.		
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for	3. The ~~Commission~~ ***European Data Protection Board*** shall be ~~empowered to adopt delegated acts~~	***deleted***	

the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.	~~in accordance with Article 86 for the purpose of~~ ~~further specifying the criteria and conditions~~ ***entrusted with the task of issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1)*** for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default~~, unless paragraph 4 applies~~.		
4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:	***deleted***	***deleted***	
(a) prevent any unauthorised access to personal data;	***deleted***	***deleted***	
(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of	***deleted***	***deleted***	

personal data;			
(c) ensure the verification of the lawfulness of processing operations.	***deleted***	***deleted***	
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	
Article 31	***Article 31***	***Article 31***	
Notification of a personal data breach to the supervisory authority	***Notification of a personal data breach to the supervisory authority***	***Notification of a personal data breach to the supervisory authority***[245]	
	Amendment 125		
1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases	1. In the case of a personal data breach, the controller shall without undue delay ~~and, where feasible, not later than 24 hours after having become aware of it,~~ notify the personal data breach to the supervisory authority. ~~The notification to the supervisory authority shall be accompanied by a reasoned justification in cases~~	1. In the case of a personal data breach ***which is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, [breach of (…) pseudonymity], damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant***	

[245] ***AT and SI scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded; SI thought this alignment could be achieved by deleting "high" before "risk" in Articles 31 and 32.***

where it is not made within 24 hours.	~~where it is not made within 24 hours~~.	***economic or social disadvantage***, the controller shall without undue delay and, where feasible, not later than ~~24~~ 72 hours after having become aware of it, notify the personal data breach to the supervisory authority ***competent in accordance with Article 51***. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within ~~24~~ 72 hours.	
		1a. The notification referred to in paragraph 1 shall not be required if a communication to the data subject is not required under Article 32(3)(a) and (b)[246]***.***	
2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.	2. ~~Pursuant to point (f) of Article 26(2), the~~ ***The*** processor shall alert and inform the controller ~~immediately~~ ***without undue delay*** after the establishment of a personal data breach.	2. ~~Pursuant to point (f) of Article 26(2), the~~ The processor shall ~~alert~~ ***notify*** ~~and inform~~ the controller ~~immediately after the establishment~~ ***without undue delay after becoming award*** of a personal data breach.	
3. The notification referred to	3. The notification referred to in	3. The notification referred to in	

[246] ***AT and PL thought this paragraph should be deleted.***

in paragraph 1 must at least:	paragraph 1 must at least:	paragraph 1 must at least:	
(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;	(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;	(a) describe the nature of the personal data breach including ***where possible and appropriate,*** the ***approximate*** categories and number of data subjects concerned and the categories and ***approximate*** number of data records concerned;	
(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;	(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;	(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;	
(c) recommend measures to mitigate the possible adverse effects of the personal data breach;	(c) recommend measures to mitigate the possible adverse effects of the personal data breach;	***deleted***	
(d) describe the consequences of the personal data breach;	(d) describe the consequences of the personal data breach;	(d) describe the ***likely*** consequences of the personal data breach ***identified by the controller***;	
(e) describe the measures proposed or taken by the controller to address the personal data breach.	(e) describe the measures proposed or taken by the controller to address the personal data breach ***and/or mitigate its effects***. ***The information may if necessary be provided in phases.***	(e) describe the measures ***taken or*** proposed ~~or~~ ***to be*** taken by the controller to address the personal data breach~~.~~; ***and***	

		(f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach.	
		3a. Where, and in so far as, it is not possible to provide the information referred to in paragraph 3 (d), (e) and (f) at the same time as the information referred to in points (a) and (b) of paragraph 3, the controller shall provide this information without undue further delay.	
4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.	4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must ***be sufficient to*** enable the supervisory authority to verify compliance with this Article ***and with Article 30***. The documentation shall only include the information necessary for that purpose.	4. The controller shall document any personal data breaches ***referred to in paragraphs 1 and 2***, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. ~~The documentation shall only include the information necessary for that purpose.~~	
	4a. The supervisory authority shall keep a public register of the types of breaches notified.		

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.	**5.** The ~~Commission~~ ***European Data Protection Board*** shall be ~~empowered to adopt delegated acts in accordance with Article 86 for the purpose~~ ***entrusted with the task*** of ~~further specifying the criteria and requirements~~ ***issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1)*** for establishing the data breach ***and determining the undue delay*** referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor ~~is~~***are*** required to notify the personal data breach.	***deleted***	
6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted	***deleted***	***deleted***[247]	

[247] ***COM reservation on deletion.***

in accordance with the examination procedure referred to in Article 87(2).			
Article 32	***Article 32***	***Article 32***	
Communication of a personal data breach to the data subject	***Communication of a personal data breach to the data subject***	***Communication of a personal data breach to the data subject***[248]	
	Amendment 126		
1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.	1. When the personal data breach is likely to adversely affect the protection of the personal data***, the*** ~~or~~ privacy***, the rights or the legitimate interests*** of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.	1. When the personal data breach is likely to ~~adversely affect the protection of the personal data or privacy of the data subject~~ ***result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage***, the controller shall~~, after the notification referred to in Article 31,~~ communicate the personal data breach to the data subject without undue delay.	

[248] ***AT scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded.***

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).	2. The communication to the data subject referred to in paragraph 1 shall ***be comprehensive and use clear and plain language. It shall*** describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) ~~and~~**,** (c) ***and (d)*** of Article 31(3) ***and information about the rights of the data subject, including redress*****.**	2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b)**,** (e) and (~~e~~f) of Article 31(3).	
3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.	3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.	3. The communication ~~of a personal data breach~~ to the data subject ***referred to in paragraph 1*** shall not be required if: a. the controller ~~demonstrates to the satisfaction of the supervisory authority that it~~ has implemented appropriate technological ***and organisational*** protection measures, and that those measures were applied to the data ~~concerned~~ ***affected*** by the personal data breach***, in particular those that*** ~~.~~ ~~Such technological protection measures shall~~ render the data unintelligible to any person who is not authorised to access it***, such as***	

		encryption;or ***b. the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; or*** ***c. it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or*** ***d. it would adversely affect a substantial public interest.***	
4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse	4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects	***deleted***	

effects of the breach, may require it to do so.	of the breach, may require it to do so.		
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.	5. The ~~Commission~~***European Data Protection Board*** shall be ~~empowered to adopt delegated acts in accordance with Article 86 for the purpose~~ ***entrusted with the task*** of ~~further specifying the criteria and requirements~~ ***issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1)*** as to the circumstances in which a personal data breach is likely to adversely affect the personal data***, the privacy, the rights or the legitimate interests of the data subject*** referred to in paragraph 1.	***deleted***	
6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article	***deleted***	***deleted***[249]	

[249] ***COM reservation on deletion.***

87(2).			
	Amendment 127		
	Article 32a		
	Respect to Risk		
	1. The controller, or where applicable the processor, shall carry out a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks..		
	2. The following processing operations are likely to present specific risks:		
	(a) processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;		
	(b) processing of special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large		

	scale filing systems;		
	(c) profiling on which measures are based that produce legal effects concerning the individual or similarly significantly affect the individual;		
	(d) processing of personal data for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;		
	(e) automated monitoring of publicly accessible areas on a large scale;		
	(f) other processing operations for which the consultation of the data protection officer or supervisory authority is required pursuant to point (b) of Article 34(2);		
	(g) where a personal data breach would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate		

	interests of the data subject;		
	(h) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects;		
	(i) where personal data are made accessible to a number of persons which cannot reasonably be expected to be limited.		
	3. According to the result of the risk analysis:		
	(a) where any of the processing operations referred to in points (a) or (b) of paragraph 2 exist, controllers not established in the Union shall designate a representative in the Union in line with the requirements and exemptions laid down in Article 25;		
	(b) where any of the processing operations referred to in points (a), (b) or (h)of paragraph 2 exist, the controller shall designate a data		

	protection officer in line with the requirements and exemptions laid down in Article 35;		
	(c) where any of the processing operations referred to in points (a), (b), (c), (d), (e), (f), (g) or (h) of paragraph 2 exist, the controller or the processor acting on the controller's behalf shall carry out a data protection impact assessment pursuant to Article 33;		
	(d) where processing operations referred to in point (f) of paragraph 2 exist, the controller shall consult the data protection officer, or in case a data protection officer has not been appointed, the supervisory authority pursuant to Article 34.		
	4. The risk analysis shall be reviewed at the latest after one year, or immediately, if the nature, the scope or the purposes of the data processing operations change significantly. Where pursuant to point (c) of paragraph 3 the controller is not obliged to carry out a data protection impact assessment, the risk analysis shall		

	be documented.		
	Amendment 128		
SECTION 3 **DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION**	**SECTION 3** ***LIFECYCLE* DATA PROTECTION *MANAGEMENT***	**SECTION 3** **DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION**	
Article 33	***Article 33***	***Article 33***	
Data protection impact assessment	***Data protection impact assessment***	***Data protection impact assessment***[250]	
1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	1. Where ~~processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes,~~ ***required pursuant to point (c) of Article 32a(3***) the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the ***rights and freedoms of the data subjects, especially their right***	1. Where ***a type of*** processing ***in particular using new technologies, and taking into account*** ~~operations present specific risks to the rights and freedoms of data subjects by virtue of their~~ ***the*** nature, ~~their~~ ***scope, context and*** ~~***or*** their~~ purposes ***of the processing, is likely to result in a high***[251] ***risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss,***	

[250] ***FR, HU, AT and COM expressed doubts on the concept of new types of processing, which is now clarified in recital 70. UK thought this obligation should not apply where there is an overriding public interest for the processing to take place (such as a public health emergency).***

[251] ***FR, RO, SK and UK warned against the considerable administrative burdens flowing from the proposed obligation. The UK considers that any requirements to carry out a data protection impact assessment should be limited to those cases where there is an identified high risk to the rights of data subjects.***

	to protection of personal data. ***A single assessment shall be sufficient to address a set of similar processing operations that present similar risks.***	***damage to the reputation, [breach of pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage***, the controller[252] ~~or the processor acting on the controller's behalf~~ shall***, prior to the processing,*** carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	
		1a. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.	
2. The following processing operations in particular present specific risks referred to in paragraph 1:	***deleted***	2. ~~The following processing operations in particular present specific risks~~ ***A data protection impact assessment*** referred to in paragraph 1 ***shall in particular be required in the following cases***:	
(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular	***deleted***	(a) a systematic and extensive evaluation of personal aspects relating to ~~a~~ natural person<u>s</u> ~~or for analysing or predicting in particular~~	

[252] ***COM reservation on deletion.***

the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;		~~the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing~~ ***which is based on profiling*** and on which ~~measures~~ ***decisions***[253] are based that produce legal effects concerning ~~the individual~~ ***data subjects*** or ~~significantly~~ ***severely*** affect ~~the individual~~***data subjects***;	
(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;	***deleted***	(b) ~~information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases~~ ***processing of special categories of personal data under Article 9(1) (…)***[254]***, biometric data or data on criminal convictions and offences or related security measures***, where the data are processed for taking ~~measures or~~ decisions regarding specific individuals on a large scale;	
(c) monitoring publicly accessible areas, especially when	***deleted***	(c) monitoring publicly accessible areas on a large scale, especially	

253 ***In the future this wording will be aligned to the eventual wording of Article 20.***

254 **HU suggested that data pertaining to children be also reinserted.**

using optic-electronic devices (video surveillance) on a large scale;		when using optic-electronic devices ~~(video surveillance) on a large scale~~;	
(d) personal data in large scale filing systems on children, genetic data or biometric data;	***deleted***	***deleted***	
(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).	***deleted***	***deleted***[255]	
		2a. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the European Data Protection Board. [256]	
		2b. The supervisory authority may also establish and make public a list of the kind of processing	

[255] ***FR scrutiny reservation. PL thought a role could be given to the EDPB in order to determine high-risk operations.***

[256] ***CZ reservation.HU wondered what kind of legal consequences, if any, would be triggered by the listing of a type of processing operation by a DPA with regard to on-going processing operations as well as what its territorial scope would be. In the view of the Presidency any role for the EDPB in this regard should be discussed in the context of Chapter VII.***

		operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.	
		2c. Prior to the adoption of the lists referred to in paragraphs 2a and 2b the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union. [257]	
3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures	3. The assessment shall ***have regard to the entire lifecycle management of personal data from collection to processing to deletion. It shall*** contain at least ~~a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of~~	3. The assessment shall contain at least a general description of the envisaged processing operations, an ~~assessment~~ ***evaluation*** of the risk~~s to the rights and freedoms of data subjects~~***referred to in paragraph 1***, the measures envisaged to address the risk~~s,~~ ***including*** safeguards,	

[257] ***CZ reservation.***

and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.	~~data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned~~***:***	security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned[***258***].	
	(a) a systematic description of the envisaged processing operations, the purposes of the processing and, if applicable, the legitimate interests pursued by the controller;		
	(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;		
	(c) an assessment of the risks to the rights and freedoms of data subjects, including the risk of discrimination being embedded in or reinforced by the operation;		
	(d) a description of the measures envisaged to address the risks and minimise the volume of personal		

258 ***FR scrutiny reservation.***

	data which is processed;		
	(e) a list of safeguards, security measures and mechanisms to ensure the protection of personal data, such as pseudonymisation, and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned;		
	(f) a general indication of the time limits for erasure of the different categories of data;		
	(g) an explanation which data protection by design and default practices pursuant to Article 23 have been implemented;		
	(h) a list of the recipients or categories of recipients of the personal data;		
	(i) where applicable, a list of the intended transfers of data to a third country or an international organisation, including the identification of that third country or international organisation ~~***and, in case of transfers referred to in***~~		

	~~*point (h) of Article 44(1), the documentation of appropriate safeguards*~~*;*		
	(j) an assessment of the context of the data processing.		
	3a. If the controller or the processor has designated a data protection officer, he or she shall be involved in the impact assessment proceeding.		
	3b. The assessment shall be documented and lay down a schedule for regular periodic data protection compliance reviews pursuant to Article 33a(1). The assessment shall be updated without undue delay, if the results of the data protection compliance review referred to in Article 33a show compliance inconsistencies. The controller and the processor and, if any, the controller's representative shall make the assessment available, on request, to the supervisory authority.		
		3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant	

		controllers or processors shall be taken into due account in assessing lawfulness and impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment[259].	
4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	***deleted***	4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations[260].	
5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the	***Deleted***	5. Where ~~the controller is a public authority or body and where~~ the processing ~~results from a legal obligation~~ pursuant to point (c) ***or (e)*** of Article 6(1) ~~providing for rules and procedures pertaining to the processing operations and regulated by~~ ***has a legal basis in*** Union law~~, paragraphs 1 to 4 shall not apply, unless~~***or the law of the*** Member State~~s~~ ***to which the controller is subject, and such law***	

259 HU thought this should be moved to a recital.

260 CZ and FR indicated that this was a completely impractical obligation; IE reservation.

processing activities.		***regulates the specific processing operation or set of operations in question[261], paragraphs 1 to 3 shall not apply, unless Member States*** deem it necessary to carry out such assessment prior to the processing activities.	
6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.	***deleted***	***deleted***	
7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those	***deleted***	***deleted***	

[261] ***BE and SI stated that this will have to be revisited in the context of the future debate on how to include the public sector in the scope of the Regulation.***

implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).			
	Amendment 130		
	Article 33 a (new)		
	Data protection compliance review		
	1. At the latest two years after the carrying out of an impact assessment pursuant to Article 33(1), the controller or the processor acting on the controller's behalf shall carry out a compliance review. This compliance review shall demonstrate that the processing of personal data is performed in compliance with the data protection impact assessment.		
	2. The compliance review shall be carried out periodically at least once every two years, or immediately when there is a change in the specific risks presented by the processing operations.		

	3. Where the compliance review results show compliance inconsistencies, the compliance review shall include recommendations on how to achieve full compliance.		
	4. The compliance review and its recommendations shall be documented. The controller and the processor and, if any, the controller's representative shall make the compliance review available, on request, to the supervisory authority.		
	5. If the controller or the processor has designated a data protection officer, he or she shall be involved in the compliance review proceeding.		
Article 34	***Article 34***	***Article 34***	
	Amendment 131		
Prior authorisation and prior consultation	***Prior consultation***	**Prior ~~authorisation and prior~~ consultation**	
1. The controller or the processor as the case may be shall	***deleted***	***deleted***	

obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.			
2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:	2. The controller or processor acting on the controller's behalf shall consult the ***data protection officer, or in case a data protection officer has not been appointed, the*** supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the	2. The controller[262] ~~or processor acting on the controller's behalf~~ shall consult the supervisory authority prior to the processing of personal data ***where a data protection impact assessment as provided for in Article 33 indicates that the*** ~~in order to ensure the compliance of the intended~~ processing ~~with this Regulation and in particular to mitigate the~~ ***would result in a high*** risk~~s involved for~~	

[262] ***COM and LU reservation on deleting processor.***

	data subjects where:	~~the data subjects where:~~***in the absence of measures to be taken by the controller to mitigate the risk.***	
(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or	(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or	***deleted***	
(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.	(b) ***the data protection officer or*** the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.	***deleted***	
3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy	3. Where the ***competent*** supervisory authority ~~is of the opinion~~ ***determines in accordance with its power*** that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make	3. Where the supervisory authority is of the opinion that the intended processing ***referred to in paragraph 2 would*** ~~does~~ not comply with this Regulation, in particular where ***the controller has*** ~~risks are~~ insufficiently identified or mitigated, it shall~~ prohibit the intended processing and make~~	

such incompliance.	appropriate proposals to remedy such non-compliance.	~~appropriate proposals to remedy such incompliance~~***within a maximum period of 6 weeks following the request for consultation give advice to the data controller , in writing, and may use any of its powers referred to in[263] Article 53. This period may be extended for a further six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.***	
4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.	4. The ~~supervisory authority~~ ***European Data Protection Board*** shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to ~~point (b) of~~ paragraph 2. ~~The supervisory authority shall communicate those lists to the European Data Protection Board~~.	***deleted***	

[263] ***UK reservation; it thought the power to prohibit processing operations should not apply during periods in which there is an overriding public interest for the processing to take place (such as a public health emergency). The Presidency thinks this issue should however be debated in the context of Chapter VI on the powers of the DPA, as these may obviously also be used regardless of any consultation.***

5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.	***deleted***	***deleted***	
6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.	6. The controller or processor shall provide the supervisory authority***, on request,*** with the data protection impact assessment ~~provided for in~~ ***pursuant to*** Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.	6. ***When consulting the supervisory authority pursuant to paragraph2,*** ~~The~~ the controller ~~or processor~~ shall provide the supervisory authority, with ***(a) where applicable, the respective responsibilities of controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;*** ***(b) the purposes and means of the intended processing;*** ***(c) the measures and safeguards provided to protect the***	

		rights and freedoms of data subjects pursuant to this Regulation; ***(d) where applicable , the contact details of the data protection officer;*** ***(e)*** the data protection impact assessment provided for in Article 33***;*** and ***(f)***~~, on request, with~~ any other information ~~to allow~~ ***requested by*** the supervisory authority~~ to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards~~.	
7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.	7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.	7. Member States shall consult the supervisory authority ~~in~~ ***during*** the preparation of a ***proposal for a*** legislative measure ~~to be~~ adopted by ~~the~~ a national parliament or of a measure based on such a legislative measure~~,~~ which ~~defines the nature of the processing, in order to ensure the compliance of the intended~~ ***provide for the*** processing~~ with this Regulation and in particular to mitigate the risks involved for the~~	

		~~data subjects~~***of personal data***[264].	
		7a. Notwithstanding paragraph 2, Member States' law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health[265]***.***	
8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.	***deleted***	***deleted***	
9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard	***deleted***	***deleted***	

264 ***IE scrutiny reservation on deletion.***

265 SE scrutiny reservation.

forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).			

SECTION 4 DATA PROTECTION OFFICER	SECTION 4 DATA PROTECTION OFFICER	SECTION 4 DATA PROTECTION OFFICER	
Article 35	***Article 35***	***Article 35***	
Designation of the data protection officer	***Designation of the data protection officer***	***Designation of the data protection officer***	
	Amendment 132		
1. The controller and the processor shall designate a data protection officer in any case where:	1. The controller and the processor shall designate a data protection officer in any case where :	1. The controller ~~and~~ ***or*** the processor ***may,or where required by Union or Member State law*** shall[266] designate a data protection officer ~~in any case where:~~.	
(a) the processing is carried out by a public authority or body; or	(a) the processing is carried out by a public authority or body; or	***deleted***	
(b) the processing is carried out by an enterprise employing 250 persons or more; or	(b) the processing is carried out by ~~an enterprise employing 250 persons or more~~ ***a legal person and relates to more than 5000 data subjects in any consecutive 12-month period***; or	***deleted***	

[266] ***Made optional further to decision by the Council. AT scrutiny reservation. DE, HU and AT would have preferred to define cases of a mandatory appointment of DPA in the Regulation itself and may want to revert to this issue at a later stage. COM reservation on optional nature and deletion of points a) to c).***

(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.	(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects***; or***	***deleted***	
	(d) the core activities of the controller or the processor consist of processing special categories of data pursuant to Article 9(1), location data or data on children or employees in large scale filing systems.		
2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.	2. ~~In the case referred to in point (b) of paragraph 1, a~~ ***A*** group of undertakings may appoint a ~~single~~ ***main responsible*** data protection officer***, provided it is ensured that a data protection officer is easily accessible from each establishment.***	2. ~~In the case referred to in point (b) of paragraph 1, a~~ A group of undertakings may appoint a single data protection officer.	
3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the	3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the	3. Where the controller or the processor is a public authority or body, ~~the~~ ***a single*** data protection officer may be designated for several ~~of its entities~~***such authorities or bodies***, taking	

public authority or body.	public authority or body.	account of the***ir*** organisational structure~~ of the public authority or body~~***and size***.	
4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.	4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.	***deleted***	
5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.	5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.	5. The ~~controller or processor shall designate the~~ data protection officer ***shall be designated*** on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37***, particularly the absence of any conflict of interests***.~~ The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.~~	
6. The controller or the processor shall ensure that any other professional duties of the data	6. The controller or the processor shall ensure that any other professional duties of the data	***deleted***	

protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.	protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.		
7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.	7. The controller or the processor shall designate a data protection officer for a period of at least ~~two~~ ***four*** years ***in case of an employee or two years in case of an external service contractor***. The data protection officer may be reappointed for further terms. During ~~their~~ ***his or her*** term of office, the data protection officer may only be dismissed, if ~~the data protection officer~~ ***he or she*** no longer fulfils the conditions required for the performance of ~~their~~ ***his or her*** duties.	7. ~~The controller or the processor shall designate a~~ ***During their term of office, the*** data protection officer ~~for a period of at least two years. The data protection officer~~ may***, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant,*** ~~be reappointed for further terms. During their term of office, the data protection officer may only~~ be dismissed~~,~~***only*** if the data protection officer no longer fulfils the conditions required for the performance of ~~their duties~~***his or her tasks pursuant to Article 37***.	
8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.	8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.	8. The data protection officer may be ~~employed by~~ ***a staff member of*** the controller or processor, or fulfil ~~his or her~~ ***the*** tasks on the basis of a service contract.	
9. The controller or the processor shall communicate the name and contact details of the data	9. The controller or the processor shall communicate the name and contact details of the data protection	9. The controller or the processor shall ~~communicate~~ ***publish*** the ~~name and~~ contact details of the data	

protection officer to the supervisory authority and to the public.	officer to the supervisory authority and to the public.	protection officer ***and communicate these*** to the supervisory authority ~~and to the public~~.	
10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.	10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.	10. Data subjects ~~shall have the right to~~ ***may*** contact the data protection officer on all issues related to the processing of the data subject's data and ~~to request exercising the~~ ***the exercise of their*** rights under this Regulation.	
11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.	***deleted***	***deleted***	

Article 36	*Article 36*	*Article 36*	
Position of the data protection officer	***Position of the data protection officer***	***Position of the data protection officer***	
	Amendment 133		
1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	
2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.	2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the ***executive*** management of the controller or the processor. ***The controller or processor shall for this purpose designate an executive management member who shall be responsible for the compliance with the provisions of this Regulation***.	2. The controller or processor shall ~~ensure that~~ ***support*** the data protection officer ***in*** perform~~s~~***ing*** the ~~duties and~~ tasks ***referred to in Article 37 by providing resources necessary to carry out these tasks as well as access to personal data and processing operations*** ~~independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor~~***.***	

3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.	3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide ***all means, including*** staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37***, and to maintain his or her professional knowledge***.	3. The controller or ~~the~~ processor shall ~~support~~ ***ensure that*** the data protection officer ***can act*** in ***an independent manner with respect to the*** perform~~ing~~***ance of his or her*** ~~the~~ tasks and ~~shall provide staff, premises, equipment and any other resources necessary to carry out the duties~~ and ***does not receive any instructions regarding the exercise of these*** tasks ~~referred to in Article 37~~***. He or she shall not be penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.***	
	4. Data protection officers shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless they are released from that obligation by the data subject.		
		4. The data protection officer may fulfil other tasks and duties. The controller or processor shall	

		ensure that any such tasks and duties do not result in a conflict of interests.	
Article 37	***Article 37***	***Article 37***	
Tasks of the data protection officer	***Tasks of the data protection officer***	***Tasks of the data protection officer***	
	Amendment 134		
1. The controller or the processor shall entrust the data protection officer at least with the following tasks:	~~1.~~ The controller or the processor shall entrust the data protection officer at least with the following tasks:	1. The ~~controller or the processor shall entrust the~~ data protection officer ~~at least with~~ ***shall have*** the following tasks:	
(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;	(a) ***to raise awareness,*** to inform and advise the controller or the processor of their obligations pursuant to this Regulation***, in particular with regard to technical and organisational measures and procedures,*** and to document this activity and the responses received;	(a) to inform and advise the controller or the processor ***and the employees who are processing personal data*** of their obligations pursuant to this Regulation and ~~to document this activity and the responses received~~***other Union or Member State data protection provisions***;	
(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff	(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing	(b) to monitor ***compliance with this Regulation, with other Union or Member State data protection provisions and with*** the ~~implementation and application of the~~ policies of the controller or processor in relation to the	

involved in the processing operations, and the related audits;	operations, and the related audits;	protection of personal data, including the assignment of responsibilities, ***awareness-raising and*** ~~the~~ training of staff involved in the processing operations, and the related audits;	
(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;	(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;	***deleted***	
(d) to ensure that the documentation referred to in Article 28 is maintained;	(d) to ensure that the documentation referred to in Article 28 is maintained;	***deleted***	
(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;	(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;	***deleted***	
(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for	(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for	(f) to ~~monitor the performance of~~ ***provide advice where requested as regards*** the data protection impact assessment ~~by the controller or~~	

prior authorisation or prior consultation, if required pursuant Articles 33 and 34;	prior ~~authorisation or prior~~ consultation, if required pursuant ***to*** Articles ***32a,*** 33 and 34;	~~processor and the application for prior authorisation or prior consultation, if required~~ ***monitor its performance*** pursuant Article~~s~~ 33 ~~and 34~~;	
(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;	(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;	(g) to monitor ~~the~~ response~~s~~ to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, ***to*** co-~~operating~~ operate with the supervisory authority at the latter's request or on the data protection officer's own initiative;	
(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.	(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative**.**	(h) to act as the contact point for the supervisory authority on issues related to the processing ***of pesonal data, including the prior*** ~~*and*~~ consult***ation referred to in Article 34, and consult, as*** ~~with the supervisory authority, if~~ appropriate, on ~~his/her own initiative~~***any other matter***.	
	(i) to verify the compliance with this Regulation under the prior consultation mechanism laid out in Article 34;		

	(j) to inform the employee representatives on data processing of the employees.		
2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.	***deleted***	***deleted***	
		2a. The data protection officer shall in the performance his or her tasks have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of the processing.	

SECTION5 CODES OF CONDUCT AND CERTIFICATION	SECTION5 CODES OF CONDUCT AND CERTIFICATION	SECTION5 CODES OF CONDUCT AND CERTIFICATION	
Article 38	***Article 38***	***Article 38***	
Codes of conduct	***Codes of conduct***	***Codes of conduct*** [267]	
	Amendment 135		
1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:	1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct ***or the adoption of codes of conduct drawn up by a supervisory authority*** intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:	1. The Member States, the supervisory authorities***, the European Data Protection Board*** and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors~~, in particular in relation to:~~***and the specific needs of micro, small and medium-sized enterprises.***	
		1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for	

[267] ***AT, FI, SK and PL scrutiny reservation.***

		the purpose of specifying the application of provisions of this Regulation, such as:	
(a) fair and transparent data processing;	(a) fair and transparent data processing;	(a) fair and transparent data processing;	
	(aa) respect for consumer rights;		
		(aa) the legitimate interests pursued by controllers in specific contexts;	
(b) the collection of data;	(b) the collection of data;	(b) the collection of data;	
		(bb) the pseudonymisation of personal data;	
(c) the information of the public and of data subjects;	(c) the information of the public and of data subjects;	(c) the information of the public and of data subjects;	
(d) requests of data subjects in exercise of their rights;	(d) requests of data subjects in exercise of their rights;	(d) ~~requests of data subjects in~~***the*** exercise of the~~ir~~ rights ***of data subjects***;	
(e) information and protection of children;	(e) information and protection of children;	(e) information and protection of children ***and the way to collect the parent's and guardian's consent***;	
		(ee) measures and procedures referred to in Articles 22 and 23	

		and measures to ensure security of processing referred to in Article 30;	
		(ef) notification of personal data breaches to supervisory authorities and communication of such breaches to data subjects;	
(f) transfer of data to third countries or international organisations;	(f) transfer of data to third countries or international organisations;	***deleted***	
(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;	(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;	***deleted***	
(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.	(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.	***deleted***	
		1ab. In addition to adherence by controller or processor subject to the regulation, codes of conduct approved pursuant to paragraph 2	

		may also be adhered to by controllers or processors that are not subject to this Regulation according to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(d). Such controllers or processors shall make binding and enforceable commitments, via contractual instruments or otherwise, to apply those appropriate safeguards including as regards data subjects' rights.	
		1b. Such a code of conduct shall contain mechanisms which enable the body referred to in paragraph 1 of article 38a to carry out the mandatory[268] monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.	

[268] CZ preferred this monitoring to be optional.

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.	2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority ~~may~~ ***shall without undue delay*** give an opinion ***on*** whether ***the processing under*** the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.	2. Associations and other bodies ***referred to in paragraph 1a*** ~~representing categories of controllers or processors in one Member State~~ which intend to ~~draw up~~ ***prepare a*** code~~s~~ of conduct or to amend or extend existing code~~s, of conduct may~~***shall*** submit the~~m to an opinion of~~***draft code to*** the supervisory authority~~ in that Member State~~***which is competent pursuant to Article 51***. The supervisory authority ~~may~~ ***shall*** give an opinion ***on*** whether the draft code***, or amended or extended*** ~~of~~ conduct ~~or the amendment~~ is in compliance with this Regulation ***and shall approve such draft, amended or extended coded if it finds that it provides sufficient appropriate safeguards***. ~~The supervisory authority shall seek the views of data subjects or their representatives on these drafts.~~	
		2a. Where the opinion referred to in paragraph 2 confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation and the code is approved, and if the code of	

		conduct does not relate to processing activities in several Member States, the supervisory authority shall register the code and publish the details thereof.	
		2b. Where the draft code of conduct relates to processing activities in several Member States, the supervisory authority competent pursuant to Article 51 shall, before approval, submit it in the procedure referred to in Article 57 to the European Data Protection Board which shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation or, in the situation referred to in paragraph 1ab, provides appropriate safeguards[269].	
3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of	3. Associations and other bodies representing categories of controllers ***or processors*** in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of	3. ~~Associations and other bodies representing categories of controllers in several Member States may submit draft~~ ***Where the opinion referred to in paragraph 2b confirms that the*** code~~s~~ of	

[269] ***FR made a proposal for a paragraph 2c: 'Approved codes of conduct pursuant to paragraph 2a shall constitute an element of the contractual relationship between the controller and the data subject. When such codes of conduct determine the compliance of the controller or processor with this Regulation, they shall be legally binding and enforceable.'***

conduct to the Commission.	conduct to the Commission.	conduct***,*** ~~and~~ ***or*** amendme~~nts~~***ed*** or exten~~sions~~***ed*** ~~to existing codes~~ code,~~of conduct to the Commission~~ ***is in compliance with this Regulation, or, in the situation referred to in paragraph 1ab, provides appropriate safeguards ,the European Data Protection Board shall submit its opinion to the Commission***.	
4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	4. The Commission ~~may adopt implementing acts~~ ***shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86*** for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 ***are in line with this Regulation and*** have general validity within the Union. Those ~~implementing acts~~ ***delegated acts*** shall ~~be adopted in accordance with the examination procedure set out in Article 87(2)~~ ***confer enforceable rights on data subjects.***	4. The Commission may adopt implementing acts for deciding that the ***approved*** codes of conduct and amendments or extensions to existing ***approved*** codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.	5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.	5. The Commission shall ensure appropriate publicity for the ***approved*** codes which have been decided as having general validity in accordance with paragraph 4.	
		5a. The European Data Protection Board shall collect all approved codes of conduct and amendments thereto in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.	
		Article 38a	
		Monitoring of approved codes of conduct[270]	
		1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38 (1b), may be carried out by a body[271] ***which has an appropriate***	

[270] ***AT, LU scrutiny reservation.***

[271] ***CZ, ES, LU are opposed to giving this role to such separate bodies. Concerns were raised, inter alia, on the administrative burden involved in the setting up of such bodies. Codes of conduct are an entirely voluntary mechanism in which no controller is obliged to participate.***

		level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.	
		2. A body referred to in paragraph 1 may be accredited for this purpose if:	
		(a) it has demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;	
		(b) it has established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;	
		(c) it has established procedures and structures to deal with complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make these procedures and structures transparent to data	

		subjects and the public;	
		(d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.	
		3. The competent supervisory authority shall submit the draft criteria for accreditation of a body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.	
		4. Without prejudice to the provisions of Chapter VIII, a body referred to in paragraph 1 may, subject to adequate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.	

		5. The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation. ***This article shall not apply to the processing of personal data carried out by public authorities and bodies.***	
Article 39	***Article 39***	***Article 39***	
Certification	***Certification***	***Certification***[272]	
	Amendment 136		
1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and	***deleted***	1. The Member States***, the European Data Protection Board*** and the Commission shall encourage, in particular at ~~European~~ ***Union*** level, the establishment of data protection certification mechanisms and of data protection seals and marks, ***for the purpose of demonstrating***	

[272] ***AT, FR, FI scrutiny reservation. FR thought the terminology used was unclear an that the DPA should be in a position to check compliance with certified data protection policies; this should be clarified in Article 53.***

processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.		***compliance with this Regulation of processing operations carried out*** ~~allowing data subjects to quickly assess the level of data protection provided~~ by controllers and processors. The ~~data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the~~ specific ~~features of the various sectors and different processing operations~~***needs of micro, small and medium-sized entreprises shall be taken into account***.	
		1a. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 2a may also be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation according to Article 3 within the framework of personal data transfers to third countries or international organisations under	

		the terms referred to in Article 42(2)(e). Such controllers or processors shall make binding and enforceable commitments, via contractual instruments or otherwise, to apply those appropriate safeguards, including as regards data subjects' rights.	
	1a. Any controller or processor may request any supervisory authority in the Union, for a reasonable fee taking into account the administrative costs, to certify that the processing of personal data is performed in compliance with this Regulation, in particular with the principles set out in Article 5, 23 and 30, the obligations of the controller and the processor, and the data subject's rights.		
	1b. The certification shall be voluntary, affordable, and available via a process that is transparent and not unduly burdensome.		
	1c. The supervisory authorities and the European Data Protection Board shall cooperate under the		

	consistency mechanism pursuant to Article 57 to guarantee a harmonised data protection certification mechanism including harmonised fees within the Union.		
	1d. During the certification procedure, the supervisory ~~authority~~ authorities may accredit specialised third party auditors to carry out the auditing of the controller or the processor on their behalf. Third party auditors shall have sufficiently qualified staff, be impartial and free from any conflict of interests regarding their duties. Supervisory authorities shall revoke accreditation, if there are reasons to believe that the auditor does not fulfil its duties correctly. The final certification shall be provided by the supervisory authority.		
	1e. Supervisory authorities shall grant controllers and processors, who pursuant to the auditing have been certified that they process personal data in compliance with this Regulation, the standardised data protection mark named		

	"European Data Protection Seal".		
	1f. The "European Data Protection Seal" shall be valid for as long as the data processing operations of the certified controller or processor continue to fully comply with this Regulation.		
	1g. Notwithstanding paragraph 1f, the certification shall be valid for maximum five years.		
	1h. The European Data Protection Board shall establish a public electronic register in which all valid and invalid certificates which have been issued in the Member States can be viewed by the publc.		
	1i. The European Data Protection Board may on its own initiative certify that a data protection-enhancing technical standard is compliant with this Regulation.		
2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification	2. The Commission shall be empowered to adopt***, after requesting an opinion of the European Data Protection Board and consulting with stakeholders, in particular industry and non-***	***Moved and modified underArticle 39 point 7***	

mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.	***governmental organisations,*** delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in ~~paragraph 1~~***paragraphs 1a to 1h***, including ***requirements for accreditation of auditors,*** conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries. ***Those delegated acts shall confer enforceable rights on data subjects***.		
		2. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.	
		2a. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 39a, or where applicable, by the competent supervisory	

		authority on the basis of the criteria approved by the competent supervisory authority or, pursuant to Article 57, the European Data Protection Board[273].	
3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	***deleted***	***Moved under 39a point 8.***	
		3. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 39a, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.	

[273] ***This is without prejudice to the future discussion on the exact powers of the EDPB. This discussion will take place in the context of the discussion on the one-stop-shop mechanism.***

		4. The certification shall be issued to a controller or processor for a maximum period of 3 years and may be renewed under the same conditions as long as the relevant requirements continue to be met. It shall be withdrawn by the certification bodies referred to in Article 39a, or where applicable, by the competent supervisory authority where the requirements for the certification are not or no longer met.	
		5. The European Data Protection Board shall collect all certification mechanisms and data protection seals in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.	
		Article 39a	
		Certificationbody and procedure[274]	
		1. Without prejudice to the tasks and powers of the competent	

[274] ***AT, FR, LU scrutiny reservation.***

		supervisory authority under Articles 52 and 53, the certification shall be issued and renewed by a certification body which has an appropriate level of expertise in relation to data protection. Each Member State shall provide whether these certification bodies are accredited by:	
		(a) the supervisory authority which is competent according to Article 51 or 51a; and/or	
		(b) the National Accreditation Body named in accordance with Regulation (EC) 765/2008 of the European parliament and the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products in compliance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent according to Article 51 or 51a.	
		2. The certification body referred to in paragraph 1 may be	

		accredited for this purpose only if:	
		(a) it has demonstrated its independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;	
		(aa) it has undertaken to respect the criteria referred to in paragraph 2a of Article 39 and approved by the supervisory authority which is competent according to Article 51 or 51a or , pursuant to Article 57, the European Data Protection Board;	
		(b) it has established procedures for the issue, periodic review and withdrawal of data protection seals and marks;	
		(b) it has established procedures and structures to deal with complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make these procedures and structures	

		transparent to data subjects and the public;	
		(c) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.	
		3. The accreditation of the certification bodies referred to in paragraph 1 shall take place on the basis of criteria approved by the supervisory authority which is competent according to Article 51 or 51a or, pursuant to Article 57, the European Data Protection Board[275]. In case of an accreditation pursuant to point (b) of paragraph 1, these requirements complement those envisaged in Regulation 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.	
		4. The certification body referred to in paragraph 1 shall be responsible for the proper	

[275] ***This is without prejudice to the future discussion on the exact powers of the EDPB. This discussion will take place in the context of the discussion on the one-stop-shop mechanism.***

		assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation is issued for a maximum period of five years and can be renewed in the same conditions as long as the body meets the requirements.	
		5. The certification body referred to in paragraph 1 shall provide the competent supervisory authority with the reasons for granting or withdrawing the requested certification.	
		6. The requirements referred to in paragraph 3, the criteria referred to in paragraph 2a of Article 39 shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit these to the European Data Protection Board. The European Data Protection Board shall collect all certification mechanisms and data protection	

		seals in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.	
		6a. Without prejudice to the provisions of Chapter VIII, the competent supervisory authority or the National Accreditation Body shall revoke the accreditation it granted to a certification body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation[276].	
		7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86, for the purpose of specifying the criteria and requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1, [including contions	

[276] ***CZ, FR and HU though the national accreditation body should always consult the DPA before accrediting a certification body.***

		for granting and revocation, and requirements for recognition of the certification and the requirements for a standardised 'European Data Protection Seal' within the Union and in third countries].	
		7a. The European Data Protection Board shall give an opinion to the Commission on the criteria and requirements referred to in paragraph 7[277].	
3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	***deleted***	***8.*** The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2)[278].	

[277] ***This is without prejudice to the future discussion on the exact powers of the EDPB. This discussion will take place in the context of the discussion on the one-stop-shop mechanism.***

[278] ***DE pleaded in favour of deleting the last two paragraphs and suggested adding a new paragraph: "The previous paragraphs shall not affect provisions governing the responsibility of national certification bodies, the accreditation procedures and the specification of criteria for security and data protection. Commission's power to adopt acts pursuant to paragraphs 7 and 8 shall not apply to national and international certification procedures carried out on this basis. Security certificates issued by the responsible bodies or bodies accredited by them in the framework of these procedures shall be mutually recognized." ES also thought that this should not be left exclusively to the Commission.***

CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS	CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS	CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS[279] [280] [281] [282]	
Article 40	***Article 40***	***Article 40***	
General principle for transfers	***General principle for transfers***	***General principle for transfers***	
Any transfer of personal data which are undergoing processing or are intended for processing after	Any transfer of personal data which are undergoing processing or are intended for processing after	***deleted***	

[279] ***In light of the fact that the public interest exception would in many cases be the main ground warranting an international transfer of personal data, some delegations (CZ, DE, LV, UK) queried whether the 'old' adequacy principle/test should still maintained and set out in such detail, as it would in practice not be applied in that many cases. DE in particular thought that the manifold exceptions emptied the adequacy rule of its meaning. Whilst they did not disagree with the goal of providing protection against transfer of personal data to third countries, it doubted whether the adequacy principle was the right procedure therefore, in view of the many practical and political difficulties (the latter especially regarding the risk of a negative adequacy decision, cf. DE, FR, UK). The feasibility of maintaining an adequacy-test was also questioned with reference to the massive flows of personal data in in the context of cloud computing: BG, DE, FR, IT, NL, SK and UK. FR and DE asked whether a transfer of data in the context of cloud computing or the disclosure of personal data on the internet constitutes an international transfer of data. DE also thought that the Regulation should create a legal framework for 'Safe Harbor-like' arrangements under which certain guarantees to which companies in a third country have subscribed on a voluntary basis are monitored by the public authorities of that country. The applicability to the public sector of the rules set out in this Chapter was questioned (EE), as well as the delimitation to the scope of proposed Directive (FR). The impact of this Chapter on existing Member State agreements was raised by several delegations (FR, PL).***

[280] ***NL and UK pointed out that under the 1995 Data Protection Directive the controller who wants to transfer data is the first one to assess whether this possible in under the applicable (EU) law and they would like to maintain this basic principle, which appears to have disappeared in the Commission proposal.***

[281] ***DE asked which law would apply to data transferred controllers established in third countries that come within the ambit of Article 3(2); namely whether this would be EU law in accordance with that provision.***

[282] ***AT has made a number of proposals regarding this chapter set out in 10198/14 DATAPROTECT 82 JAI 363 MI 458 DRS 73 DAPIX 71 FREMP 103 COMIX 281 CODEC 1351.***

transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.	transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.		
Article 41	***Article 41***	***Article 41***	
Transfers with an adequacy decision	***Transfers with an adequacy decision***	***Transfers with an adequacy decision***[283]	
	Amendment 137		
1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an	1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an	1. A transfer ***of personal data to a third country or an international organisation*** may take place where the Commission[284] has decided that the third country, or a territory or ***oner***	

[283] ***Some delegations raised concerns on the time taken up by adequacy procedures and stressed the need to speed up this process. COM stated that this should not be at the expense of the quality of the process of adequacy.***

[284] ***CZ, DE and SI reservation on giving such power to the Commission. NL and UK indicated that on this point the proposal seemed to indicate a shift from the 1995 Data Protection Directive, which put the responsibility for assessing a third country's data protection legislation in the first place with the controller who wanted to transfer personal data. UK had considerable doubts on the feasibility of the list in paragraph 2.***

adequate level of protection. Such transfer shall not require any further authorisation.	adequate level of protection. Such transfer shall not require any ~~further~~***specific*** authorisation.	***or more specified*** ~~a processing~~ sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any ~~further~~ ***specific*** authorisation.	
2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:	2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:	2. When assessing the adequacy of the level of protection, the Commission shall***, in particular, take account of*** ~~give consideration to~~ the following elements:	
(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being	(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law ***as well as the implementation of this legislation***, the professional rules and security measures which are complied with in that country or by that international organisation, ***jurisprudential precedents,*** as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data	(a) the rule of law, ***respect for human rights and fundamental freedoms,*** relevant legislation~~ in force~~[285], both general and sectoral, ***data protection*** ~~including concerning public security, defence, national security and criminal law, the professional~~ rules and security measures***, including rules for onward transfer of personal data to another third country or international organisation,*** which are complied with in that country or ~~by that~~ international organisation, as well	

[285] ***AT would have preferred including a reference to national security.***

transferred;	subjects residing in the Union whose personal data are being transferred;	as ***the existences of*** effective and enforceable ***data subject*** rights ~~including~~ ***and*** effective administrative and judicial redress for data subjects~~, in particular for those data subjects residing in the Union~~ whose personal data are being transferred[286];	
(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and	(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, ***including sufficient sanctioning powers***, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and	(b) the existence and effective functioning of one or more independent supervisory authorities[287] in the third country or ***to which an*** international organisation ~~in question~~ ***is subject, with*** responsib~~le~~***ility*** for ensuring ***and enforcing*** compliance with the data protection rules ***including adequate sanctioning powers*** for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States;~~ and~~	
(c) the international commitments the third country or	(c) the international commitments the third country or international	(c) the international commitments the third country or	

[286] ***NL thought that Article 41 was based on fundamental rights and legislation whereas Safe harbour is of a voluntary basis and that it was therefore useful to set out elements of Safe Harbour in a separate Article. DE asked how Safe Harbour could be set out in Chapter V.***

[287] ***NL queried how strict this independence would need to be assessed. BE suggested adding a reference to independent judicial authorities, FI suggested to refer to 'authorities' tout court.***

international organisation in question has entered into.	organisation in question has entered into***, in particular any legally binding conventions or instruments with respect to the protection of personal data***.	international organisation ~~in question~~ ***concerned*** has entered into ***or other obligations arising from its participation in multilateral or regional systems, in particular in relation to the protection of personal data***.	
		2a. The European Data Protection Board shall give the Commission an opinion[288] for the assessment of the adequacy of the level of protection in a third country or international organization, including for the assessment whether a third country or the territory or the international organization or the specified sector no longer ensures an adequate level of protection.	
3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an	3. The Commission ~~may~~***shall be empowered to adopt delegated acts in accordance with Article 86 to*** decide that a third country, or a	3. The Commission, ***after assessing the adequacy[289] of the level of protection,*** may decide that a third country, or a territory or ***one or***	

288 ***CZ would prefer stronger language on the COM obligation to request an opinion from the EDPB.***

289 ***CZ, RO and SI reservation on giving such power to the Commission. DE thought that stakeholders should be involved in this process. NL and UK indicated that on this point the proposal seemed to indicate a shift from the 1995 Data Protection Directive, which put the responsibility for assessing a third country's data protection legislation in the first place with the controller who wanted to transfer personal data.***

international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. ~~Those implementing acts~~ ***Such delegated acts*** shall ~~be adopted in accordance with the examination procedure referred to in Article 87(2)~~ ***provide for a sunset clause if they concern a processing sector and shall be revoked according to paragraph 5 as soon as an adequate level of protection according to this Regulation is no longer ensured.***	***more specified*** ~~a processing~~ sectors within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2[290]. Th~~os~~e implementing act~~s~~ ***shall specify its territorial and sectoral application and, where applicable, identify the (independent) supervisory authority(ies) mentioned in point(b) of paragraph 2. The implementing act*** shall be adopted in accordance with the examination procedure referred to in Article 87(2)[291].	
		3a. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission[292] in accordance with	

[290] ***CZ, DE, DK, HR, IT, NL, PL, SK and RO thought an important role should be given to the EDPB in assessing these elements.COM has pointed out that there can be no additional step in the Comitology procedure, in order to be in line with the Treaties and Regulation 182/2011.***

[291] ***DE queried the follow-up to such decisions and warned against the danger that third countries benefiting from an adequacy decision might not continue to offer the same level of data protection. COM indicated there was monitoring of third countries for which an adequacy decision was taken.***

[292] ***Moved from paragraph 8. CZ and AT thought an absolute maximum time period should be set (sunset clause), to which COM was opposed. NL, PT and SI thought this paragraph 3a was superfluous or at least unclear. Also RO thought that, if maintained, it should be moved to the end of the Regulation.***

		the examination procedure referred to in Article 87(2)[293].	
4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.	4. The ~~implementing~~***delegated*** act shall specify its ~~geographical~~***territorial*** and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.	***deleted***	
	4a. The Commission shall, on an on-going basis, monitor developments in third countries and international organisations that could affect the elements listed in paragraph 2 where a delegated act pursuant to paragraph 3 has been adopted.	***4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC[294].***	
5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of	5. The Commission ~~may~~***shall be empowered to adopt delegated acts in accordance with Article 86 to*** decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not	5. The Commission may decide that a third country, or a territory or a ~~processing~~ ***specified*** sector within that third country, or an international organisation ~~does not~~ ***no longer*** ensure***s*** an adequate level of protection within the meaning of	

293 ***DE and ES suggested to request the Board for an opinion. COM has pointed out that there can be no additional step in the Comitology procedure, in order to be in line with the Treaties and Regulation 182/2011. DE asked if a decision in paragraph 3a lasted forever. IE considered paragraph 3a providing necessary flexibility. CZ thought that new States should not be disadvantaged compared to those having received an adequacy decision under Directive 1995.***

294 ***BE queried about the reference to the 1995 Directive. CZ perceives this as superfluous.***

paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).	ensure ***or no longer ensures*** an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).~~	paragraph 2 ***and may, where necessary, repeal, amend or suspend such decision without retro-active effect*** ~~of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred~~. Th~~os~~e implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency ~~for individuals with respect to their right to personal data protection~~, in accordance with the procedure referred to in Article 87(3).[295]	
6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third	6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third	6. ~~Where the Commission decides~~***A decision*** pursuant to paragraph 5~~, any~~ ***is wihtout prejudice to*** transfer***s*** of personal data to the third country, or ~~a~~ ***the***	

[295] ***FR and UK suggested the EDPB give an opinion before COM decided to withdraw an adequacy decision.***

country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.	country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the ~~Decision~~ ***decision*** made pursuant to paragraph 5 of this Article.	territory or ~~a processing~~ ***specified*** sector within that third country, or the international organisation in question ~~shall be prohibited, without prejudice~~ ***pursuant*** to Articles 42 to 44[296]. ~~At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.~~	
	6a. Prior to adopting a delegated act pursuant to paragraphs 3 and 5, the Commission shall request the European Data Protection Board to provide an opinion on the adequacy of the level of protection. To that end, the Commission shall provide the European Data Protection Board with all necessary documentation, including correspondence with the government of the third country, territory or processing sector within that third country or the international organisation.		

[296] ***DE asked for the deletion of paragraph 6. DK thought the moment when third countries should be consulted was unclear.***

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.	7. The Commission shall publish in the *Official Journal of the European Union* ***and on its website*** a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.	7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and ~~processing~~ ***specified*** sectors within a third country and international organisations ~~where it has decided that an adequate level of protection is or is not ensured~~ ***in respect of which decisions have been taken pursuant to paragraphs 3, 3a and5***.	
8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission.	8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until ***five years after the entry into force of this Regulation unless*** amended, replaced or repealed by the Commission ***before the end of this period.***	***deleted***	

Article 42	*Article 42*	*Article 42*	
Transfers by way of appropriate safeguards	***Transfers by way of appropriate safeguards***	***Transfers by way of appropriate safeguards***[297]	
	Amendment 138		
1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.	1. Where the Commission has taken no decision pursuant to Article 41, ***or decides that a third country, or a territory or processing sector within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 41(5),*** a controller or processor may ***not*** transfer personal data to a third country, territory or an international organisation ***unless*** the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.	1. ~~Where the Commission has taken no~~ ***In the absence of***decision pursuant to ***paragraph 3 of*** Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards~~ with respect to the protection of personal data in a legally binding instrument~~***, also covering onward transfers***.	
2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:	2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:	2. The appropriate safeguards referred to in paragraph 1 ~~shall~~ ***may*** be provided for, ~~in particular~~***without requiring any***	

[297] ***UK expressed concerns regarding the length of authorisation procedures and the burdens these would put on DPA resources. The use of these procedures regarding data flows in the context of cloud computing was also questioned.***

		specific authorisation from a supervisory authority, by:	
		(oa) a legally binding <u>and</u> enforceable instrument between public authorities or bodies[298]; or	
(a) binding corporate rules in accordance with Article 43; or	(a) binding corporate rules in accordance with Article 43; or	(a) binding corporate rules ~~in accordance with~~ ***referred to in*** Article 43; or	
	(aa) a valid "European Data Protection Seal" for the controller and the recipient in accordance with paragraph 1e of Article 39; or		
(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or	***deleted***	(b) standard data protection clauses adopted by the Commission~~. Those implementing acts shall be adopted~~ in accordance with the examination procedure referred to in Article 87(2)[299]; or	
(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to	(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57	(c) standard data protection clauses adopted by a supervisory authority ~~in accordance with the consistency mechanism referred to in Article 57~~	

[298] ***HU has serious concerns; the proposed general clause ("a legally binding instrument") is too vague because the text does not define its content. Furthermore, the text does not provide for previous examination by the DPA either. HU therefore suggests either deleting this point or subjecting such instrument to the authorisation of the DPA, as it believes that there is a real risk that transfers based on such a vague instrument might seriously undermine the rights of the data subjects.***

[299] ***FR reservation on the possibility for COM to adopt such standard clauses.***

in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or	when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or	~~when declared generally valid~~ ***and adopted*** by the Commission pursuant to ~~point (b) of Article 62(1)~~***the examination procedure referred to in Article 87(2)***; or	
(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.	(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.	(d) ~~contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.~~***an approved code of conduct pursuant to Article 38 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights ; or***	
		(e) an approved certification mechanism pursuant to Article 39 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.	
		2a. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in	

		paragraph 1 may also be provided for, in particular, by: ***(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the data in the third country or international organisation; or*** ***(b) (…)*** ***(c) (…)*** ***(d) provisions to be inserted into administrative arrangements between public authorities or bodies .***	
3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.	3. A transfer based on standard data protection clauses***, a "European Data Protection Seal"*** or binding corporate rules as referred to in point (a), ~~(b)~~ ***(aa)*** or (c) of paragraph 2 shall not require any ~~further~~***specific*** authorisation.	***deleted***	
4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the	4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses ~~according to point (a) of Article 34(1)~~ from the	***deleted***	

supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.	supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.		
5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free	5. ~~Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within~~	***deleted***	

movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.	~~the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.~~ Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid~~,~~ until ***two years after the entry into force of this Regulation unless*** amended, replaced or repealed by that supervisory authority ***before the end of that period.***		
		5a. The supervisory authority shall apply the consistency mechanism in the cases referred to in points (ca), (d), (e) and (f) of Article 57 (2).	
		5b. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed by that supervisory authority[300]. Decisions adopted by the Commission on the basis of Article 26(4) of Directive	

[300] ***UK and ES disagreed with the principle of subjecting non-standardised contracts to prior authorisation by DPAs. IT was thought that this was contrary to the principle of accountability. DE emphasised the need of monitoring.***

		95/46/EC shall remain in force until amended, replaced or repealed by the Commission[301] in accordance with the examination procedure referred to in Article 87(2)[302].	
Article 43	***Article 43***	***Article 43***	
Transfers by way of binding corporate rules	***Transfers by way of binding corporate rules***	***~~Transfers by way of b~~Binding corporate rules[303]***	
	Amendment 139		
1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:	1. ~~A~~***The*** supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:	1. ~~A~~ ***The competent*** supervisory authority shall ***approve***[304] ***binding corporate rules*** in accordance with the consistency mechanism set out in Article ~~58~~***57*** ~~approve binding corporate rules~~, provided that they:	
(a) are legally binding and apply to and are enforced by every member within the controller's or	(a) are legally binding and apply to and are enforced by every member within the controller's group of	(a) are legally binding and apply to and are enforced by every member ***concerned of the*** ~~within the~~	

301 ***AT thought an absolute time period should be set.***

302 ***DE and ES have suggested to request the Board for an opinion. COM has pointed out that there can be no additional step in the Comitology procedure, in order to be in line with the Treaties and Regulation 182/2011.***

303 ***NL thought it should be given a wider scope. BE and NL pointed to the need for a transitional regime allowing to 'grandfather' existing BCRs. NL asked whether the BCRs should also be binding upon employees. SI thought BCRs should also be possible with regard to some public authorities, but COM stated that it failed to see any cases in the public sector where BCRs could be applied. HU said that it thought that BCRs were used not only by profit-seeking companies but also by international bodies and NGOs.***

304 ***DE and UK expressed concerns on the lengthiness and cost of such approval procedures. The question was raised which DPAs should be involved in the approval of such BCRs in the consistency mechanism.***

processor's group of undertakings, and include their employees;	undertakings ***and those external subcontractors that are covered by the scope of the binding corporate rules***, and include their employees;	~~controller's or processor's~~ group of undertakings ***or group of enterprises engaged in a joint economic activity***~~, and include their employees~~;	
(b) expressly confer enforceable rights on data subjects;	(b) expressly confer enforceable rights on data subjects;	(b) expressly confer enforceable rights on data subjects ***with regard to the processing of their personal data***;	
(c) fulfil the requirements laid down in paragraph 2.	(c) fulfil the requirements laid down in paragraph 2	(c) fulfil the requirements laid down in paragraph 2.	
	1a. With regard to employment data, the representatives of the employees shall be informed about and, in accordance with Union or Member State law and practice, be involved in the drawing-up of binding corporate rules pursuant to Article 43.		
2. The binding corporate rules shall at least specify:	2. The binding corporate rules shall at least specify.	2. The binding corporate rules ***referred to in paragraph 1*** shall ~~at least~~ specify at least :	
(a) the structure and contact details of the group of undertakings and its members;	(a) the structure and contact details of the group of undertakings and its members ***and those external subcontractors that are covered by the scope of the binding corporate***	(a) the structure and contact details of the ***concerned*** group ~~of undertakings~~ and ***of each of*** its members;	

	rules;		
(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;	(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;	(b) the data transfers or ~~set~~ ***categories*** of transfers, including the ~~categories~~ ***types*** of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;	
(c) their legally binding nature, both internally and externally;	(c) their legally binding nature, both internally and externally;	(c) their legally binding nature, both internally and externally;	
(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;	(d) the general data protection principles, in particular purpose limitation, ***data minimisation, limited retention periods,*** data quality, ***data protection by design and by default,*** legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;	(d) ***application of*** the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of ~~sensitive~~ ***special categories of*** personal data~~;~~**,** measures to ensure data security~~;~~**,** and the requirements ~~for~~ ***in respect of*** onward transfers to ~~organisations~~ ***bodies*** ~~which are~~ not bound by the ~~policies~~***binding corporate rules***;	
(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article	(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the	(e) the rights of data subjects ***in regard to the processing of their personal data*** and the means to exercise these rights, including the right not to be subject to ~~a measure~~	

20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;	right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;	~~based on~~ profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;	
(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;	(f) the acceptance by the controller ~~or processor~~ established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller ~~or the processor~~ may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;	(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member ***concerned*** ~~of the group of undertakings~~ not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, ~~if he proves~~ ***on proving*** that that member is not responsible for the event giving rise to the damage[305];	
(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this	(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this	(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this	

[305] ***DE thought that the reference to exemptions should be deleted here.***

paragraph is provided to the data subjects in accordance with Article 11;	paragraph is provided to the data subjects in accordance with Article 11;	paragraph is provided to the data subjects in accordance with Articles ~~11~~14 and 14a;	
(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;	(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;	(h) the tasks of ~~the~~ ***any*** data protection officer designated in accordance with Article 35 ***or any other person or entity in charge of the*** ~~, including~~ monitoring ~~within the group of undertakings the~~ compliance with the binding corporate rules ***within the group***, as well as monitoring the training and complaint handling;	
		(hh) the complaint procedures;	
(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;	(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;	(i) the mechanisms within the group ~~of undertakings aiming at~~ ***for*** ensuring the verification of compliance with the binding corporate rules***. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred under point h) and to the board of the controlling undertaking or of the group of enterprises, and should be***	

		available upon request to the competent supervisory authority;	
(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;	(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;	(j) the mechanisms for reporting and recording changes to the ~~policies~~ ***rules*** and reporting these changes to the supervisory authority;	
(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.	(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.	(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group ~~of undertakings~~, in particular by making available to the supervisory authority the results of ~~the~~ verifications of the measures referred to in point (i) of this paragraph***;***[306]	
		(l) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules[307]***; and***	

[306] ***BE suggested making this more explicit in case of a conflict between the 'local' legislation applicable to a member of the group and the BCR.***

[307] ***CZ expressed concerns about the purpose of this provision and its application. UK found this point very prescriptive and wanted BCRs to be flexible to be able to be used for different circumstances.***

		(m) the appropriate data protection training to personnel having permanent or regular access to personal data (...).	
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.	3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the ***format, procedures,*** criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, ***including transparency for data subjects,*** the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.	***[***3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.***]***[308]	
4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding	***deleted***	4. The Commission may specify the format and procedures for the exchange of information ~~by electronic means~~ between controllers, processors and supervisory authorities for binding	

[308] ***CZ, IT, SE and NL reservation. FR scrutiny reservation regarding (public) archives. RO and HR thought the EDPB should be involved. PL and COM wanted to keep paragraph 3.***

corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).		corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	
	Amendment 140		
	Article 43a (new)		
	Transfers or disclosures not authorised by Union law		
	1. No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognised or be enforceable in any manner, without prejudice to a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.		
	2. Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data,		

	the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer or disclosure by the supervisory authority.		
	3. The supervisory authority shall assess the compliance of the requested disclosure with the Regulation and in particular whether the disclosure is necessary and legally required in accordance with points (d) and (e) of Article 44(1) and Article 44(5). Where data subjects from other Member States are affected, the supervisory authority shall apply the consistency mechanism referred to in Article 57.		
	4. The supervisory authority shall inform the competent national authority of the request. Without prejudice to Article 21, the controller or processor shall also inform the data subjects of the request and of the authorisation by the supervisory authority and		

	where applicable inform the data subject whether personal data was provided to public authorities during the last consecutive 12-month period, pursuant to point (ha) of Article 14(1).		
Article 44	***Article 44***	***Article 44***	
Derogations	~~***Derogations***~~	***Derogations for specific situations***[309]	
	Amendment 141		
1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:	1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:	1. In the absence of an adequacy decision pursuant to ***paragraph 3 of*** Article 41**,** or of appropriate safeguards pursuant to Article 42, ***including binding corporate rules*** a transfer or a ~~set~~ ***category*** of transfers of personal data to a third country or an international organisation may take place only on condition that:	
(a) the data subject has consented to the proposed transfer, after having been informed of the	(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such	(a) the data subject has ***explicitly***[310] consented to the proposed transfer, after having been informed ~~of the~~	

[309] ***EE reservation. NL parliamentary reservation. CZ, EE and UK and other delegations that in reality these 'derogations' would become the main basis for international data transfers and this should be acknowledged as such by the text of the Regulation.***

[310] ***UK thought the question of the nature of the consent needed to be discussed in a horizontal manner.***

risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or	transfers due to the absence of an adequacy decision and appropriate safeguards; or	~~risks of~~ ***that*** such transfers ***may involve risks for the data subject*** due to the absence of an adequacy decision and appropriate safeguards; or	
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or	(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or	(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or	
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or	(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or	(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or	
(d) the transfer is necessary for important grounds of public interest; or	(d) the transfer is necessary for important grounds of public interest; or	(d) the transfer is necessary for important ~~grounds~~ ***reasons*** of public interest[311]; or	
(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or	(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or	(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or	

[311] ***DE remarked that the effects of (d) in conjunction with paragraph 5 need to be examined, in particular with respect to the transfer of data on the basis of court judgments and decisions by administrative authorities of third states, and with regard to existing mutual legal assistance treaties. IT reservation on the (subjective) use of the concept of public interest. HR suggested adding 'which is not overridden by the legal interest of the data subject'.***

(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or	(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or	(f) the transfer is necessary in order to protect the vital interests of the data subject or of ~~an~~other persons, where the data subject is physically or legally incapable of giving consent; or	
(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or	(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case**.**	(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate ***a*** legitimate interest~~,~~ ***but only*** to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or	
(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or	***deleted***	(h) the transfer***, which is not large scale or frequent***[312]**,** is necessary for the purposes of the legitimate interests pursued by the controller ***which are not oveerriden by the interests or rights and freedoms of***	

[312] ***AT, ES, HU, MT, PL, PT and SI would prefer to have this derogation deleted as they think it is too wide; it was stated that data transfers based on the legitimate interest of the data controller and directed into third countries that do not provide for an adequate level of protection with regard to the right of the data subjects would entail a serious risk of lowering the level of protection the EU acquis currently provides for.) DE and ES scrutiny reservation on the terms 'frequent or massive'. DE, supported by SI, proposed to narrow it by referring to 'overwhelming legitimate interest'. ES proposed to replace it by 'are small-scale and occasional'; UK asked why it was needed to add another qualifier to the legitimate interest of the transfer and thought that such narrowing down of this derogation was against the risk-based approach.***

processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.		***the data subject*** ~~or the processor, which cannot be qualified as frequent or massive,~~ and where the controller ~~or processor~~ has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced ~~appropriate~~ ***suitable*** safeguards[313] with respect to the protection of personal data~~, where necessary~~.	
2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.	2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.	2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.	
3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing	***deleted***	***deleted***	

---

[313] ***AT and NL reservation: it was unclear how this reference to appropriate safeguards relates to appropriate safeguards in Article 42.***

operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.			
4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.	4. Points (b)~~,~~ ***and*** (c) ~~and (h)~~ of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.	4. Points ***(a),*** (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers[314].	
5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.	5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.	5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the ***national*** law of the Member State to which the controller is subject.	
		5a. In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or	

[314] ***BE scrutiny reservation. FR has a reservation concerning the exception of public authorities.***

		an international organisation[315]. Member States shall notify such provisions to the Commission[316].	
6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.	***deleted***	6. The controller or processor shall document the assessment as well as the ~~appropriate~~ ***suitable*** safeguards ~~adduced~~ referred to in point (h) of paragraph 1 ~~of this Article~~ in the ~~documentation~~ ***recoreds*** referred to in Article 28~~ and shall inform the supervisory authority of the transfer~~.	
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.	7. The ~~Commission~~ ***European Data Protection Board*** shall be ~~empowered to adopt delegated acts in accordance with Article 86~~ ***entrusted with the task of issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1)*** for the purpose of further specifying ~~'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as~~ the criteria and requirements for ~~appropriate safeguards referred to in~~	***deleted***	

315 ***SI and UK scrutiny reservation. FR and ES proposed that this provision should be included in another provision.***

316 ***Some delegations (FR, PL, SI) referred to the proposal made by DE (for new Article 42a: 12884/13 DATAPROTECT 117 JAI 689 MI 692 DRS 149 DAPIX 103 FREMP 116 COMIX 473 CODEC 186) and the amendment voted by the European Parliament (Article 43a), which will imply discussions at a later stage.***

	~~point (h)~~ ***data transfers on the basis*** of paragraph 1.		
Article 45	***Article 45***	***Article 45***	
International co-operation for the protection of personal data	***International co-operation for the protection of personal data***	***International co-operation for the protection of personal data***[317]	
	Amendment 142		
1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:	1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:	1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:	
(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;	(a) develop effective international co-operation mechanisms to ~~facilitate~~ ***ensure*** the enforcement of legislation for the protection of personal data;	(a) develop ~~effective~~ international co-operation mechanisms to facilitate the ***effective*** enforcement of legislation for the protection of personal data;	
(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and	(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and	(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through ~~notification,~~ complaint referral, investigative assistance and	

[317] ***PL thought (part of) Article 45 could be inserted into the preamble. NL, RO and UK also doubted the need for this article in relation to adequacy and thought that any other international co-operation between DPAs should be dealt with in Chapter VI. NL thought this article could be deleted. ES has made an alternative proposal, set out in 6723/6/13 REV 6 DATAPROTECT 20 JAI 130 MI 131 DRS 34 DAPIX 30 FREMP 15 COMIX 111 CODEC 394.***

information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;	information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;	information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms[318];	
(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;	(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;	(c) engage relevant stakeholders in discussion and activities aimed at ~~furthering~~ ***promoting*** international co-operation in the enforcement of legislation for the protection of personal data;	
(d) promote the exchange and documentation of personal data protection legislation and practice.	d) promote the exchange and documentation of personal data protection legislation and practice~~.~~**;**	(d) promote the exchange and documentation of personal data protection legislation and practice.	
	Amendment 143		
	(da) clarify and consult on jurisdictional conflicts with third countries.		
2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission	2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission	***deleted***	

[318] ***AT and FI thought this subparagraph was unclear and required clarification.***

has decided that they ensure an adequate level of protection within the meaning of Article 41(3).	has decided that they ensure an adequate level of protection within the meaning of Article 41(3).		
	Amendment 144		
	Article 45a (new)		
	Report by the Commission		
	The Commission shall submit to the European Parliament and the Council at regular intervals, starting not later than four years after the date referred to in Article 91(1), a report on the application of Articles 40 to 45. For that purpose, the Commission may request information from the Member States and supervisory authorities, which shall be supplied without undue delay. The report shall be made public.		

CHAPTER VI INDEPENDENT SUPERVISORY AUTHORITIES	CHAPTER VI INDEPENDENT SUPERVISORY AUTHORITIES	CHAPTER VI INDEPENDENT SUPERVISORY AUTHORITIES	
SECTION 1 INDEPENDENT STATUS	**SECTION 1 INDEPENDENT STATUS**	**SECTION 1 INDEPENDENT STATUS**	
Article 46	***Article 46***	***Article 46***	
Supervisory authority	***Supervisory authority***	***Supervisory authority***[319]	
1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-	1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with	1. Each Member State shall provide that one or more ***independent*** public authorities are responsible for monitoring the application of this Regulation ~~and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-~~	

[319] ***At the request of IT, COM clarified that this DPA could be the same as the one designated/set up under the future Data Protection Directive. ES asked for clarification that a DPA may be composed of more members, but t this is already sufficiently clear from the current text. DE indicated that it would require an intra-German consistency mechanism between the its various DPAs.***

operate with each other and the Commission.	each other and the Commission.	~~operate with each other and the Commission~~.	
		1a Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For this purpose, the supervisory authorities shall co-operate with each other and the Commission in accordance with Chapter VII.	
2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57.	2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57.	2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which ~~functions as a single contact point for the effective participation of~~ ***shall represent*** those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57.	
3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at	3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the	***[***3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at	

the latest and, without delay, any subsequent amendment affecting them.	latest and, without delay, any subsequent amendment affecting them.	the latest and, without delay, any subsequent amendment affecting them[320].]	
Article 47	***Article 47***	***Article 47***	
Independence	***Independence***	***Independence***	
	Amendment 145		
1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it.	1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it***, notwithstanding co-operative and consistency arrangements related to Chapter VII of this Regulation***.	1. ~~The~~ ***Each*** supervisory authority shall act with complete independence in ***performing the duties[321] and*** exercising the ~~duties and~~ powers entrusted to it ***in accordance with this Regulation.***.	
2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.	2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.	2. The ***member or*** members of ~~the~~ ***each*** supervisory authority shall, in the performance of their duties ***and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect~~,~~ and*** neither seek nor take instructions from anybody[322].	

320 ***DE, FR and EE that thought that this paragraph could be moved to the final provisions.***

321 ***GR scrutiny reservation.***

322 ***IE reservation: IE thought the latter part of this paragraph was worded too strongly.***

3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.	3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.	***deleted***[323]	
4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.	4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.	***deleted***[324]	
5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board.	5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board.	5. Each Member State shall ensure that ~~the~~ ***each*** supervisory authority is provided with the ~~adequate~~ human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and ***exercise of its*** powers, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board.	

[323] ***AT, BE, DE and HU would prefer to reinstate this text. CZ, EE and SE were satisfied with the deletion.***

[324] ***COM and DE, AT reservation on deletion of paragraphs 3 and 4.***

6. Each Member State shall ensure that the supervisory authority has its own staff which shall be appointed by and be subject to the direction of the head of the supervisory authority.	6. Each Member State shall ensure that the supervisory authority has its own staff which shall be appointed by and be subject to the direction of the head of the supervisory authority.	6. Each Member State shall ensure that ~~the~~ ***each*** supervisory authority has its own staff which shall be ~~appointed by and be~~ subject to the direction of the ***member or members*** ~~head~~ of the supervisory authority.	
7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.	7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.	7. Member States shall ensure that ~~the~~ ***each*** supervisory authority is subject to financial control[325] which shall not affect its independence. Member States shall ensure that ~~the~~ ***each*** supervisory authority has separate***, public,*** annual budgets***, which may be part of the overall state or national budget***. ~~The budgets shall be made public.~~	
	Amendment 146		
	7a. Each Member State shall ensure that the supervisory authority shall be accountable to the national parliament for reasons of budgetary control.		

[325] ***EE reservation.***

Article 48	*Article 48*	*Article 48*	
General conditions for the members of the supervisory authority	***General conditions for the members of the supervisory authority***	***General conditions for the members of the supervisory authority***	
1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.	1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.	1. Member States shall provide that the ***member or*** members of ~~the~~ ***each*** supervisory authority must be appointed ~~either~~ by the parliament ***and/***or the government of ***head of State of*** the Member State concerned ***or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure***[326].	
2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties notably in the area of protection of personal data are demonstrated.	2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties notably in the area of protection of personal data are demonstrated.	2. The ***member or*** members shall ***have the qualifications,*** ~~be chosen from persons whose independence is beyond doubt and whose~~ experience and skills required to perform their duties ~~notably in the area of protection of personal data are demonstrated~~***and exercise their powers***.	

[326] ***Several delegations (FR, SE, SI and UK) thought that other modes of appointment should have been allowed for. FR (and RO) thought that a recital should clarify that "independent body" also covers courts.***

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5.	3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5.	3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with ~~paragraph 5~~***the law of the Member State concerned***[327].	
4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.	4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.	***deleted***	
5. Where the term of office expires or the member resigns, the member shall continue to exercise the duties until a new member is appointed.	5. Where the term of office expires or the member resigns, the member shall continue to exercise the duties until a new member is appointed.	***deleted***[328]	

[327] ***COM reservation and DE scrutiny reservation on the expression "in accordance with the law of the Member States concerned". The question is whether this means that the Member States are being granted the power to define the duties further or whether the wording should be understood as meaning that only constitutional conditions or other legal framework conditions (e.g. civil service law) should be taken into account. DE and HU also suggest that rules in the event of death or invalidity be added (see, for example, Article 42(4) of Regulation (EC) No 45/2001) as well as referring to a procedure for the nomination of a representative in case the member is prevented from performing his or her duties. CZ, NO, SE see no need for paragraph 3***

[328] ***COM, DE and AT scrutiny reservation on deletion of paragraphs 4 and 5.***

Article 49	***Article 49***	***Article 49***	
Rules on the establishment of the supervisory authority	***Rules on the establishment of the supervisory authority***	***Rules on the establishment of the supervisory authority***[329]	
Each Member State shall provide by law within the limits of this Regulation:	Each Member State shall provide by law within the limits of this Regulation:	Each Member State shall provide by law ~~within the limits of this Regulation~~***for***:	
(a) the establishment and status of the supervisory authority;	(a) the establishment and status of the supervisory authority;	(a) the establishment ~~and status~~ of ~~the~~ ***each*** supervisory authority;	
(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;	(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;	(b) the qualifications~~, experience and skills~~ required to perform the duties of the members of the supervisory authority[330];	
(c) the rules and procedures for the appointment of the members of the supervisory authority, as well the rules on actions or occupations incompatible with the duties of the office;	(c) the rules and procedures for the appointment of the members of the supervisory authority, as well the rules on actions or occupations incompatible with the duties of the office;	(c) the rules and procedures for the appointment of the ***member or*** members of ~~the~~ ***each*** supervisory authority~~, as well the rules on actions or occupations incompatible with the duties of the office~~;	
(d) the duration of the term of the members of the supervisory authority which shall be no less than four years, except for the first	(d) the duration of the term of the members of the supervisory authority which shall be no less than four years, except for the first	(d) the duration of the term of the ***member or*** members of ~~the~~ ***each*** supervisory authority which shall ***not*** be ~~no~~ less than four years,	

[329] ***AT scrutiny reservation. DE and FR queried which was the leeway given to Member States by this article as compared to the rules flowing from the previous Articles from the Regulation. Several delegations (FR, GR, SE, SI UK) thought that some of these rules, in particular those spelled out in subparagraphs (c) and (d) were too detailed.***

[330] ***IE reservation: IE thought these qualifications need not be laid down in law.***

appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;	appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;	except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;	
(e) whether the members of the supervisory authority shall be eligible for reappointment;	(e) whether the members of the supervisory authority shall be eligible for reappointment;	(e) whether***and, if so, for how many terms*** the ***member or*** members of ~~the~~ ***each***supervisory authority shall be eligible for reappointment;	
(f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority;	(f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority;	(f) the ~~regulations and common~~ conditions governing the ~~duties~~ ***obligations*** of the ***member or*** members and staff of ~~the~~ ***each*** supervisory authority***, prohibitions on actions and occupations incompatible therewith during and after the term of office and rules governing the cessation of employment***;	
(g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including in case that	(g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including in case that they	***deleted***[331]	

[331] ***CZ, DE scrutiny reservation on deletion of this point.***

they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.	no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.		
		2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their duties or exercise of their powers	
Article 50	***Article 50***	***Article 50***	
Professional secrecy	***Professional secrecy***	***Professional secrecy***[332]	
	Amendment 147		
The members and the staff of the supervisory authority shall be subject, both during and after their term of office, to a duty of professional secrecy with regard to	The members and the staff of the supervisory authority shall be subject, both during and after their term of office ***and in conformity with national legislation and***	***deleted***	

[332] ***UK pointed out that also transparency concerns should be taken into account. Many delegations (CZ, DE, FR, FI, GR, IT, SE, SI, UK) raised practical questions as to the scope and the exact implications of this article. All thought that the rules on professional secrecy should be left to national law and hence the suggestion by CZ (supported by EE, SE, SI and RO) to move this to Article 49 was followed. COM and DE scrutiny reservation on moving this provision to Article 49.***

any confidential information which has come to their knowledge in the course of the performance of their official duties.	***practice***, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties***, whilst conducting their duties with independence and transparency as set out in the Regulation.***		

SECTION 2 **DUTIES AND POWERS**	**SECTION 2** **DUTIES AND POWERS**	**SECTION 2** **~~DUTIES~~ COMPETENCE, TASKS AND POWERS**	
Article 51	***Article 51***	***Article 51***	
Competence	***Competence***	***Competence***	
	Amendment 148		
1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.	1. Each supervisory authority shall ***be competent to perform the duties and to*** exercise~~, on the territory of its own Member State,~~ the powers conferred on it in accordance with this Regulation ***on the territory of its own Member State, without prejudice to Articles 73 and 74. Data processing by a public authority shall be supervised only by the supervisory authority of that Member State.***	1. Each supervisory authority shall ***be competent to perform the tasks and*** exercise~~ on the territory of its own Member State,~~ the powers conferred on it in accordance with this Regulation on the territory of its own Member State.	
	Amendment 149		
2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is	***deleted***	2. Where the processing ~~of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is~~	

established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.		~~established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.~~ ***is carried out by public authorities or private bodies acting on the basis of points (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent***[333]***. In such cases Article 51a does not apply.***	
3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.	3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.	3. ~~The s~~Supervisory ~~authority~~ authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity[334].	
		Article 51a	

[333] ***COM opposes the exclusion of private bodies from the one-stop mechanism, pointing to the example of cross-border infrastructure provided by private bodies in the public interest. AT, IE, FR and FI preferred to refer to ' processing carried out by public authorities and bodies of a Member State or by private bodies acting on the basis of a legal obligation to discharge functions in the public interest'.***

[334] ***FR, HU, RO and UK scrutiny reservation. DE suggested adding "other matters assigned to courts for independent performance. The same shall apply insofar as judicially independent processing has been ordered, approved or declared admissible", as the derogation must apply whenever courts' work falls within the scope of their institutional independence, which is not only the case in the core area of judicial activity but also in areas where courts are assigned tasks specifically for independent performance.***

		Competence of the lead supervisory authority	
		1. Without prejudice to Article 51 the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the transnational processing of this controller or processor in accordance with the procedure in Article 54a.	
		2a. By derogation from paragraph 1, each supervisory authority shall be competent to deal with a complaint lodged with it or to deal with a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.	
		2b. In the cases referred to in paragraph 2a, the supervisory authority shall inform the lead supervisory authority without delay on this matter. Within a	

		period of three weeks after being informed the lead supervisory authority shall decide whether or not it will deal with the case in accordance with the procedure provided in Article 54a, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.	
		2c. Where the lead supervisory authority decides to deal with the case, the procedure provided in Article 54a shall apply. The supervisory authority which informed the lead supervisory authority may submit to such supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in paragraph 2 of Article 54a.	
		2d. In case the lead supervisory authority decides not to deal with it, the supervisory authority which informed the lead supervisory	

		authority shall deal with the case according to Articles 55 and 56.	
		3. The lead supervisory authority shall be the sole interlocutor of the controller or processor for their transnational processing	
		Article 51b	
		Identification of the supervisory authority competent for the main establishment	
		deleted	
		Article 51c	
		One-stop shop register	
		deleted[335]	
Article 52	***Article 52***	***Article 52***	
Duties	~~***Duties***~~	***<u>Tasks</u>***[336]	
1. The supervisory authority shall:	1. The supervisory authority shall:	1. ~~***The***~~ ***Without prejudice to other tasks set out under this Regulation, each*** supervisory	

[335] ***AT reservation on the deletion of Articles 51b and 51c.***

[336] ***DE, IT, AT, PT and SE scrutiny reservation.***

		authority shall ***on its territory***:	
(a) monitor and ensure the application of this Regulation;	(a) monitor and ensure the application of this Regulation;	(a) monitor and ~~ensure~~ ***enforce*** the application of this Regulation;	
		(aa) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention;	
		(ab) advise, in accordance with national law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;	
		(ac) promote the awareness of controllers and processors of their obligations under this Regulation;	
		(ad) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, co-operate with the	

		supervisory authorities in other Member States to this end;	
	Amendment 150		
(b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;	(b) hear complaints lodged by any data subject, or by an association ~~representing that data subject~~ in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;	(b) ~~hear~~ ***deall with*** complaints lodged by ~~any~~ a data subject, or ***body, organisation or*** ~~by an~~ association representing ~~that~~ a data subject in accordance with Article 73***, and*** investigate, to the extent appropriate, the ***subject*** matter ***of the complaint*** and inform the data subject or the ***body, organisation or*** association of the progress and the outcome of the ~~complaint~~ ***investigation*** within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;	
(c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation;	(c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation;	(c) ~~share~~ ***cooperate with, including sharing*** information ~~with,~~ and provide mutual assistance to other supervisory authorities ***with a view to*** ~~and ensure~~ ensuring the consistency of application and enforcement of this Regulation;	
	Amendment 151		

(d) conduct investigations either on its own initiative or on the basis of a complaint or on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the investigations within a reasonable period;	(d) conduct investigations, either on its own initiative or on the basis of a complaint or ***of specific and documented information received alleging unlawful processing or*** on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the investigations within a reasonable period;	(d) conduct investigations ~~either on its own initiative or on the basis of a complaint or on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this~~ ***on the application of this Regulation, including on the basis of information received from another*** supervisory authority~~, of the outcome of the investigations within a reasonable period~~***or other public authority***;	
(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;	(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;	(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;	
(f) be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;	(f) be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;	(f) ~~be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data~~ ***adopt standard contractual clauses referred to in Article 26(2c);***	

		(fa) establish and make a list in relation to the requirement for data protection impact assessment pursuant to Article 33(2a);	
(g) authorise and be consulted on the processing operations referred to in Article 34;	(g) ~~authorise and~~ be consulted on the processing operations referred to in Article 34;	(g) ~~authorise and be consulted~~ ***give advice*** on the processing operations referred to in Article 34***(3)***;	
		(***ga) encourage the drawing up of codes of conduct pursuant to Article 38 and give an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 38 (2);***	
		(gb) promote the establishment of data protection certification mechanisms and of data protection seals and marks, and approve the criteria of certification pursuant to Article 39(2a);	
		(gc) where applicable, carry out a periodic review of certifications issued in accordance with Article 39(4);	
(h) issue an opinion on the draft codes of conduct pursuant to	(h) issue an opinion on the draft codes of conduct pursuant to Article	(h) ~~issue an opinion on the~~ draft ***and publish the criteria for***	

Article 38(2);	38(2);	***accreditation of a body for monitoring*** codes of conduct pursuant to Article 38~~(2)~~a ***and of a certification body pursuant to Article 39a***;	
		(ha) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 38a and of a certification body pursuant to Article 39a;	
		(hb) authorise contractual clauses referred to in Article 42(2a)(a);	
(i) approve binding corporate rules pursuant to Article 43;	(i) approve binding corporate rules pursuant to Article 43;	(i) approve binding corporate rules pursuant to Article 43;	
(j) participate in the activities of the European Data Protection Board.	(j) participate in the activities of the European Data Protection Board.	(j) ~~participate in~~ ***contribute to*** the activities of the European Data Protection Board~~.~~**;**	
		(k) fulfil any other tasks related to the protection of personal data.	
	Amendment 152		
	(ja) certify controllers and processors pursuant to Article 39.		

	Amendment 153		
2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention.	2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data ***and on appropriate measures for personal data protection***. Activities addressed specifically to children shall receive specific attention.	***deleted***	
	Amendment 154		
	2a. Each supervisory authority shall together with the European Data Protection Board promote the awareness for controllers and processors on risks, rules, safeguards and rights in relation to the processing of personal data. This includes keeping a register of sanctions and breaches. The register should enrol both all warnings and sanctions as detailed as possible and the resolving of breaches. Each supervisory authority shall provide micro, small and medium sized enterprise controllers and processors on request with general information		

	on their responsibilities and obligations in accordance with this Regulation.		
3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.	3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.	***deleted***	
4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.	4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.	4. ~~For~~ ***Each supervisory authority shall facilitate the submission of*** complaints referred to in point (b) of paragraph 1, ~~the supervisory authority shall provide a~~ ***by measures such as providing a*** complaint submission form, which can be completed ***also*** electronically, without excluding other means of communication.	
5. The performance of the duties of the supervisory authority shall be free of charge for the data subject.	5. The performance of the duties of the supervisory authority shall be free of charge for the data subject.	5. The performance of the ~~duties~~ ***tasks*** of ~~the~~ ***each*** supervisory authority shall be free of charge for the data subject ***and for the data protection officer, if any***.	

	Amendment 155		
6. Where requests are manifestly excessive, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action requested by the data subject. The supervisory authority shall bear the burden of proving the manifestly excessive character of the request.	6. Where requests are manifestly excessive, in particular due to their repetitive character, the supervisory authority may charge a ***reasonable*** fee or not take the action requested by the data subject. ***Such a fee shall not exceed the costs of taking the action requested.*** The supervisory authority shall bear the burden of proving the manifestly excessive character of the request.	6. Where requests are manifestly ***unfounded or*** excessive, in particular ~~due to~~ ***because of*** their repetitive character, the supervisory authority may~~ charge a fee or not take the action requested by the data subject~~ ***refuse to act on the request***. The supervisory authority shall bear the burden of ~~proving~~ ***demonstrating*** the manifestly ***unfounded or*** excessive character of the request[337].	
Article 53	***Article 53***	***Article 53***	
Powers	***Powers***	***Powers***[338]	
	Amendment 156		
1. Each supervisory authority shall have the power:	1. Each supervisory authority shall***, in line with this Regulation,*** have the power:	1. Each ***Member State shall provide by law that its*** supervisory authority shall have ***at least***[339] the ***following investigative*** powers:	

[337] ***DE and SE reservation: this could be left to general rules.***

[338] ***DE, RO, PT and SE scrutiny reservation; SE thought this list was too broad. Some Member States were uncertain (CZ, RO and UK) or opposed (DE, DK, and IE) to categorising the DPA powers according to their nature.***

[339] ***RO argued in favour of the inclusion of an explicit reference to the power of DPAs to issue administrative orders regarding the uniform application of certain data protection rules. COM and ES scrutiny reservation on 'at least' in paragraphs 1 and 1a.***

(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;	(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject***, or to order the controller to communicate a personal data breach to the data subject***;	(a) to ~~notify~~ ***order*** the controller ~~or~~ ***and*** the processor ~~of an alleged breach of the provisions governing the processing of personal data,~~ and, where ~~appropriate~~***applicable***, ~~order~~ the controller's ~~or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject~~***representative to provide any information it requires for the performance of its tasks***;	
		(aa) to carry out investigations in the form of data protection audits[340];	
		(ab) to carry out a review on certifications issued pursuant to Article 39(4);	
(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation;	(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation;	***deleted***	
(c) to order the controller and the processor, and, where applicable, the representative to	(c) to order the controller and the processor, and, where applicable, the representative to provide any	***deleted***	

[340] ***CZ, IT, PL scrutiny reservation. CZ and PL pleaded for a recital explaining that audit could be understood as inspection.***

provide any information relevant for the performance of its duties;	information relevant ~~for~~ the performance ~~of~~ its duties;		
(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;	(d) to ensure the compliance with ~~prior authorisations and~~ prior consultations referred to in Article 34;	(d) to ~~ensure~~ ***notify*** the ~~compliance with prior authorisations and prior consultations referred to in Article 34~~***controller or the processor of an alleged infringment of this Regulation***;	
		(da) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;	
		(db) to obtain access to any premises of the controller and the processor , including to any data processing equipment and means, in conformity with Union law or Member State procedural law.	
		1a. (…). ***1b. Each Member State shall provide by law that its supervisory authority shall have the following corrective powers:***	
		(a) to issue warnings to a controller or processor that	

		intended processing operations are likely to infringe provisions of this Regulation;	
		(b) to issue reprimands[341] to a controller or processor where processing operations have infringed provisions of this Regulation[342];	
		(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;	
		(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; in particular by ordering the rectification, restriction or erasure of data pursuant to Articles 16, 17 and 17a and the notification of such actions to recipients to whom the data have been disclosed pursuant to Articles	

[341] ***PL scrutiny reservation.***

[342] ***PL scrutiny reservation on points (a) and (b).***

		17(2a) and 17b;	
(e) to warn or admonish the controller or the processor;	(e) to warn or admonish the controller or the processor;	***(e) to impose a temporary or definitive limitation on processing;***	
(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed;	(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed;	(f) to order the ~~rectification, erasure or destruction of all~~ data ~~when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed~~ ***data flows to a recipient in a third country or to an international organisation***;	
(g) to impose a temporary or definitive ban on processing;	(g) to impose a temporary or definitive ban on processing;	(g) to impose ~~a temporary or definitive ban on processing;~~***an administrative fine pursuant to Articles 79 and 79a[343], in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.***	
(h) to suspend data flows to a recipient in a third country or to an international organisation;	(h) to suspend data flows to a recipient in a third country or to an international organisation;	(h) to ***order the*** ~~suspend~~ suspension ***of*** data flows to a recipient in a third country or to an international organisation[344];	

[343] ***DK constitutional reservation on the introduction of administrative fines, irrespective of the level of the fines.***

[344] ***SK reservation.***

(i) to issue opinions on any issue related to the protection of personal data;	(i) to issue opinions on any issue related to the protection of personal data;	***deleted***	
	(ia) to certify controllers and processors pursuant to Article 39;		
(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.	(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data***;***	***deleted***	
	(ja) to put in place effective mechanisms to encourage confidential reporting of breaches of this Regulation, taking into account guidance issued by the European Data Protection Board pursuant to Article 66(4b).		
		1c. Each Member State shall provide by law that its supervisory authority shall have the following authorisation and advisory powers:	
		(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 34;	

		(aa) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;	
		(ab) to authorise processing referred to in Article 34(7a), if the law of the Member State requires such prior authorisation;	
		(ac) to issue an opinion and adopt draft codes of conduct pursuant to Article 38(2);	
		(ad) to accredit certification bodies under the terms of Article 39a;	
		(ae) to issue certifications and approve criteria of certification in accordance with Article 39(2a);	
		(b) to adopt standard data protection clauses referred to in point (c) of Article 42(2);	

		(c) to authorise contractual clauses referred to in point (a) of Article 42(2a);	
		(ca) to authorise administrative agreements referred to in point (d) of Article 42 (2a);	
		(d) to approve binding corporate rules pursuant to Article 43.	
2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:	2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor ***without prior notice***:	2. ~~Each supervisory authority shall have the investigative power to obtain from the controller or the processor:~~ ***The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter of Fundamental Rights of the European Union.***[345]	
(a) access to all personal data and to all information necessary for the performance of its duties;	(a) access to all personal data and to all ***documents and*** information necessary for the performance of its	***deleted***	

[345] ***CY, ES, FR, IT and RO thought this could be put in a recital as these obligations were binding upon the Member States at any rate.***

	duties;		
(b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there.	(b) access to any of its premises, including to any data processing equipment and means~~, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there~~.	***deleted***	
The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.	The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.	***deleted***	
3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).	3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).	3. Each ***Member State shall provide by law that its*** supervisory authority shall have the power to bring ~~violations~~ ***infringements*** of this Regulation to the attention of the judicial authorities and ***where appropriate,*** to ***commence or*** engage ***otherwise*** in legal proceedings[346]~~, in particular pursuant to Article 74(4) and Article 75(2)~~***, in order to enforce the provisions of this Regulation***[347]***.***	

346 ***DE, FR and RO reservation on proposed DPA power to engage in legal proceedings. UK scrutiny reservation. CZ and HU reservation on the power to bring this to the attention of the judicial authorities.***

347 ***DE thought para. 3 and 4 should be deleted.***

4. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).	4. Each supervisory authority shall have the power to sanction administrative offences, in ~~particular those referred to in~~ ***accordance with*** Article 79~~(4), (5) and (6)~~. ***This power shall be exercised in an effective, proportionate and dissuasive manner.***	***deleted***	
Article 54	***Article 54***	***Article 54***	
Activity report	***Activity report***	***Activity report***	
	Amendment 157		
Each supervisory authority must draw up an annual report on its activities. The report shall be presented to the national parliament and shall be made be available to the public, the Commission and the European Data Protection Board.	Each supervisory authority must draw up ~~an annual~~ ***a*** report on its activities ***at least every two years***. The report shall be presented to the ~~national~~ ***respective*** parliament and shall be made ~~be~~ available to the public, the Commission and the European Data Protection Board.	Each supervisory authority ~~must~~ shall draw up an annual report on its activities. The report shall be ~~presented~~ ***transmitted*** to the national ~~parliament~~ Parliament ***, the government and other authorities as designated by national law.*** ~~and~~ ***It*** shall be made ~~be~~ available to the public, the ***European*** Commission and the European Data Protection Board.	

	Amendment 157		
	Article 54a (new)		
	Lead Authority		
	1. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, or where personal data of the residents of several Member States are processed, the supervisory authority of the main establishment of the controller or processor shall act as the lead authority responsible for the supervision of the processing activities of the controller or the processor in all Member States, in accordance with the provisions of Chapter VII of this Regulation.		
	2. The lead ~~supervisory~~ authority shall take appropriate measures for the supervision of the processing activities of the controller or processor for which it is		

	responsible only after consulting all other competent supervisory authorities within the meaning of paragraph 1 of Article 51(1) in an endeavour to reach a consensus. For that purpose it shall in particular submit any relevant information and consult the other authorities before it adopts a measure intended to produce legal effects vis-à-vis a controller or a processor within the meaning of ~~paragraph 1 of~~ Article 51(1). The lead authority shall take the utmost account of the opinions of the authorities involved. The lead authority shall be the sole authority empowered to decide on measures intended to produce legal effects as regards the processing activities of the controller or processor for which it is responsible		
	3. The European Data Protection Board shall, at the request of a competent supervisory authority, issue an opinion on the identification of the lead authority responsible for a controller or processor, in cases where:		

	(a) it is unclear from the facts of the case where the main establishment of the controller or processor is located; or		
	(b) the competent authorities do not agree on which supervisory authority shall act as lead authority; or		
	(c) the controller is not established in the Union, and residents of different Member States are affected by processing operations within the scope of this Regulation.		
	3a. Where the controller exercises also activities as a processor, the supervisory authority of the main establishment of the controller shall act as lead authority for the supervision of processing activities.		
	4. The European Data Protection Board may decide on the identification of the lead authority.		

		Article 54a	
		Cooperation between the lead supervisory authority and other supervisory authorities concerned[348]	
		1. In the cases referred to in Article 51a, the lead supervisory authority shall cooperate with the supervisory authorities concerned in accordance with this article in an endeavour to reach consensus.	
		1a. In the cases referred to in paragraph 1 of Article 51a, each supervisory authority concerned shall inform the lead supervisory authority and refer the matter to the lead supervisory authority without delay.	
		The lead supervisory authority shall, without delay, further investigate the subject matter and communicate the relevant information on the matter to the supervisory authorities concerned	

[348] ***BE, CZ, CY, DE, EE, FR, FI, IE, LU, RO, PT and NL scrutiny reservation. IE pointed out that in the case of personal data processed by social media or other internet platforms, all 28 MS DPAs would be 'concerned'. LU and NL doubted that one DPA concerned would be sufficient to trigger the consistency mechanisms. BE, FR, PL and LU expressed a preference for amicable settlements.***

		and shall submit a draft decision including on whether there is an infringement of this Regulation or not and on the exercise of the powers referred to in paragraphs 1, 1b and 1c of Article 53 to all supervisory authorities concerned for their opinion and take due account of the views of those supervisory authorities.	
		2a. (…) ***2b. The lead supervisory authority may request at any time the supervisory authorities concerned to provide mutual assistance pursuant to Article 55 and may conduct joint operations pursuant to Article 56, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.***	
		3. Where any of the supervisory authorities concerned expresses a reasoned objection within a period of four weeks after having been consulted in	

		accordance with paragraph 2 to the draft decision, the lead supervisory authority shall, if it does not follow the objection, submit the matter to the consistency mechanism referred to in Article 57. In such a case, the European Data Protection Board shall settle the dispute and be binding on the lead supervisory authority and all the supervisory authorities concerned pursuant to point 2(a) of Article 57 and Article 58a. Where a supervisory authority concerned has not objected within this period, it is deemed to be in agreement with the draft decision.	
		4. Where no supervisory authority concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraph 3, the lead supervisory authority and the supervisory authorities concerned shall agree on a single decision jointly.	
		4a. The lead supervisory authority shall give legal effect to	

		the jointly agreed single decision and notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and inform the European Data Protection Board of the decision in question including a summary of the relevant facts and grounds.	
		4b. Where the jointly agreed single decision concerns a complaint and as far as it adversely affects the complainant, notably where the complaint is rejected, dismissed or granted only in part, the supervisory authority that has received such complaint shall give legal effect to the jointly agreed the single decision concerning that complaint and serve it on the complainant. The complainant shall be informed in any case of the outcome of the complaint pursuant to Article 73, paragraph 5.[349]	
		4c. After being notified of the decision of the lead supervisory	

[349] ***PL scrutiny reservation on paragraph 4b.***

		authority pursuant to paragraph 4a, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards the processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall then inform all the supervisory authorities concerned. The supervisory authorities concerned shall be bound by the single decision adopted jointly in the manner described above.	
		4d. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 61 shall apply.	
		5. The lead supervisory authority and the supervisory authorities concerned shall supply the information required under	

		this Article to each other by electronic means, using a standardised format.	

CHAPTER VII CO-OPERATION AND CONSISTENCY	CHAPTER VII CO-OPERATION AND CONSISTENCY	CHAPTER VII[350] CO-OPERATION AND CONSISTENCY	
SECTION 1 CO-OPERATION	SECTION 1 CO-OPERATION	SECTION 1 CO-OPERATION	
		Article 54a	
		Cooperation between the lead supervisory authority and other concerned supervisory authorities[351]	
		1. The lead supervisory authority shall cooperate with the other concerned supervisory authorities in accordance with this article in an endeavour to reach consensus. The lead supervisory authority and the concerned supervisory authorities shall exchange all relevant information with each other.	
		1a. The lead supervisory authority may request at any time	

[350] ***AT and FR scrutiny reservation on Chapter VII.***

[351] ***CZ, CY, DE, EE, FR, FI, IE, LU, RO and PT scrutiny reservation.***

		other concerned supervisory authorities to provide mutual assistance pursuant to Article 55 and may conduct joint operations pursuant to Article 56, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.	
		2. The lead supervisory authority shall, without delay communicate the relevant information on the matter to the other concerned supervisory authorities. It shall without delay submit a draft decision to the other concerned supervisory authorities for their opinion and take due account of their views.	
		3. Where any[352] of the other concerned supervisory authorities within a period of four weeks after having been consulted in accordance with paragraph 2, expresses a relevant and reasoned	

[352] ***A number of Member States (CZ, IE, NL, PL, FI and UK) still prefers a quantitative threshold by which an objection would need to be supported by 1/3 of the concerned supervisory authorities before the lead authority is obliged to refer the matter to the EDPB.***

		objection to the draft decision, the lead supervisory authority shall, if it does not follow the objection or is of the opinion it is not relevant and reasoned, submit the matter to the consistency mechanism referred to in Article 57.	
		3a. Where the lead supervisory authority intends to follow the objection made, it shall submit to the other concerned supervisory authorities a revised draft decision for their opinion. This revised draft decision shall be subject to the procedure referred to in paragraph 3 within a period of two weeks.	
		4. Where none of the other concerned supervisory authority has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 3 and 3a, the lead supervisory authority and the concerned supervisory authorities shall be deemed to be in agreement with this draft decision and shall be bound by it.	

		4a. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other concerned supervisory authorities and the European Data Protection Board of the decision in question including a summary of the relevant facts and grounds. The supervisory authority to which a complaint has been lodged shall inform the complainant on the decision.	
		4b. By derogation from paragraph 4a, where a complaint is dismissed or rejected, the supervisory authority to which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.	
		4bb. Where the lead supervisory authority and the concerned supervisory authorities are in agreement to dismiss or reject parts of a complaint and to act on	

		other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter.The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller and notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof[353], while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint and notify it on that complainant[354] and shall inform the controller or processor thereof. [355]	
		4c. After being notified of the decision of the lead supervisory authority pursuant to paragraph 4a and 4bb, the controller or processor shall take the necessary measures to ensure compliance	

[353] ***Further to suggestions from HU and IE.***

[354] ***SI scrutiny reservation. PL reservation on paras 4b and 4bb: PL and FI thought para. 4bb should be deleted as it was opposed to the concept of a split decision. IT thought para 4bb overlapped with para 4b.***

[355] ***Further to suggestions from HU and IE.***

		with the decision as regards the processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other concerned supervisory authorities.	
		4d. Where, in exceptional circumstances, a concerned supervisory authority has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 61 shall apply.	
		5. The lead supervisory authority and the other concerned supervisory authorities shall supply the information required under this Article to each other by electronic means, using a standardised format.	

Article 55	***Article 55***	***Article 55***	
Mutual assistance	***Mutual assistance***	***Mutual assistance***[356]	
	Amendment 159		
1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and prompt information on the opening of cases and ensuing developments where data subjects in several Member States are likely to be affected by processing operations.	1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior ~~authorisations and~~ consultations, inspections ***and investigations*** and prompt information on the opening of cases and ensuing developments ***where the controller or processor has establishments in several Member States or*** where data subjects in several Member States are likely to be affected by processing operations. ***The lead authority as defined in Article 54a shall ensure the coordination with***	1. Supervisory authorities shall provide each other ***with*** relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and ~~prompt information on the opening of cases and ensuing developments where data subjects in several Member States are likely to be affected by processing operations~~***investigations***.	

[356] ***DE, NL SE and UK scrutiny reservation.***

	involved supervisory authorities and shall act as the single contact point for the controller or processor.		
2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation.	2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation.	2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without ***undue*** delay and no later than one month[357] after having received the request. Such measures may include, in particular, the transmission of relevant information on the ~~course~~ ***conduct*** of an investigation~~ or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation~~.	
3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.	3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.	3. The request for assistance shall contain all the necessary information[358], including the purpose of the request and reasons for the request. Information exchanged shall be used only ~~in respect of the matter~~ ***for the***	

[357] ***ES, supported by PT, had suggested 15 days. RO and SE found one month too short. COM indicated that it was only a deadline for replying, but that paragraph 5 allowed longer periods for executing the assistance requested.***

[358] ***EE and SE scrutiny reservation.***

		purpose for which it was requested.	
4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:	4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:	4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:	
(a) it is not competent for the request; or	(a) it is not competent for the request; or	(a) it is not competent for the ***subject-matter of the*** request ***or for the measures it is requested to execute***[359]; or	
(b) compliance with the request would be incompatible with the provisions of this Regulation.	(b) compliance with the request would be incompatible with the provisions of this Regulation.	(b) compliance with the request would be incompatible with the provisions of this Regulation ***or with Union or Member State law to which the supervisory authority receiving the request is subject***.	
5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.	5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.	5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to ~~meet~~ ***respond to*** the request ~~by the requesting supervisory authority~~.***In case of a refusal under paragraph 4, it shall explain its reasons for refusing the***	

[359] ***Several delegations stressed the importance of establishing which is the competent DPA: DE, EE, SE, SI. and IT asked for further clarification.***

		request*[360]*.	
6. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.	6. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.	6. Supervisory authorities shall***, as a rule,*** supply the information requested by other supervisory authorities by electronic means[361] ~~and within the shortest possible period of time~~, using a standardised format.	
	Amendment 160		
7. No fee shall be charged for any action taken following a request for mutual assistance.	7. No fee shall be charged ***to the requesting supervisory authority*** for any action taken following a request for mutual assistance.	7. No fee shall be charged for any action taken following a request for mutual assistance. ***Supervisory authorities may agree with other supervisory authorities rules for indemnification by other supervisory authorities for specific expenditure arising from the provision of mutual assistance in exceptional circumstances*[362]*.***	
	Amendment 161		
8. Where a supervisory authority does not act within one month on request of another	8. Where a supervisory authority does not act within one month on request of another supervisory	8. Where a supervisory authority does not ~~act~~ ***provide the information reeferred to in***	

[360] ***RO scrutiny reservation.***

[361] ***PT (supported by RO) suggested adding "or other means if for some reason, electronic means are not available, and the communication is urgent".***

[362] ***PT, UK and DE asked for clarification in relation to the resources needed / and estimate of costs.***

supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.	authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57. ***Where no definitive measure is yet possible because the assistance is not yet completed, the requesting supervisory authority may take interim measures under Article 53 in the territory of its Member State.***	***paragraph 5*** within one month***of receiving the*** ~~on~~ request of another supervisory authority, the requesting supervisory ~~authorities~~ authority ~~shall be competent to take~~ ***may adopt*** a provisional measure[363] on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the ~~procedure~~ ***consistency mechanism*** referred to in Article 57[364].	
	Amendment 162		
9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.	9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission ***in accordance with the procedure***	9. The supervisory authority shall specify the period of validity of such provisional measure ***which*** ~~.~~ ~~This period~~ shall not exceed three months[365]. The supervisory authority shall, without delay, communicate ~~those~~ ***such a*** measure~~s~~, ***together*** with ~~full~~ ***its*** reasons ***for adopting it***, to the European Data Protection Board	

[363] ***LU requested more clarification with regard to what would happen if this provisional measure were not confirmed.***

[364] ***EE, FR, RO, and UK reservation. DE scrutiny.***

[365] ***DE asked for deletion of this deadline; the measure should be withdrawn if the conditions for imposing it were no longer fulfilled.***

	referred to in Article 57.	~~and to the Commission~~***in accordance with the consistency mechanism referred to in Article 57***.	
	Amendment 163		
10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	10. The ~~Commission~~ ***European Data Protection Board*** may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~	10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)[366].	

[366] ***DE, IT, EE and CZ reservation.***

Article 56	***Article 56***	***Article 56***	
Joint operations of supervisory authorities	***Joint operations of supervisory authorities***	***Joint operations of supervisory authorities***[367]	
1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint investigative tasks, joint enforcement measures and other joint operations, in which designated members or staff from other Member States' supervisory authorities are involved.	1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint investigative tasks, joint enforcement measures and other joint operations, in which designated members or staff from other Member States' supervisory authorities are involved.	1. ~~In order to step up co-operation and mutual assistance, the~~ The supervisory authorities ~~shall carry out~~ ***may , where appropriate, conduct*** joint ***operations including joint investigations and*** ~~investigative tasks,~~ joint enforcement measures ~~and other joint operations,~~ in which ~~designated~~ members or staff from other Member States' supervisory authorities are involved.	
	Amendment 164		
2. In cases where data subjects in several Member States are likely to be affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint investigative tasks or joint	2. In cases ***where the controller or processor has establishments in several Member States or*** where data subjects in several Member States are likely to be affected by processing operations, a supervisory authority of each of those Member	2. In cases where ***the controller or procecssor has establishments in several Member States or where a significant number of***[368] data subjects in ~~several~~ ***more than one*** Member State~~s~~ are likely to be ***substantially*** affected by	

[367] ***DE, EE, PT and UK scrutiny reservation.***

[368] ***COM reservation; IT, supported by FR and CZ suggested stressing the multilateral aspect.***

operations, as appropriate. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the respective joint investigative tasks or joint operations and respond to the request of a supervisory authority to participate in the operations without delay.	States shall have the right to participate in the joint investigative tasks or joint operations, as appropriate. The ~~competent supervisory authority~~ ***lead authority as defined in Article 54a*** shall ~~invite~~ ***involve*** the supervisory authority of each of those Member States ~~to take part~~ in the respective joint investigative tasks or joint operations and respond to the request of a supervisory authority to participate in the operations without delay. ***The lead authority shall act as the single contact point for the controller or processor.***	processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint ~~investigative tasks or joint~~ operations, as appropriate. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the ~~respective~~ joint ~~investigative tasks or joint~~ operations ***concerned*** and respond ***without delay*** to the request of a supervisory authority to participate ~~in the operations without delay~~.	
3. Each supervisory authority may, as a host supervisory authority, in compliance with its own national law, and with the seconding supervisory authority's authorisation, confer executive powers, including investigative tasks on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their	3. Each supervisory authority may, as a host supervisory authority, in compliance with its own national law, and with the seconding supervisory authority's authorisation, confer executive powers, including investigative tasks on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their	3. ~~Each~~ A supervisory authority may, ~~as a host supervisory authority,~~ in compliance with its own ~~national~~ ***Member State*** law, and with the seconding supervisory authority's authorisation, confer ~~executive~~ powers, including investigative ~~tasks~~ ***powers*** on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the ***law of the Member State of the*** host supervisory authority~~'s law~~ permits, allow the seconding supervisory	

executive powers in accordance with the seconding supervisory authority's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. The host supervisory authority shall assume responsibility for their actions.	executive powers in accordance with the seconding supervisory authority's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. The host supervisory authority shall assume responsibility for their actions.	authority's members or staff to exercise their ~~executive~~ ***investigative*** powers in accordance with the ***law of the Member State of the*** seconding supervisory authority~~'s law~~. Such ~~executive~~ ***investigative*** powers may be exercised only under the guidance and~~, as a rule,~~ in the presence of members or staff ~~from~~ ***of*** the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law[369]. ~~The host supervisory authority shall assume responsibility for their actions.~~	
		3a. Where, in accordance with paragraph 1, staff of a seconding supervisory authority are operating in another Member State, the Member State of the host supervisory authority shall be liable for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.	

[369] ***DE, LU, PT and COM scrutiny reservation on the deletion of this last phrase.***

		3b. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse the latter in full any sums it has paid to the persons entitled on their behalf.	
		3c. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 3b, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement of damages it has sustained from another Member State[370].	
4. Supervisory authorities shall lay down the practical aspects of specific co-operation actions.	4. Supervisory authorities shall lay down the practical aspects of specific co-operation actions.	***deleted***	
5. Where a supervisory	5. Where a supervisory authority	5. Where ***a joint operation is***	

[370] ***UK reservation on paras. 3a, 3b and 3c.***

authority does not comply within one month with the obligation laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1).	does not comply within one month with the obligation laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1).	***intended and*** a supervisory authority does not comply within one month with the obligation laid down in ***the second sentence of*** paragraph 2, the other supervisory authorities ~~shall be competent to take~~ ***may adopt*** a provisional measure on the territory of its Member State in accordance with Article 51(1).	
6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission and shall submit the matter in the mechanism referred to in Article 57.	6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission and shall submit the matter in the mechanism referred to in Article 57.	6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5 ***which*** ~~. This period~~ shall not exceed three months. The supervisory authority shall, without delay, communicate ~~those~~ ***such a*** measure~~s~~, ***together*** with ~~full~~ ***its*** reasons ***for adopting it***, to the European Data Protection Board ~~and to the Commission and shall submit the matter in the~~ ***in accordance with the consistency*** mechanism referred to in Article 57.	

SECTION 2 CONSISTENCY	**SECTION 2 CONSISTENCY**	**SECTION 2 CONSISTENCY**[371]	
Article 57	***Article 57***	***Article 57***	
Consistency mechanism	***Consistency mechanism***	***Consistency mechanism***[372]	
	Amendment 165		
For the purposes set out in Article 46(1), the supervisory authorities shall co-operate with each other and the Commission through the consistency mechanism as set out in this section.	For the purposes set out in Article 46(1), the supervisory authorities shall co-operate with each other and the Commission through the consistency mechanism ~~as set out~~ ***both on matters of general application and in individual cases in accordance with the provisions of*** in this section.	***1.*** For the purposes set out in Article 46(1***a***), the supervisory authorities shall co-operate with each other ~~and the Commission~~ through the consistency mechanism as set out in this section[373].	
		2. The European Data Protection Board shall issue an opinion whenever a competent supervisory authority intends to adopt any of the measures below). To that end, the competent supervisory authority shall	

[371] ***IT and SI scrutiny reservation. DE parliamentary reservation and BE and UK reservation on the role of COM in the consistency mechanism.***

[372] ***EE, FI, and UK scrutiny reservation.***

[373] ***CZ, DE, ES and RO thought that supervisory authorities of third countries for which there is an adequacy decision should be involved in the consistency mechanism; if third countries participated in the consistency mechanism; if third countries participated in the consistency mechanism, they would be bound by uniform implementation and interpretation.***

		communicate the draft decision to the European Data Protection Board, when it:	
		(a) (…); ***(b) (…);*** ***(c) aims at adopting a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 33(2a); or***	
		(ca) concerns a matter pursuant to Article 38(2b) whether a draft code of conduct or an amendment or extension to a code of conduct is in compliance with this Regulation; or	
		(cb) aims at approving the criteria for accreditation of a body pursuant to paragraph 3 of Article 38a or a certification body pursuant to paragraph 3 of Article 39a;	
		(d) aims at determining standard data protection clauses referred to in point (c) of Article 42(2); or	

		(e) aims to authorising contractual clauses referred to in point (d) of Article 42(2); or	
		(f) aims at approving binding corporate rules within the meaning of Article 43.	
		3. The European Data Protection Board shall adopt a binding decision in the following cases:	
		a) ***Where, in a case referred to in paragraph 3 of Article 54a, a concerned supervisory authority has expressed a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected an objection as being not relevant and/or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of the Regulation;***	
		b) ***Where, there are conflicting views on which of the***	

		concerned supervisory authorities is competent for the main establishment;	
		c) ***(…);***	
		d) ***Where a competent supervisory authority does not request the opinion of the European Data Protection Board in the cases mentioned in paragraph 2 of this Article, or does not follow the opinion of the European Data Protection Board issued under Article 58. In that case, any concerned supervisory authority or the Commission may communicate the matter to the European Data Protection Board.***	
		4. Any supervisory authority, the Chair of the European Data Protection Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the European Data Protection Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the	

		obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.	
		5. Supervisory authorities and the Commission shall electronically communicate to the European Data Protection Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other concerned supervisory authorities .	
		6. The chair of the European Data Protection Board shall without undue delay electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the European Data Protection Board shall, where necessary, provide translations of relevant information.	

Article 58	*Article 58*	*Article 58*	
	Amendment 166		
Opinion by the European Data Protection Board	~~Opinion by the European Data Protection Board~~***Consistency on matters of general application***	***Opinion by the European Data Protection Board***[374]	
1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.	1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.	***deleted***	
2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:	2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:	***deleted***	
(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or	***deleted***	***deleted***	
(b) may substantially affect the free movement of personal data	***deleted***	***deleted***	

[374] ***UK scrutiny reservation.***

within the Union; or			
(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or	***deleted***	***deleted***	
(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or	(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or	***deleted***	
(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or	(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or	***deleted***	
(f) aims to approve binding corporate rules within the meaning of Article 43.	(f) aims to approve binding corporate rules within the meaning of Article 43.	***deleted***	
3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with	3. Any supervisory authority or the European Data Protection Board may request that any matter ***of general application*** shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with	***deleted***	

Article 56.	Article 56.		
4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.	4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter ***of general application*** shall be dealt with in the consistency mechanism.	***deleted***	
5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.	5. Supervisory authorities and the Commission shall ***without undue delay*** electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.	***deleted***	
6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where	6. The chair of the European Data Protection Board shall ~~immediately~~ ***without undue delay*** electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The ~~chair~~ ***secretariat*** of the European Data Protection Board shall provide translations of relevant information,	***deleted***	

necessary.	where necessary.		
	6a. The European Data Protection Board shall adopt an opinion on matters referred to it under paragraph 2.		
7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.	7. The European Data Protection Board ~~shall issue~~ ***may decide by simple majority whether to adopt*** an opinion on ~~the~~ ***any*** matter~~, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.~~ ***submitted under paragraphs 3 and***	7. ***In the cases referred to in paragraphs 2 and 4 of Article 57,*** ~~The~~ the European Data Protection Board shall issue an opinion on the ***same matter***~~, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The~~ This opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board.~~ The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public~~ ***This period may be***	

	4 taking into account :	***extended by a further month, taking into account the complexity of the subject matter. Regarding the draft decision circulated to the members of the Board in accordance with paragraph 6 of Article 57, a member which has not objected within the period indicated by the Chair, shall be deemed to be in agreement with the draft decision.].***	
	(a) whether the matter presents elements of novelty, taking account of legal or factual developments, in particular in information technology and in the light of the state of progress in the information society; and		
	(b) whether the European Data Protection Board has already issued an opinion on the same matter.		
		7a. Within the period referred to in paragraph 7 the competent supervisory authority shall not adopt its draft decision in accordance with paragraph 2 of Article 57.	

		7b. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 2 and 4 of Article 57 and the Commission of the opinion and make it public.	
8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.	8. ~~The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format~~***The European Data Protection Board shall adopt opinions pursuant to paragraphs 6a and 7 by a simple majority of its members. These opinions shall be made public***.	8. The supervisory authority referred to in paragraph ~~1~~ 2***of Article 57*** ~~and the supervisory authority competent under Article 51~~ shall take ***utmost*** account of the opinion of the European Data Protection Board and shall within two weeks after ~~the information on~~ ***receiving*** the opinion ~~by the chair of the European Data Protection Board~~, electronically communicate to the chair of the European Data Protection Board ~~and to the Commission~~ whether it maintains or ***will*** amend~~s~~ its draft ~~measure~~ ***decision*** and, if any, the amended draft ~~measure~~***decision***, using a standardised format.	

		9. Where the concerned supervisory authority informs the chair of the European Data Protection Board within the period referred to in paragraph 8 that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, paragraph 3 of Article 57 shall apply.	
	Amendment 167		
	Article 58a (new)		
	Consistency in individual cases		
	1. Before taking a measure intended to produce legal effects within the meaning of Article 54a, the lead authority shall share all relevant information and submit the draft measure to all other competent authorities. The lead authority shall not adopt the measure if a competent authority has, within a period of three weeks, indicated it has serious objections to the measure.		
	2. Where a competent authority		

	has indicated that it has serious objections to a draft measure of the lead authority, or where the lead authority does not submit a draft measure referred to in paragraph 1 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56, the issue shall be considered by the European Data Protection Board.		
	3. The lead authority and/or other competent authorities involved and the Commission shall without undue delay electronically communicate to the European Data Protection Board using a standardised format any relevant information, including as the case may be a summary of the facts, the draft measure, the grounds which make the enactment of such measure necessary, the objections raised against it and the views of other supervisory authorities concerned.		
	4. The European Data Protection Board shall consider the issue,		

	taking into account the impact of the draft measure of the lead authority on the fundamental rights and freedoms of data subjects, and shall decide by simple majority of its members whether to issue an opinion on the matter within two weeks after the relevant information has been provided pursuant to paragraph 3.		
	5. In case the European Data Protection Board decides to issue an opinion, it shall do so within six weeks and make the opinion public.		
	6. The lead authority shall take utmost account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.		

	Where the lead authority intends not to follow the opinion of the European Data Protection Board, it shall provide a reasoned justification.		
	7. In case the European Data Protection Board still objects to the measure of the supervisory authority as referred to in paragraph 5, it may within one month adopt by a two thirds majority a measure which shall be binding upon the supervisory authority.		
		Article 58a	
		Dispute Resolution by the European Data Protection Board[375]	
		1. In the cases referred to in paragraph 3 of Article 57, the European Data Protection Board shall adopt a decision on the subject-matter submitted to it in order to ensure the correct and consistent application of this Regulation in individual cases.	

[375] ***PL scrutiny reservation. IE thought the controller should have standing to intervene in the proceedings before the EDPB.***

		The decision shall be reasoned and addressed to the lead supervisory authority and all the concerned supervisory authorities and binding on them.	
		2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-third majority of the members of the Board. This period may be extended by a further month on account of the complexity of the subject-matter.	
		3. In case the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board[376]. In case the members of the Board are	

[376] ***AT and HU reservation. HU believes that this option will make the general two-thirds majority rule meaningless and symbolic, since there will be no effective incentive for the EDPB to adopt a decision that reflects the view of the vast majority of DPAs of the Member States, as eventually every decision could be adopted by only a slight majority of them. It would also undermine the general validity of the EDPB's decision, since the fact that the Board could not come to an agreement on a particular matter supported by at least the two-thirds of its members might give rise to serious doubts whether the finding of such decision is commonly shared across the Union. AT believes that a simple majority would be more effective and would not prolong the procedure.***

		split, the decision shall by adopted by the vote of its Chair.	
		4. The concerned supervisory authorities shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.	
		5. (…)	
		6. The Chair of the European Data Protection Board shall notify, without undue delay, the decision referred to in paragraph 1 to the concerned supervisory authorities. It shall inform the Commission thereof. The decision shall be published on the website of the European Data Protection Board without delay after the supervisory authority has notified the final decision referred to in paragraph 7.	
		7. The lead supervisory authority or, as the case may be, the supervisory authority to which the complaint has been lodged shall adopt their final decision on the basis of the decision referred to in	

		paragraph 1[377], without undue delay and at the latest by one month after the European Data Protection Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority to which the complaint has been lodged, shall inform the European Data Protection Board of the date when its final decision is notified respectively to the controller or the processor and the data subject. The final decision of the concerned supervisory authorities shall be adopted under the terms of Article 54a, paragraph 4a, 4b and 4bb. The final decision shall refer to the decision referred to in paragraph 1 and shall specify that the decision referred to in paragraph 1 will be published on the website of the European Data Protection Board in accordance with paragraph 6. The final decision shall attach the decision referred to in paragraph 1.	

[377] ***FI reservation; would prefer a system under which the EDPB decision would be directly applicable and would not have to be transposed by the lead DPA.***

	Amendment 168		
Article 59	***Article 59***	***Article 59***	
Opinion by the Commission	***Opinion by the Commission***	***Opinion by the Commission***[378]	
1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.	***deleted***	***deleted***	
2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.	***deleted***	***deleted***	
3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the	***deleted***	***deleted***	

[378] ***COM and FR reservation on deletion.***

supervisory authority.			
4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.	***deleted***	***deleted***	
	Amendment 169		
Article 60	***Article 60***	***Article 60***	
Suspension of a draft measure	***Suspension of a draft measure***	***Suspension of a draft measure***[379]	
1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned decision requiring the supervisory authority to suspend	***deleted***	***deleted***	

[379] ***COM and FR reservation on deletion.***

the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to:			
(a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or	***deleted***	***deleted***	
(b) adopt a measure pursuant to point (a) of Article 62(1).	***deleted***	***deleted***	
2. The Commission shall specify the duration of the suspension which shall not exceed 12 months.	***deleted***	***deleted***	
3. During the period referred to in paragraph 2, the supervisory authority may not adopt the draft measure.	***deleted***	***deleted***	

	Amendment 170		
	Article 60a (new)		
	Notification of the European Parliament and the Council		
	The Commission shall notify the European Parliament and the Council at regular intervals, at least every six months, on the basis of a report from the Chair of the European Data Protection Board, of the matters dealt with under the consistency mechanism, setting out the conclusions drawn by the Commission and the European Data Protection Board with a view to ensuring the consistent implementation and application of this Regulation.		
Article 61	***Article 61***	***Article 61***	
Urgency procedure	***Urgency procedure***	***Urgency procedure***[380]	
	Amendment 171		
1. In exceptional circumstances, where a supervisory	1. In exceptional circumstances, where a supervisory authority	1. In exceptional circumstances, where a ***concerned*** supervisory	

[380] ***DE scrutiny reservation.***

authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.	considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article ~~58~~***58a***, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.	authority considers that there is an urgent need to act in order to protect the ~~interests~~ ***rights and freedoms*** of data subjects, ***it may,*** ~~in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons,~~ by way of derogation from the ~~procedure~~ ***consistency mechanism*** referred to in Article 5~~8~~***7***[381] ***or the procedure referred to in Article 54a***, ~~it may~~ immediately adopt provisional measures ***intended to produce legal effects within the territory of its own Member State***[382]***,*** with a specified period of validity. The supervisory authority shall, without delay, communicate those measures~~, with full~~***and the*** reasons ***for adopting them***, to ***the other concerned supervisory authorities,*** the European Data Protection Board and to the Commission.	

[381] ***HU remarked that it should be clarified whether provisional measures can be adopted pending a decision by the EDPB. The Presidency thinks that the reference to Article 57 makes it clear that this is indeed possible.***

[382] ***COM scrutiny reservation.***

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.	2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.	2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion ***or an urgent binding decision form*** ~~of~~ the European Data Protection Board, giving reasons for requesting such opinion~~, including for the urgency of final measures~~***or decision***.	
3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.	3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.	3. Any supervisory authority may request an urgent opinion ***or an urgent binding decision, as the case may be, from the European Data Protection Board*** where ~~the~~ ***a*** competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the ~~interests~~ ***rights and freedoms*** of data subjects, giving reasons for requesting such opinion ***or decision***, including for the urgent need to act.	
	Amendment 172		
4. By derogation from Article 58(7), an urgent opinion referred to	4. ~~By derogation from Article 58(7), a~~An urgent opinion referred to in	4. By derogation from ***paragraph 7 of*** Article 58~~(7)~~ ***and paragraph 2***	

in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.	paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.	***of Article 58a***, an urgent opinion ***or an urgent binding decision*** referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.	
Article 62	***Article 62***	***Article 62***	
Implementing acts	***Implementing acts***	***Implementing acts***	
	Amendment 173		
1. The Commission may adopt implementing acts for:	1. The Commission may adopt implementing acts ***of general application***, ***after requesting an opinion of the European Data Protection Board,*** for:	1. The Commission may adopt implementing acts ***of general scope*** for:	
(a) deciding on the correct application of this Regulation in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has been adopted pursuant to Article 60(1), or concerning a matter in	***deleted***	***deleted***[383]	

383 COM reservation on deletion.

relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59;			
(b) deciding, within the period referred to in Article 59(1), whether it declares draft standard data protection clauses referred to in point (d) of Article 58(2), as having general validity;	(b) deciding~~, within the period referred to in Article 59(1),~~ whether it declares draft standard data protection clauses referred to in point (d) of Article ~~58~~***42***(2), as having general validity;	***deleted***	
(c) specifying the format and procedures for the application of the consistency mechanism referred to in this section;	***deleted***	***deleted***	
(d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 58(5), (6) and (8).	(d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 58(5), (6) and (8).	(d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article ***57(5) and (6) and in Article*** 58~~(5), (6) and~~ (8).	

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	
2. On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not exceeding 12 months.	***deleted***	***deleted***	
3. The absence or adoption of a measure under this Section does not prejudice any other measure by the Commission under the Treaties.	3. The absence or adoption of a measure under this Section does not prejudice any other measure by the Commission under the Treaties.	***deleted***	
Article 63	***Article 63***	***Article 63***	
Enforcement	***Enforcement***	***Enforcement***	
1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.	1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.	***deleted***	

	Amendment 174		
2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.	2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) ***and (2) or adopts a measure despite an indication of serious objection pursuant to Article 58a(1)***, the measure of the supervisory authority shall not be legally valid and enforceable.	***deleted***	

SECTION 3 EUROPEAN DATA PROTECTION BOARD	SECTION 3 EUROPEAN DATA PROTECTION BOARD	SECTION 3 EUROPEAN DATA PROTECTION BOARD	
Article 64	***Article 64***	***Article 64***	
European Data Protection Board	***European Data Protection Board***	***European Data Protection Board***	
1. A European Data Protection Board is hereby set up.	1. A European Data Protection Board is hereby set up.	1.***a*** ~~A~~ The European Data Protection Board is hereby ~~set up~~***established as body of the Union and shall have legal personality.***	
		1b. The European Data Protection Board shall be represented by its Chair.	
2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.	2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.	2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and ***or his/her representative*** ~~of the European Data Protection Supervisor~~.	
3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the	3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of	3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, ~~they shall nominate the head of one of~~	

head of one of those supervisory authorities as joint representative.	those supervisory authorities as joint representative.	~~those supervisory authorities as~~ ***a*** joint representative ***shall be appointed in accordance with the national law of that Member State***.	
4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.	4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.	4. The Commission ***and the European Data Protection Supervisor or his/her representative*** shall have the right to participate in the activities and meetings of the European Data Protection Board ~~and shall designate a representative~~ ***without voting right***. ***The Commission shall designate a representative.*** The chair of the European Data Protection Board shall, ~~without delay, inform~~ ***communicate to*** the Commission ***the*** ~~on all~~ activities of the European Data Protection Board.	
Article 65	***Article 65***	***Article 65***	
Independence	***Independence***	***Independence***	
1. The European Data Protection Board shall act independently when exercising its tasks pursuant to Articles 66 and	1. The European Data Protection Board shall act independently when exercising its tasks pursuant to	1. The European Data Protection Board shall act independently when ~~exercising~~ ***performing*** its tasks ***or exercising its powers*** pursuant to	

67.	Articles 66 and 67.	Articles 66 and 67[384].	
2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.	2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.	2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks ***or the exercise of its powers***, neither seek nor take instructions from anybody[385].	
Article 66	***Article 66***	***Article 66***	
Tasks of the European Data Protection Board	***Tasks of the European Data Protection Board***	***Tasks of the European Data Protection Board***	
	Amendment 175		
1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:	1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the ***European Parliament, Council or*** Commission, in particular:	1. The European Data Protection Board shall ~~ensure~~ ***promote*** the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:	

[384] ***UK and SI scrutiny reservation.***

[385] ***DE scrutiny reservation.***

		(aa) monitor and ensure the correct application of this Regulation in the cases provided for in Article 57(3) without prejudice to the tasks of national supervisory authorities;	
(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;	(a) advise the ~~Commission~~ ***European institutions*** on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;	(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;	
(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;	(b) examine, on its own initiative or on request of one of its members or on request of the ***European Parliament, Council or*** ***the*** Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation***, including on the use of enforcement powers***;	(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices ~~addressed to the supervisory authorities~~ in order to encourage consistent application of this Regulation;	
		(ba) draw up guidelines for supervisory authorities concerning the application of measures	

		referred to in paragraph 1, 1b and 1c of Article 53 and the fixing of administrative fines pursuant to Articles 79 and 79a[386];	
(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;	(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;	(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and ~~report regularly to the Commission on these~~***(ba)***;	
		(ca) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 38 and 39;	
		(cb) carry out the accreditation of certification bodies and its periodic review pursuant to Article 39a and maintain a public register of accredited bodies pursuant to paragraph 6 of Article 39a and of the accredited controllers or processors established in third countries pursuant to paragraph 4	

[386] ***DK constitutional reservation on the introduction of administrative fines, irrespective of the level of the fines.***

		of Article 39[387];	
		(cd) specify the requirements mentioned in paragraph 3 of Article 39a with a view to the accreditation of certification bodies under Article 39;	
		(ce) give the Commission an opinion on the level of protection in third countries or international organisations, in particular in the cases referred to in Article 41;	
(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;	(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;	(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in ***paragraph 2 and on matters submitted pursuant to paragraph 4 of*** Article 57;	
	(da) provide an opinion on which authority should be the lead authority pursuant to Article 54a(3);		
(e) promote the co-operation and the effective bilateral and multilateral exchange of	(e) promote the co-operation and the effective bilateral and multilateral exchange of	(e) promote the co-operation and the effective bilateral and multilateral exchange of	

[387] ***HU said that paragraphs (ca) and (cb) were contrary to the text of the general approach reached in June 2014 (11028/14); it is for the national supervisory authority to do this.***

information and practices between the supervisory authorities;	information and practices between the supervisory authorities***, including the coordination of joint operations and other joint activities, where it so decides at the request of one or several supervisory authorities;***	information and practices between the supervisory authorities;	
(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;	(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;	(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;	
(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.	(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide**;**	(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.	
	(ga) give its opinion to the Commission in the preparation of delegated and implementing acts based on this Regulation;		
	(gb) give its opinion on codes of conduct drawn up at Union level pursuant to Article 38(4);		

	(gc) give its opinion on criteria and requirements for the data protection certification mechanisms pursuant to Article 39(3);		
	(gd) maintain a public electronic register on valid and invalid certificates pursuant to Article 39(1h);		
	(ge) provide assistance to national supervisory authorities, at their request;		
	(gf) establish and make public a list of the processing operations which are subject to prior consultation pursuant to Article 34;		
	(gg) maintain a registry of sanctions imposed on controllers or processors by the competent supervisory authorities.		
		(h) (…)	
		(i) maintain a publicly accessible electronic register of decisions taken by supervisory	

		authorities and courts on issues dealt with in the consistency mechanism.	
2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.	2. Where the ***European Parliament, the Council or*** the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.	2. Where the Commission requests advice from the European Data Protection Board, it may ~~lay out~~ ***indicate*** a time limit ~~within which the European Data Protection Board shall provide such advice~~, taking into account the urgency of the matter.	
3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.	3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the ***European Parliament, the Council and*** the Commission and to the committee referred to in Article 87 and make them public.	3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.	
4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.	4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.	***deleted***	

	4a. The European Data Protection Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The European Data Protection Board shall, without prejudice to Article 72, make the results of the consultation procedure publicly available.		
	4b. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with point (b) of paragraph 1 for establishing common procedures for receiving and investigating information concerning allegations of unlawful processing and for safeguarding confidentiality and sources of information received.		
Article 67	***Article 67***	***Article 67***	
Reports	***Reports***	***Reports***	
	Amendment 176		
1. The European Data	1. The European Data Protection	***deleted***	

Protection Board shall regularly and timely inform the Commission about the outcome of its activities. It shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Union and in third countries.	Board shall regularly and timely inform the ***European Parliament, the Council and the*** Commission about the outcome of its activities. It shall draw up ~~an annual~~ ***a*** report ***at least every two years*** on the situation regarding the protection of natural persons with regard to the processing of personal data in the Union and in third countries.		
The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).	The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).	***deleted***	
2. The report shall be made public and transmitted to the European Parliament, the Council and the Commission.	2. The report shall be made public and transmitted to the European Parliament, the Council and the Commission.	2. The ***European Data Protection Board shall draw up an annual*** report ***regarding the protection of natural persons with regard to the processing of personal data in the Union and, where relevant, in third countries and international organisations. The report*** shall be made public and ***be*** transmitted to the European Parliament, the Council and the Commission.	
		3. The annual report shall include a review of the practical application of the guidelines,	

		recommendations and best practices referred to in point (c) of Article 66(1) as well as of the binding decisions referred to in paragraph 3 of Article 57.	
Article 68	***Article 68***	***Article 68***	
Procedure	***Procedure***	***Procedure***	
	Amendment 177		
1. The European Data Protection Board shall take decisions by a simple majority of its members.	1. The European Data Protection Board shall take decisions by a simple majority of its members***, unless otherwise provided in its rules of procedure***.	1. The European Data Protection Board shall ~~take decisions~~ ***adopt binding decisions referred to in paragraph 3 of Article 57 in accordance with majority requirements set out in paragraphs 2 and 3 of Article 58a. As regards decisions related to the other tasks listed in Article 66 hereof, they shall be taken*** by a simple majority of its members.	
2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. In particular, it shall provide for the continuation of exercising duties when a member's term of office expires or a member	2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. In particular, it shall provide for the continuation of exercising duties when a member's term of office expires or a member resigns, for the	2. The European Data Protection Board shall adopt its own rules of procedure ***by a two-third majority of its members*** and organise its own operational arrangements. ~~In particular, it shall provide for the continuation of exercising duties when a member's term of office~~	

resigns, for the establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 57.	establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 57.	~~expires or a member resigns, for the establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 57.~~	
Article 69	***Article 69***	***Article 69***	
Chair	***Chair***	***Chair***	
	Amendment 178		
1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members. One deputy chairperson shall be the European Data Protection Supervisor, unless he or she has been elected chair.	1. The European Data Protection Board shall elect a chair and ***at least*** two deputy chairpersons from amongst its members. ~~One deputy chairperson shall be the European Data Protection Supervisor, unless he or she has been elected chair~~.	1. The European Data Protection Board shall elect a chair and two deputy ~~chairpersons~~ chairs from amongst its members ***by simple majority***[388][389]. ~~One deputy chairperson shall be the European Data Protection Supervisor, unless he or she has been elected chair.~~	
2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable.	2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable.	2. The term of office of the chair and of the deputy ~~chairpersons~~ chairs shall be five years and be renewable ***once***[390].	

[388] ***IE proposal.***
[389] ***COM reservation on deletion.***
[390] ***COM scrutiny reservation.***

	Amendment 179		
	2a. The position of the chair shall be a full-time position.		
Article 70	***Article 70***	***Article 70***	
Tasks of the chair	***Tasks of the chair***	***Tasks of the chair***	
1. The chair shall have the following tasks:	1. The chair shall have the following tasks:	1. The chair shall have the following tasks:	
(a) to convene the meetings of the European Data Protection Board and prepare its agenda;	(a) to convene the meetings of the European Data Protection Board and prepare its agenda;	(a) to convene the meetings of the European Data Protection Board and prepare its agenda;	
		(aa) to notify decisions adopted by the European Data Protection Board pursuant to Article 58a to the lead supervisory authority and the concerned supervisory authorities;	
(b) to ensure the timely fulfilment of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.	(b) to ensure the timely fulfilment of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.	(b) to ensure the timely ~~fulfilment~~ ***performance*** of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.	
2. The European Data Protection Board shall lay down the	2. The European Data Protection Board shall lay down the attribution	2. The European Data Protection Board shall lay down the attribution	

attribution of tasks between the chair and the deputy chairpersons in its rules of procedure.	of tasks between the chair and the deputy chairpersons in its rules of procedure.	of tasks between the chair and the deputy chairpersons in its rules of procedure.	
Article 71	***Article 71***	***Article 71***	
Secretariat	***Secretariat***	***Secretariat***	
1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat.	1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat.	1. The European Data Protection Board shall have a secretariat***, which shall be provided by the secretariat of*** ~~. The~~the European Data Protection Supervisor~~ shall provide that secretariat~~.	
		1a. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the European Data Protection Board.	
		1b. The staff of the secretariat of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation shall be organizationally separated from, and subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection	

		Supervisor[391].	
		1c. Where needed, the European Data Protection Board in consultation with the European Data Protection Supervisor shall establish and publish a Code of Conduct implementing this Article and applicable to the staff of the secretariat of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation.	
	Amendment 180		
2. The secretariat shall provide analytical, administrative and logistical support to the European Data Protection Board under the direction of the chair.	2. The secretariat shall provide analytical, ***legal,*** administrative and logistical support to the European Data Protection Board under the direction of the chair.	2. The secretariat shall provide analytical[392], administrative and logistical support to the European Data Protection Board ~~under the direction of the chair~~.	
3. The secretariat shall be responsible in particular for:	3. The secretariat shall be responsible in particular for:	3. The secretariat shall be responsible in particular for:	
(a) the day-to-day business of the European Data Protection Board;	(a) the day-to-day business of the European Data Protection Board;	(a) the day-to-day business of the European Data Protection Board;	

391 CZ reservation on last part of the task.

392 ***UK suggested deleting "analytical".***

(b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public;	(b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public;	(b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public;	
(c) the use of electronic means for the internal and external communication;	(c) the use of electronic means for the internal and external communication;	(c) the use of electronic means for the internal and external communication;	
(d) the translation of relevant information;	(d) the translation of relevant information;	(d) the translation of relevant information;	
(e) the preparation and follow-up of the meetings of the European Data Protection Board;	(e) the preparation and follow-up of the meetings of the European Data Protection Board;	(e) the preparation and follow-up of the meetings of the European Data Protection Board;	
(f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection Board.	(f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection Board.	(f) the preparation, drafting and publication of opinions, ***decisions on the settlement of disputes between supervisory authorities*** and other texts adopted by the European Data Protection Board.	

Article 72	***Article 72***	***Article 72***	
Confidentiality	***Confidentiality***	***Confidentiality***[393]	
	Amendment 181		
1. The discussions of the European Data Protection Board shall be confidential.	1. The discussions of the European Data Protection Board ***may*** be confidential ***where necessary, unless otherwise provided in its rules of procedure***. ***The agendas of the meetings of the European Protection Board shall be made public***.	1. The discussions[394] of the European Data Protection Board shall be confidential.	
2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.	2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 ***of the European Parliament and of the Council***[1] or the European Data Protection Board otherwise makes them public.	2. ***Access to*** ~~Documents~~ documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be ~~confidential, unless access is granted to those documents in accordance with~~ ***governed by*** Regulation (EC) No 1049/2001~~ or the European Data Protection Board otherwise makes them public~~.	

[393] ***DE, EE, ES, RO, PL, PT, SE and UK reservation: it was thought that the EDPB should operate in a manner as transparent as possible and a general confidentiality duty was obviously not conducive to this. This article should be revisited once there is more clarity on the exact role and powers of the board, including the question whether the EDPS shall ensure the Secretariat.***

[394] ***IT scrutiny reservation: it suggested replacing this term with 'minutes' or 'summary records', thereby distinguishing between confidentiality of decision-making and access to documents.***

	[1] ***Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L145, 31.5.2001, p.43)***		
3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.	3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.	***deleted***	

CHAPTER VIII REMEDIES, LIABILITY AND SANCTIONS	CHAPTER VIII REMEDIES, LIABILITY AND SANCTIONS	CHAPTER VIII REMEDIES, LIABILITY AND SANCTIONS[395]	
Article 73	***Article 73***	***Article 73***	
Right to lodge a complaint with a supervisory authority	***Right to lodge a complaint with a supervisory authority***	***Right to lodge a complaint with a supervisory authority[396]***	
	Amendment 182		
1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.	1. Without prejudice to any other administrative or judicial remedy ***and the consistency mechanism***, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.	1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a ***single*** supervisory authority***, in particular***[397] in ~~any~~ ***the*** Member State ***of his or her habitual residemce.place of work or place of the alleged infringment*** if ~~they~~ ***data subject*** consider that the processing of personal data relating to ~~them~~ ***him or her*** does not	

395 ***AT, FR, EE, ES and RO scrutiny reservation.***

396 ***BE, CY, CZ, EE, IE, LY, PT and SI scrutiny reservation.***

397 ***COM, BG, IT and LU though that the data subject should be able to lodge a complaint with any DPA without limitation since the protection of personal data was a fundamental right.***

		comply with this Regulation[398].	
2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.	2. Any body, organisation or association which ~~aims to protect data subjects' rights and interests concerning the protection of their personal data~~ ***acts in the public interest*** and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.	***deleted***	
3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.	3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that ~~a personal data~~ breach ***of this Regulation*** has occurred.	***deleted***	

[398] ***DE, supported by NL, suggested adding "when its rights are not being respected".***

		4. (…) ***5. The supervisory authority to which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant Article 74[399] or, as regards decisions taken by the European Data Protection Board pursuant to Article 76b.***	
Article 74	***Article 74***	***Article 74***	
Right to a judicial remedy against a supervisory authority	***Right to a judicial remedy against a supervisory authority***	***Right to a judicial remedy against a supervisory authority[400]***	
	Amendment 183		
1. Each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.	1. ***Without prejudice to any other administrative or non-judicial remedy,*** ~~E~~each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.	1. ***Without prejudice to any other administrative or non-judicial remedy,*** ~~Each~~ each natural or legal person shall have the right to a***n effective*** judicial remedy against ***a legally binding*** decision~~s~~ of a supervisory authority concerning	

[399] ***NL and FR scrutiny reservation. Article 54c (2) already provides for a general duty for the supervisory authority with which a complaint has been lodged to notify the data subject of any measures taken (i.e. the scenario of a 'positive' reply by the DPA).***

[400] ***ES, PT and SI reservation. EE, IT and UK scrutiny reservation.***

		them[401].	
2. Each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 52(1).	2. ***Without prejudice to any other administrative or non-judicial remedy,*** ~~E~~each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 52(1).	2. ***Without prejudice to any other administrative or non-judicial remedy,*** ~~Each~~ each data subject shall have the right to a judicial remedy ~~obliging~~ ***where*** the supervisory authority ***competent in accordance with Article 51[402] does not deal with*** ~~to act on~~ a complaint ~~in the absence of a decision necessary to protect their rights,~~ or ~~where the supervisory authority~~ does not inform the data subject within three months ***or any shorter period provided under Union or Member State law[403]*** on the progress or outcome of the complaint ~~pursuant to point (b) of~~ ***lodged under*** Article ~~52(1)~~***73[404]***.	
3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the	3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is	3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the	

401 ***DE, supported by IE and SE, suggested adding: 'by which it is adversely affected'.***

402 ***COM reservation.***

403 ***SI indicated that under its law the DPA was obliged to reply within two months.***

404 ***SE scrutiny reservation. BE reservation. BE said that there was a link to Article 53 and the main establishment and the DPA of the habitual residence. Support from NL. IT thought that paragraphs 1 and 2 overlapped. NO wanted to delete paragraph 2 since a court review would endanger the independency of the DPA.***

supervisory authority is established.	established.	supervisory authority is established[405].	
		3a. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or decision of the European Data Protection Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.	
4. A data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State.	4. ***Without prejudice to the consistency mechanism*** ~~A~~a data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State.	***deleted***	
5. The Member States shall enforce final decisions by the	5. The Member States shall enforce final decisions by the courts	***deleted***[406]	

[405] ***IT suggests stating that proceedings may be brought before the courts of the Member state where the natural or legal person has his/her habitual residence or is established.***

[406] ***COM reservation on deletion of paragraphs 4 and 5. DE scrutiny reservation on deletion of paragraphs 4 and 5.***

courts referred to in this Article.	referred to in this ~~Article~~.		
Article 75	***Article 75***	***Article 75***	
Right to a judicial remedy against a controller or processor	***Right to a judicial remedy against a controller or processor***	***Right to a judicial remedy against a controller or processor***[407]	
1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.	1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.	1. Without prejudice to any available administrative ***or non-judicial*** remedy[408] , including the right to lodge a complaint with a supervisory authority ~~as referred to in~~ ***under*** Article 73, ~~every natural person~~ ***a data subject*** shall have the right to a***n effective*** judicial remedy[409] if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.	
	Amendment 184		
2. Proceedings against a controller or a processor shall be brought before the courts of the	2. Proceedings against a controller or a processor shall be brought before the courts of the Member	2. Proceedings against a controller or a processor shall be brought before the courts of the Member	

[407] ***DE, EE, PL, PT, SI and SK scrutiny reservation. ES, IT reservation.***

[408] ***SI wanted to delete non-judicial remedy.***

[409] ***ES asked how judicial remedy would be interpreted and how a missed deadline or that there will be no judicial review would be considered.***

Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers.	State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority ***of the Union or a Member State*** acting in the exercise of its public powers.	State where the controller or processor has an establishment[410]. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has ~~its~~ ***his or her*** habitual residence, unless the controller ***or processor*** is a public authority acting in the exercise of its public powers.	
3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism.	3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism.	***deleted***	
4. The Member States shall enforce final decisions by the courts referred to in this Article.	4. The Member States shall enforce final decisions by the courts referred to in this Article.	***deleted***	

[410] ***In view of the concerns raised, the reference to national law has been kept only in recital 113.***

Article 76	*Article 76*	*Article 76*[411]	
Common rules for court proceedings	***Common rules for court proceedings***	***Representation of data subjects***	
	Amendment 185		
1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.	1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 ~~and~~**,** 75 ~~on behalf of~~ ***and 77 if mandated by*** one or more data subjects.	1. ***The data subject shall have the right to mandate*** ~~Any~~ a body, organisation or association, ***which has been properly constituted according to the law of a Member State and whose statutory objectives include the protection of data subject's rights and freedoms with regard to the protection of their personal dat***[412]***a to lodge the complaint on hir or her behalf***[413] ***and*** ~~referred to in Article 73(2) shall have the right~~ to exercise the rights referred to in Articles ***73,*** 74 and 75 on ***his or her*** behalf[414] ~~of one or more data subjects~~.	

411 ***DE, ES, PT, RO and SI scrutiny reservation. CZ, EE, IT, NL, SI and UK thought this article was superfluous.***

412 ***COM said that consumer organisations and data protection organisations enhance fundamental rights so it was important that they could lodge complaints.***

413 ***IT scrutiny reservation.***

414 ***DE parliamentary reservation; BE, EE reservation and IT scrutiny reservation. EE, supported by FI and SE, thought that the data subject could choose anybody to represent her/him so this drafting was a limitation so a reference to national law was needed. Support from SE.***

		1a. [Independently of a data subject's mandate or complaint, any body, organisation or association referred to in paragraph 1[415] shall have the right to lodge a complaint with the supervisory authority competent in accordance with Article 51[416] if it has reasons to consider that a personal data breach referred to in Article 32(1) has occurred and Article 32(3) does not apply.[417]].	
2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union.	2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union.	***deleted***	
3. Where a competent court of a Member State has reasonable	3. Where a competent court of a Member State has reasonable	***deleted***	

[415] ***PL asked how an organisation could know about a breach. PT did not want to exclude the possibility of an organisation to lodge complaint if that was provided in national law but meant that the wording was not clear.***

[416] ***COM reservation on limitation to competent supervisory authority.***

[417] ***This paragraph was moved from Article 73(3). BE, EE, FR reservation. BG, DE, DK, IT, LU, NL, PT and UK scrutiny reservation. UK in particularly queried whether such possibility would also be open to an association when the data subject itself considered that the reply he/she had received was satisfactory. ES on the contrary thought that this possibility should not be limited to data breaches. UK thought that paragraph 1 was sufficient. For DK, PL and SE it was not acceptable that an organisation etc. had an independent right to lodge a complaint.***

grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such parallel proceedings.	grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such parallel proceedings.		
4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may suspend the proceedings.	4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may suspend the proceedings.	***deleted***	
5. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.	5. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.	***deleted***[418]	

[418] ***COM scrutiny reservation on deletion of paragraphs 3 to 5. FR reservation on the deletion of paragraphs 3 to 4.***

		Article 76a	
		Suspension of proceedings[419]	
		1. Where a competent court of a Member State has reasonable grounds to believe that proceedings concerning the same processing activities are pending in a court in another Member State, it shall[420] ***contact that court in the other Member State to confirm the existence of such proceedings.***	
		2. Where proceedings involving the same processing activities are pending in a court in another Member State, any competent court other than the court first seized may suspend[421] ***its proceedings.***	

[419] ***AT, BE, DK, EE, ES, FI, FR, IT, NL, PL, PT, SE and SI scrutiny reservation. ES thought that lis pendens necessitated the same persons, same proceeding, same object of dispute and same claim and that that could be difficult to establish.UK, supported by FR, cautioned against having a too prescriptive text, support from FR SE thought that GDPR should not regulate lis pendens, instead it should be up to the DPA and MS courts to decide. For LU this was a question of judicial cooperation between judicial authorities. NO and FR asked how this text related to Regulation No 44/2001 and the Lugano Convention FI considered that it was necessary to have rules on this question in GDPR.***

[420] ***LU supported by EL, suggested to replace "shall" with "may".***

[421] ***NL and PL thought that it was difficult to force courts to stay proceedings waiting for another court to decide. NL asked how it was possible for a court to know that another case was going on elsewhere. COM thought that limitation to "same parties" was not appropriate here.***

		2a. Where these proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.[422]	
		Article 76b	
		Actions before the Court of Justice of the European Union against decisions by the European Data Protection Board	
		1. Actions may be brought before the Court of Justice of the European Union in accordance with Article 263 TFEU, in order for it to review the legality of decisions taken by the European Data Protection Board pursuant to Article 58a. Such actions may be brought before the Court of Justice of the European Union by supervisory authorities, Member States and the Union institutions	

[422] ***Based on Article 28 of Brussels I Regulation.***

		as well as by natural or legal persons to whom decisions taken by the European Data Protection Board have been notified or to whom such decisions are of direct and individual concern, including data subjects who have lodged a complaint in accordance with Article 73.	
		2. The expiration of the time-period provided for in the sixth subparagraph of Article 263 TFEU and the Rules of Procedure of the General Court shall not bar the persons referred to in paragraph 1 from calling in question the lawfulness of any decision taken by the European Data Protection Board before the national courts in accordance with Article 74 or 75 and those national courts from requesting the Court of Justice of the European Union a preliminary ruling concerning the validity of any decision taken by the European Data Protection Board in accordance with Article 267 TFEU.	

		3. Where the European Data Protection Board notifies its decision in accordance with Article 58a(6), such a notification shall state the possibility for the persons referred to in paragraph 1 to bring an action for annulment before the General Court of the European Union in accordance with Article 263 TFEU as well as the time-period for such an action in accordance with the sixth subparagraph of Article 263 TFEU and the Rules of Procedure of the General Court. It shall also refer to the additional right conferred on that person pursuant to paragraph 2.	
		4. In the event that the European Data Protection Board has an obligation to act and fails to take a decision, proceedings for failure to act may be brought before the Court of Justice of the European Union in accordance with Article 265 TFEU.	
		5. The European Data Protection Board shall be required to take the necessary measures to comply	

		with the judgment of the Court of Justice of the European Union.	
Article 77	***Article 77***	***Article 77***	
Right to compensation and liability	***Right to compensation and liability***	***Right to compensation and liability***[423]	
	Amendment 186		
1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.	1. Any person who has suffered damage***, including non-pecuniary damage,*** as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to ~~receive~~ ***claim*** compensation from the controller or the processor for the damage suffered.	1. Any person who has suffered[424] damage[425] as a result of ~~an unlawful~~a processing operation ~~or of an action incompatible~~ ***which is not in compliance*** with this Regulation shall have the right to receive compensation from the controller or ~~the~~ processor[426] for the damage suffered[427].	

[423] ***Several Member States (DE, NL and UK) have queried whether there was an EU concept of damage and compensation or whether this was left to Member State law. IT suggested specifying that these rules are to be applied according to national law, support from CZ, NL, RO and SI. COM thinks that it has to be left to ECJ to interpret these rules and concepts. FR scrutiny reservation; FR questioned the division of responsibilities and the link to Articles 24 and 25 and national law in this field as well as the principle of subsidiarity.***

[424] ***DE, HU and SK suggested adding "material or immaterial/moral". NO suggested clarifying this in a recital.***

[425] ***BE asked whether a violation of the principles of the Regulation was enough to constitute a damage or whether the data subject had to prove a specific damage (obligation de moyens ou de résultat). COM said that the data subject had to prove the damage.***

[426] ***DE suggested restricting the possibility to seek compensation from the processor to cases where, in violation of point (a) of paragraph 2 of Article 26, the processor has processed personal data contrary to or in the absence of instructions from the controller. ES suggested adding a reference to 'a right to exercise a direction action', but this is already encompassed in the current draft.***

[427] ***SE supported by HU considered that Article 77 was unclear and wanted to know whether both an economic and immaterial damage was covered.***

	Amendment 187		
2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.	2. Where more than one controller or processor is involved in the processing, each ~~controller~~ ***of those controllers*** or ~~processor~~ ***processors*** shall be jointly and severally liable for the entire amount of the damage***, unless they have an appropriate written agreement determining the responsibilities pursuant to Article 24***.	2. [428]Where more than one controller or processor ***or a controller and processor*** ~~is~~ are involved in the processing ***which gives rise to the damage***, each controller or processor shall be jointly[429] and severally liable for the entire amount of the damage***. This is without prejudice to recourse claims between controllers and/or processors***[430]***.***	
3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.	3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.	3. The controller or the processor may[431] be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage[432].	
		4. Court proceedings for	

[428] ***IE queried why the reference to Article 24(2) had been removed and then the second sentence had been added: what the purpose to bring a claim against all of them and then sort out the individual responsibility?***

[429] ***UK thought that one controller or processor might be more responsible than another so it should be allowed for a relative responsibility. SE said that according Directive 95/46 (Article 23) the burden of proof and division of responsibility between the controller and the processor it was only the controller that was held responsible.***

[430] ***SI reservation: SI thought this paragraph could be deleted and left entirely to national law.***

[431] ***PL thought this should be turned into a mandatory provision.***

[432] ***DE and PL thought this paragraph needed to be further elaborated. DE in particular thought that the relationship to Article 39 needed to be further clarified. SI thought an arrangement for strict liability in the case of processing by public bodies should be inserted into this paragraph.***

		exercising the right to receive compensation shall be brought before the courts with jurisdiction for compensation claims under national law of the Member State referred to in paragraph 2 of Article 75.	
Article 78	***Article 78***	***Article 78***	
Penalties	***Penalties***	***Penalties***	
1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive.	1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive.	***deleted***[433]	
2. Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be	2. Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be	***deleted***	

[433] ***This Article was moved to Article 79b. Scrutiny reservation by SK, RO and PT.***

initiated against the controller.	initiated against ~~the controller~~.		
3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	***deleted***	
Article 79	***Article 79***	***Article 79***	
Administrative sanctions	***Administrative ~~sanctions~~***	***General conditions for imposing administrative ~~sanctions~~fines***[434]	
	Amendment 188		
1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.	1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article. ***The supervisory authorities shall co-operate with each other in accordance with Articles 46 and 57 to guarantee a harmonized level of sanctions within the Union.***	1. Each supervisory authority ***[competent in accordance with Articl 51]*** shall be empowered to impose administrative ~~sanctions in accordance with~~ ***fines purusant to*** this Article ***in respect of infringements of this Regulation referred to in Article 79a. Administrative fines shall, depending on the circumstances of each individual case, be imposed***	

[434] ***DK reservation: it indicated that this system of administrative fining was incompatible with its constitutional legal system. PL thought that Article 79 should set out guidelines only, with possibly a maximum threshold for the DPA to impose fines.***

		in addition to, or instead of, measures referred to in Article 53[435].	
2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.	2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. ~~The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.~~	2. ~~The administrative~~ Administrative ~~sanction~~ ***fines imposed pursuant to Article 79a*** shall ~~be~~ in each individual case be effective, proportionate and dissuasive. ~~The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.~~	
	2a. To anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following		

[435] ***Some delegations thought that the corrective measures of Article 53 (1b) should be listed rather here.***

	sanctions:		
	a) a warning in writing in cases of first and non-intentional non-compliance;		
	b) regular periodic data protection audits;		
	c) a fine up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is higher.		
	2b. If the controller or the processor is in possession of a valid "European Data Protection Seal" pursuant to Article 39, a fine pursuant to point (c) of paragraph 2a shall only be imposed in cases of intentional or negligent ~~in~~non-compliance.		
	2c. The administrative sanction shall take into account the following factors:		
	a) the nature, gravity and duration of the ~~in~~non-compliance,		
	b) the intentional or negligent character of the infringement,		

	c) the degree of responsibility of the natural or legal person and of previous breaches by this person,		
	d) the repetitive nature of the infringement,		
	e) the degree of co-operation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement,		
	f) the specific categories of personal data affected by the infringement,		
	(g) the level of damage, including non-pecuniary damage, suffered by the data subjects,		
	(h) the action taken by the controller or processor to mitigate the damage suffered by data subjects,		
	(i) any financial benefits intended or gained, or losses avoided, directly or indirectly from the infringement,		

	(j) the degree of technical and organisational measures and procedures implemented pursuant to: ***(i) Article 23 - Data protection by design and by default*** ***(ii) Article 30 - Security of processing*** ***(iii) Article 33 - Data protection impact assessment*** ***(iv) Article 33a - Data protection compliance review*** ***(v) Article 35 - Designation of the data protection officer***		
	(k) the refusal to cooperate with or obstruction of inspections, audits and controls carried out by the supervisory authority pursuant to Article 53,		
	(l) other aggravating or mitigating factors applicable to the circumstance of the case.		
		2a. When deciding whether to impose an administrative fine in addition to, or instead of, measures referred to in points (a)	

		to (f) of paragraph 1b of Article 53[436] and [437]deciding on the amount of the administrative fine in each individual case due regard shall be had to the following:	
		(a) the nature, gravity and duration of the infringement having regard to the nature scope or purpose of the processing concerned;	
		(b) the intentional or negligent character of the infringement,	
		(c) the number of data subjects affected by the infringement and the level of damage suffered by them;	
		(d) action taken by the controller or processor to mitigate the damage suffered by data subjects;	
		(e) the degree of responsibility of the controller or processor	

436 ***Moved here from paragraph 2b (further to remarks by FR, IE, IT and CZ).***

437 ***Some delegations (EE, SK, PL) thought that aggravating circumstances should be distinguished from mitigating circumstances. SK suggested laying down exact thresholds (e.g. more than 2/3 of the maximum fine in case of aggravating circumstances). IT thought the possibility of EDPB guidance should be referred to here. NL thought that the status of codes of conduct and certification as well as the consequences of adhering to them needed to be looked at.***

		having regard to technical and organisational measures implemented by them pursuant to Articles 23 and 30;	
		(f) any previous infringements by the controller or processor;	
		[(g) any financial benefits gained, or losses avoided, directly or indirectly from the infringement[438];]	
		(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement[439];	
		(i) in case measures referred to in point (b) and (c) of paragraph 1 and points (a), (d), (e) and (f) of paragraph 1b of Article 53, have previously been ordered against the controller or processor concerned with regard to the same	

[438] ***DK, ES and SI reservation. SI stated that a DPA was not equipped to assess this.***

[439] ***CZ was concerned that this factor might amount to a violation of the privilege against self-incrimination***

		subject-matter[440], compliance with these measures ;	
		(j) adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39[441];	
		(k) (…)[442]; ***(l) (…)[443];*** ***(m) any other aggravating or mitigating factor applicable to the circumstances of the case.***	
3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:	***deleted***	***deleted[444]***	
a) a natural person is processing personal data without a commercial	***deleted***	***deleted***	

[440] ***This should also accommodate concerns regarding the privilege against self-incrimination by removing a general reference to co-operation in the investigation. IT thought this paragraph should refer more generally to previous incidents. DE pleaded for its deletion.***

[441] ***DE reservation: DE pointed out that non-adherence to approved codes of conduct or approved certification mechanisms could as such not amount to a violation of the Regulation.***

[442] ***Removed at the suggestion of DE and SK.***

[443] ***If Member states are entirely free to decide whether or not to provide for sanctions against public authorities, it does not seem appropriate to list the fact that the controller is a public body here.***

[444] ***COM reservation on deletion; linked to reservation on Article 79a.***

interest; or			
b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.	***deleted***	b) ~~an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.~~ ***Each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State[445].***	
4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:	***deleted***	4. ~~The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:~~ ***The exercise by the supervisory authority [competent in accordance with Article 51] of its powers under this Article shall be subject to appropriate procedural safeguards in conformity with Union law and Member State law, including effective judicial remedy and due process.***	

[445] ***DE would prefer to rule out this possibility in the Regulation. ES thought it should be provided that no administrative fines can be imposed on the public sector.***

(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);	***deleted***	***deleted***	
(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).	***deleted***	***deleted***	
5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:	***deleted***	***deleted***	
(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;	***deleted***	***deleted***	
(b) does not provide access for the data subject or does not rectify	***deleted***	***deleted***	

personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13;			
(c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17;	***deleted***	***deleted***	
(d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18;	***deleted***	***deleted***	
(e) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24;	***deleted***	***deleted***	
(f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article	***deleted***	***deleted***	

31(4), and Article 44(3);			
(g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.	***deleted***	***deleted***	
6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:	***deleted***	***deleted***	
(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;	***deleted***	***deleted***	
(b) processes special categories of data in violation of Articles 9 and 81;	***deleted***	***deleted***	
(c) does not comply with an objection or the requirement	***deleted***	***deleted***	

pursuant to Article 19;			
(d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;	***deleted***	***deleted***	
(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;	***deleted***	***deleted***	
(f) does not designate a representative pursuant to Article 25;	***deleted***	***deleted***	
(g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;	***deleted***	***deleted***	
(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;	***deleted***	***deleted***	

(i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;	***deleted***	***deleted***	
(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;	***deleted***	***deleted***	
(k) misuses a data protection seal or mark in the meaning of Article 39;	***deleted***	***deleted***	
(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;	***deleted***	***deleted***	
(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);	***deleted***	***deleted***	

(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);	***deleted***	***deleted***	
(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.	***deleted***	***deleted***	
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.	7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the ***absolute*** amounts of the administrative fines referred to in ~~paragraphs 4, 5 and 6~~***paragraph 2a***, taking into account the criteria ***and factors*** referred to in ~~paragraph~~	***deleted***	

	paragraphs 2 ***and 2c***.		
		Article 79a	
		Administrative fines[446][447]	
		1. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR, or in case of an undertaking […] %[448] ***of its total worldwide annual turnover***[449] ***of the preceding financial year, on a controller who, intentionally or negligently***[450]***:***	

446 ***DE, EE, ES, PT and SI scrutiny reservation. FI and SI reservation. COM reservation on replacing 'shall' by 'may' and the deletion of amounts and percentages in paragraphs 1, 2 and 3. DE wanted the risk-based approach to be made clearer. DE thought that proportionality was important because Article 79a concerned fundamental rights/rule of law and deemed it disproportionate that a supervisory authority could impose a fine that the data subject was unaware of. DE said that it was necessary to set out the fines clearly and that the one-stop shop principle did not allow for exceptions being set out in national law. IE thought e gravity of offences was not sufficiently illustrated, e.g. infringement in para. 3(m), which according to IE is the most serious one. FR reservation: the strictness of the text may impinge on the independence of the DPA.***

447 ***A majority of Member States (BE, CY DE, EE, ES, FI, IT, LV, LU, MT and NL) appear to be in favour of different scales of sanctions. COM referred to the Market Abuse Regulation with three levels of fines. DK, HU, IE, SE and UK were opposed to maintaining different sanctions scales. FR and PL did not favour it, but could accept it.***

448 ***EE did not consider it appropriate to set out sanctions in percentage because the sanction was not predictable.. PT considered that there should be minimum penalties for a natural person and that for SMEs and micro enterprises the volume of the business should not be looked at when applying the fines (this factor should only be applicable for multinationals). PL thought that administrative fines should be implemented in the same way in all MS. PL said that the fines should be flexible and high enough to represent a deterrent, also for overseas companies***

449 ***UK commented that turnover was used in competition law and asked whether the harm was the same here. EE asked how the annual turnover was connected to the sanction. SI thought that compared to competition law where the damage concerned the society as a whole, data protection concerned private infringements. COM said that both competition law and data protection concern economic values, whereas data protection protects values of the data subject.***

450 IT wanted to delete "intentionally or negligently" and thought that those notions were already integrated part of the mechanism to calculate fines.

		(a) does not respond within the period referred to in Article 12(2) to requests of the data subject;	
		(b) charges a fee in violation of the first sentence of paragraph 4 of Article 12.	
		2. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR, or in case of an undertaking […]% of its total worldwide annual (…) turnover of the preceding financial year[451], on a controller or processor who, intentionally or negligently:[452]	
		(a) does not provide the information, or provides incomplete information, or does not provide the information timely or in a sufficiently transparent manner, to the data subject pursuant to Articles 12(3),14 and 14a;	

[451] ***DE suggestion.***

[452] ***IT considered that paragraphs 2 and 3 were very generic and only described the infringements but that the scale of gravity was not well defined. IT asked for a better categorisation of the infringements.***

		(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not comply with the rights and obligations pursuant to Articles 17, 17a, 17b, 18 or 19;	
		(c) (...) ***(d) (...)*** ***(e) does not or not sufficiently determine the respective responsibilities with joint controllers pursuant to Article 24;***	
		(f) does not or not sufficiently maintain the documentation pursuant to Article 28 and Article 31(4).	
		3. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR or, in case of an undertaking, […] % of its total worldwide annual turnover of the preceding financial year[453], on a controller or	

[453] ***DE suggestion.***

		processor who, intentionally or negligently:	
		(a) processes personal data without a [454] legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7, 8 and 9;	
		(b) (…); ***(c) (…);*** ***(d) does not comply with the conditions in relation to profiling pursuant to Article 20;***	
		(e) does not implement appropriate measures or is not able to demonstrate compliance pursuant to Articles 22 and 30;	
		(f) does not designate a representative in violation of Article 25;	
		(g) processes or instructs the processing of personal data in violation of Articles 26;	
		(h) does not alert on or notify a	

[454] ***FI pointed out that "sufficient" was unclear taking into consideration of the principles in Article 6 (f).***

		personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject in violation of Articles 31 and 32;	
		(i) does not carry out a data protection impact assessment in violation of Article 33 or processes personal data without prior consultation of the supervisory authority in violation of Article 34(1);	
		(j) (…); ***(k) misuses a data protection seal or mark in the meaning of Article 39 or does not comply with the conditions and procedures laid down in Articles 38a and 39a;***	
		(l) carries out or instructs a data transfer to a recipient in a third country or an international organisation in violation of Articles 40 to 44;	
		(m) does not comply with an order or a temporary or definite ban on processing or the	

		suspension of data flows by the supervisory authority pursuant to Article 53(1) or does not provide access in violation of Article 53(2).	
		[3a. If a controller or processor intentionally or negligently violates several provisions of this Regulation listed in paragraphs 1, 2 or 3, the total amount of the fine may not exceed the amount specified for the gravest violation.]	
		4. [The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of adjusting the maximum amounts of the administrative fines referred to in paragraphs 1, 2 and 3 to monetary developments, taking into account the criteria referred to in paragraph 2a of Article 79.][455]	

[455] ***CZ, DE, NL and RO reservation. NL that thought that guidelines from the EDPB could solve the problems on the amounts. CZ wanted to delete the paragraph and thought that the DPA could set out the amounts.***

		Article 79b	
		Penalties[456]	
		1. For infringements of the provisions of this Regulation not listed in Article 79a Member States shall[457] ***lay down the rules on penalties applicable to such infringements and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.***	
		2. (…). ***3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.***	

456 ***DE, DK, EE, ES, IT, PL and PT and SK scrutiny reservation. COM explained that infringements not listed in Article 79a were those under national law, referred to in Chapter IX, for example infringements in employment law and relating to freedom of expression. In that way Article 79b is complementary to the list in Article 79and does not exclude other penalties. IT thought it was better to delete the Article but lay down the possibility to legislate at national level. FR reservation on the imposition of criminal penalties. DE in favour of referring expressis verbis to criminal penalties.***

457 ***BE and EE reservation.***

CHAPTER IX PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS	**CHAPTER IX PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS**	**CHAPTER IX PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS**	
Article 80	***Article 80***	***Article 80***	
Processing of personal data and freedom of expression	***Processing of personal data and freedom of expression***	***Processing of personal data and freedom of expression and information***	
	Amendment 189		
1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data	1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI**,** on co-operation and consistency in Chapter VII ~~for the processing of personal data carried out solely for journalistic purposes~~	1. ***The national law of the*** Member State~~s~~ shall ~~provide for exemptions or derogations from the provisions on the general principles in Chapter II,~~ ***reconcile*** the right~~s of the data subject in Chapter III, on controller and processor in Chapter IV, on~~ ***t*** the ~~transfer~~ ***protection*** of personal data ***pursuant to this Regulation*** ~~to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for~~	

carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.	~~or the purpose of artistic or literary expression~~ ***and specific data processing situations in this Chapter ~~IX~~ whenever this is necessary*** in order to reconcile the right to the protection of personal data with the rules governing freedom of expression ***in accordance with the Charter ~~of Fundamental Rights of the European Union~~***.	***with the right to freedeom of expression and information, including*** the processing of personal data ~~carried out solely~~ for journalistic purposes ~~or~~ the purposes of ***academic,*** artistic or literary expression ~~in order to reconcile the right to the protection of personal data with the rules governing freedom of expression~~.	
2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.	2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.	***2. For the processing of personal data carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall[458] provide for exemptions or derogations from the provisions in Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organizations), Chapter VI (independent supervisory authorities), Chapter***	

[458] ***HU, AT, SI and SE reservation; they would prefer not to limit this paragraph to journalistic processing.***

		VII (co-operation and consistency)[459] if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.	
	Amendment 190		
	Article 80a (new)		
	Access to documents		
	1. Personal data in documents held by a public authority or a public body may be disclosed by this authority or body in accordance with Union or Member State legislation regarding public access to official documents, which reconciles the right to the protection of personal data with the principle of public access to official documents.		
	2. Each Member State shall notify to the Commission provisions of its law which it adopts pursuant to		

[459] ***BE, DE, FR, IE and SE had requested to include also a reference to Chapter VIII. This was opposed to by COM. The Presidency points out that in case the freedom of expression prevails over the right to data protection, there will obviously no infringement to sanction. Where an infringement is found to have place, the interference with the freedom of expression will have to taken into account as an element in the determination of the sanction. This application of the proportionality principle should be reflected in Chapter VIII.***

	paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.		
		Article 80a	
		Processing of personal data and public access to official documents [460]	
		Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union law or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.	

[460] ***SK and PT scrutiny reservation.***

		Article 80aa	
		Processing of personal data and reuse of public sector information	
		Personal data in in public sector information held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union law or Member State law to which the public authority or body is subject in order to reconcile the reuse of such official documents and public sector information with the right to the protection of personal data pursuant to this Regulation[461].	
		Article 80b[462]	
		Processing of national identification number	
		Member States may determine the specific conditions for the processing of a national	

[461] ***COM reservation in view of incompatibility with existing EU law, in particular Directive 2003/98/EC (as amended by Directive 2013/37/EU).***

[462] ***DK, PL, SK scrutiny reservation.***

		identification number or any other identifier of general application. In this case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.	
Article 81	***Article 81***	***Article 81***	
Processing of personal data concerning health	***Processing of personal data concerning health***	***Processing of personal data ~~concerning~~ for health~~-~~ related purposes***	
	Amendment 191		
1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be	1. ~~Within the limits of~~ ***In accordance with the rules set out in*** this Regulation ~~and in accordance~~***, in particular*** with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable***, consistent,*** and specific	***deleted***[463]	

[463] ***See Article 9(2)(g),(h), (hb) and (4) which enshrine the basic idea, previously expressed in Article 81, that sensitive data may be processed for purposes of medicine, health-care, public health and other public interests, subject to certain appropriate safeguards based on Union law or Member State law. This text is not part of the partial general approach which the Council is asked to agree at its meeting of 4 December 2014 and will be subject to further scrutiny at technical level.***

necessary for:	measures to safeguard the data subject's ~~legitimate~~ interests, and ~~be~~ ***fundamental rights, to the extent that these are*** necessary ***and proportionate***, ***and of which the effects shall be foreseeable by the data subject,*** for:		
(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or	(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or	***deleted***	
(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or	(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices, ***and if the processing is carried out by a person bound by a confidentiality***	***deleted***	

	obligation; or		
(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.	(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system ***and the provision of health services. Such processing of personal data concerning health for reasons of public interest shall not result in data being processed for other purposes, unless with the consent of the data subject or on the basis of Union or Member State law.***	***deleted***	
	1a. When the purposes referred to in points (a) to (c) of paragraph 1 can be achieved without the use of personal data, such data shall not be used for those purposes, unless based on the consent of the data subject or Member State law.		
	1b. Where the data subject's consent is required for the processing of medical data exclusively for public health purposes of scientific research, the consent may be given for one or		

	more specific and similar researches. However, the data subject may withdraw the consent at any time.		
	1c. For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Directive 2001/20/EC of the European Parliament and of the Council[48e1] shall apply. ***[48e1] Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practices in the conduct of clinical trials on medicinal products for human use (OJ L121, 1.5.2001, p.34)***		
2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and	2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes~~, such as patient registries set up for improving diagnoses and~~	***deleted***	

differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.	~~differentiating between similar types of diseases and preparing studies for therapies, is~~ ***shall be permitted only with the consent of the data subject, and shall be*** subject to the conditions and safeguards referred to in Article 83.		
	2a. Member States law may provide for exceptions to the requirement of consent for research, as referred to in paragraph 2, with regard to research that serves a high public interest, if that research cannot possibly be carried out otherwise. The data in question shall be anonymised, or if that is not possible for the research purposes, pseudonymised under the highest technical standards, and all necessary measures shall be taken to prevent unwarranted re-identification of the data subjects. However, the data subject shall have the right to object at any time in accordance with Article 19.		
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying	3. The Commission shall be empowered to adopt***, after requesting an opinion of the European Data Protection Board,***	***deleted***	

other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.	delegated acts in accordance with Article 86 for the purpose of further specifying ~~other reasons of~~ public interest in the area of public health as referred to in point (b) of paragraph 1~~, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1~~ ***and high public interest in the area of research as referred to in paragraph 2a.***		
	3a. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.		
Article 82	***Article 82***	***Article 82***	
Processing in the employment context	***Minimum standards for*** ~~P~~processing ***data*** in the employment context	***Processing in the employment context***	
	Amendment 192		
1. Within the limits of this Regulation, Member States may	1. ~~Within the limits of this Regulation,~~ Member States may***, in***	1. ~~Within the limits of this Regulation,~~ Member States may	

adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.	***accordance with the rules set out in this Regulation, and taking into account the principle of proportionality,*** adopt by ~~law~~ ***legal provisions*** specific rules regulating the processing of employees' personal data in the employment context, in particular ~~for~~ ***but not limited to*** the purposes of the recruitment ***and job applications within the group of undertakings***, the performance of the contract of employment, including discharge of obligations laid down by law ~~or~~ ***and*** by collective agreements, ***in accordance with national law and practice,*** management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship. ***Member States may allow for collective agreements to further specify the provisions set out in this Article.***	~~adopt~~ by law specific rules ***or by collective agreements, provide for more specific[464] rules to ensure the protection of the rights and freedoms in respect of*** ~~regulating~~ the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, ***equality and diversity in the workplace,*** health and safety at work, ***protection of employer's or customer's property*** and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.	

[464] ***DE, supported, by AT, CZ, HU, DK and SI, wanted to refer to 'stricter' rules.***

	1a. The purpose of processing such data must be linked to the reason it was collected for and stay within the context of employment. Profiling or use for secondary purposes shall not be allowed.		
	1b. Consent of an employee shall not provide a legal basis for the processing of data by the employer when the consent has not been given freely.		
	1c. Notwithstanding the other provisions of this Regulation, the legal provisions of Member States referred to in paragraph 1 shall include at least the following minimum standards:		
	(a) the processing of employee data without the employees' knowledge shall not be permitted. Notwithstanding the first sentence, Member States may, by law, provide for the admissibility of this practice, by setting appropriate deadlines for the deletion of data, providing there exists a suspicion based on factual indications that must be documented that the		

	employee has committed a crime or serious dereliction of duty in the employment context, providing also the collection of data is necessary to clarify the matter and providing finally the nature and extent of this data collection are necessary and proportionate to the purpose for which it is intended. The privacy and private lives of employees shall be protected at all times. The investigation shall be carried out by the competent authority;		
	(b) the open optical-electronic and/or open acoustic-electronic monitoring of parts of an undertaking which are not accessible to the public and are used primarily by employees for private activities, especially in bathrooms, changing rooms, rest areas, and bedrooms, shall be prohibited. Clandestine surveillance shall be inadmissible under all circumstances;		
	(c) where undertakings or authorities collect and process personal data in the context of medical examinations and/or		

	aptitude tests, they must explain to the applicant or employee beforehand the purpose for which these data are being used, and ensure that afterwards they are provided with ~~these~~ those data together with the results, and that they receive an explanation of their significance on request. Data collection for the purpose of genetic testing and analyses shall be prohibited as a matter of principle;		
	(d) whether and to what extent the use of telephone, e-mail, internet and other telecommunications services shall also be permitted for private use may be regulated by collective agreement. Where there is no regulation by collective agreement, the employer shall reach an agreement on this matter directly with the employee. In so far as private use is permitted, the processing of accumulated traffic data shall be permitted in particular to ensure data security, to ensure the proper operation of telecommunications networks and telecommunications services and		

	for billing purposes.		
	Notwithstanding the third sentence, Member States may, by law, provide for the admissibility of this practice, by setting appropriate deadlines for the deletion of data, providing there exists a suspicion based on factual indications that must be documented that the employee has committed a crime or serious dereliction of duty in the employment context, providing also the collection of data is necessary to clarify the matter and providing finally the nature and extent of this data collection are necessary and proportionate to the purpose for which it is intended. The privacy and private lives of employees shall be protected at all times. The investigation shall be carried out by the competent authority;		
	(e) workers' personal data, especially sensitive data such as political orientation and membership of and activities in trade unions, may under no circumstances be used to put workers on so-called 'blacklists',		

	and to vet or bar them from future employment. The processing, the use in the employment context, the drawing-up and passing-on of blacklists of employees or other forms of discrimination shall be prohibited. Member States shall conduct checks and adopt adequate sanctions in accordance with Article 79(6) to ensure effective implementation of this point.		
	1d. Transmission and processing of personal employee data between legally independent undertakings within a group of undertakings and with professionals providing legal and tax advice shall be permitted, providing it is relevant to the operation of the business and is used for the conduct of specific operations or administrative procedures and is not contrary to the interests and fundamental rights of the person concerned which are worthy of protection. Where employee data are transmitted to a third country and/or to an international organization, Chapter V shall apply.		

2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to ~~paragraph~~ ***paragraphs 1 and 1b***, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	2.***[*** Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.***]***	
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.	3. The Commission shall be empowered, ***after requesting an opinion from the European Data Protection Board,*** to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.	3. ~~The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1~~ ***Member States may by law determine the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee[465].***	

[465] ***This paragraph may need to be looked at again in the context of the discussions on Articles 7 and 8 for consent. COM, PL, PT scrutiny reservation.***

	Amendment 193		
	Article 82a		
	Processing in the social security context		
	1. Member States may, in accordance with the rules set out in this Regulation, adopt specific legislative rules particularising the conditions for the processing of personal data by their public institutions and departments in the social security context if carried out in the public interest.		
	2. Each Member State shall notify to the Commission those provisions which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.		

Article 83	***Article 83***	***Article 83***	
Processing for historical, statistical and scientific research purposes	***Processing for historical, statistical and scientific research purposes***	***Derogations applying to ~~Processing~~ processing of personal data for archiving, ~~historical, statistical and~~ scientific, ~~research~~ statistical and historical purposes***	
	Amendment 194		
1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:	1. ~~Within the limits of~~***In accordance with the rules set out in*** this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:	1. ~~Within the limits of this Regulation,~~ ***Where*** personal data ~~may be~~ ***are*** processed for scientific, statistical[466] or historical, ~~statistical or scientific research~~ purposes ~~only if:~~***Union or Member State law may, subject to appropriate safeguards for the rights and freedoms of the data subject, provide for derogations from Articles 14a(1) and (2), 15, 16, 17, 17a, 17b, 18 and 19[467], insofar as such derogation is necessary for the fulfilment of the specific purposes.***	
(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not	(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not	(a) ~~these purposes cannot be otherwise fulfilled by processing data which does not permit or not~~	

[466] ***PL and SI would want to restrict this to statistical processing in the public interest.***

[467] ***NL and DK proposed adding a reference to Article 7. SI supported this as far as scientific processing is concerned. PL suggested deleting the reference to Article 19.***

any longer permit the identification of the data subject;	any longer permit the identification of the data subject;	~~any longer permit the identification of the data subject;~~ ***Where personal data are processed for archiving purposes in the public interest, Union or Member State law may, subject to appropriate safeguards for the rights and freedoms of the data subject, provide for derogations from Articles 14a(1) and (2), 15, 16, 17, 17a, 17b, 18, 19, 23, 32, 33 and 53 (1b)(d) and (e), insofar as such derogation is necessary for the fulfilment of these purposes***[468]***.***	
(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.	(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information ~~as long as these purposes can be fulfilled in this manner~~ ***under the highest technical standards, and all necessary measures are taken to prevent unwarranted re-identification of the data subjects.***	(b) ~~data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner~~***In case a type of processing referred to in paragraphs 1 and 1a serves at the same time another purpose, the derogations allowed for apply only to the processing for the purposes referred to in those paragraphs.***	

[468] ***COM and AT thought the list of articles from which can be derogated should be more limited.***

2. Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:	***deleted***	2. ~~Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:~~ ***The appropriate safeguards referred to in paragraphs 1 and 1a shall be laid down in Union or Member State law and be such to ensure that technological and/or organisational protection measures pursuant to this Regulation are applied to the personal data, to minimise the processing of personal data in pursuance of the proportionality and necessity principles, such as pseudonymising the data, unless those measures prevent achieving the purpose of the processing and such purpose cannot be otherwise fulfilled within reasonable means.***	
(a) the data subject has given consent, subject to the conditions laid down in Article 7;	***deleted***	***deleted***	
(b) the publication of personal data is necessary to present research findings or to facilitate	***deleted***	***deleted***	

research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or			
(c) the data subject has made the data public.	***deleted***	***deleted***	
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.	***deleted***	***deleted***	
	Amendment 195		
	Article 83a		
	Processing of personal data by archive services		
	1. Once the initial processing for which they were collected has been		

	completed, personal data may be processed by archive services whose main or mandatory task is to collect, conserve, provide information about, exploit and disseminate archives in the public interest, in particular in order to substantiate individuals' rights or for historical, statistical or scientific research purposes. These tasks shall be carried out in accordance with the rules laid down by Member States concerning access to and the release and dissemination of administrative or archive documents and in accordance with the rules set out in this Regulation, specifically with regard to consent and the right to object.		
	2. Each Member State shall notify to the Commission provisions of its law which it adopts pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.		

Article 84	***Article 84***	***Article 84***	
Obligations of secrecy	***Obligations of secrecy***	***Obligations of secrecy***[469]	
	Amendment 196		
1. Within the limits of this Regulation, Member States may adopt specific rules to set out the investigative powers by the supervisory authorities laid down in Article 53(2) in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.	1. ~~Within the limits of~~ ***In accordance with the rules set out in*** this Regulation, Member States ~~may adopt~~ ***shall ensure that*** specific rules ~~to set~~ ***are in place setting*** out the ~~investigative~~ powers by the supervisory authorities laid down in Article 53~~(2)~~ in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of	1. ~~Within the limits of this Regulation,~~ Member States may adopt specific rules to set out the ~~investigative~~ powers by the supervisory authorities laid down in ***points (da) and (db) of*** Article 53(~~2~~1) in relation to controllers or processors that are subjects under ~~national~~ ***Union or Member State*** law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy ***or to a code of professional ethics supervised and enforced by professional bodies***, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained	

[469] ***DE and UK scrutiny reservation.***

	secrecy.	in an activity covered by this obligation of secrecy.	
2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	
Article 85	***Article 85***	***Article 85***	
Existing data protection rules of churches and religious associations	***Existing data protection rules of churches and religious associations***	***Existing data protection rules of churches and religious associations***[470]	
	Amendment 197		
1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this	1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, ~~comprehensive~~ ***adequate*** rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this	1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this	

[470] ***MT, NL, AT and PT reservation.***

Regulation.	Regulation.	Regulation.	
2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 shall provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation.	2. Churches and religious associations which apply ~~comprehensive~~ ***adequate*** rules in accordance with paragraph 1 shall ~~provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation~~ ***obtain a compliance opinion pursuant to Article 38***.	2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1, shall ***be subject to the control*** ~~provide for the establishment~~ of an independent supervisory authority ***which may be specific, provided that fulfuls the conditions laid down*** in ~~accordance with~~ Chapter VI of this Regulation.	
	Amendment 198		
	Article 85a (new)		
	Respect of fundamental rights		
	This Regulation shall not have the effect of modifying the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the TEU.		
	Amendment 199		
	Article 85b (new)		
	Standard Forms		
	1. The Commission may, taking		

	into account the specific features and necessities of various sectors and data processing situations, lay down standard forms for:		
	(a) specific methods to obtain verifiable consent referred to in Article 8(1),		
	(b) the communication referred to in Article 12(2), including the electronic format,		
	(c) providing the information referred to in paragraphs 1 to 3 of Article 14,		
	(d) requesting and granting access to the information referred to in Article 15(1), including for communicating the personal data to the data subject,		
	(e) documentation referred to in paragraph 1 of Article 28,		
	(f) breach notifications pursuant to Article 31 to the supervisory authority and the documentation referred to in Article 31(4),		

	(g) prior consultations referred to in Article 34, and for informing the supervisory authorities pursuant to Article 34(6).		
	2. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises.		
	3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).		

CHAPTER X DELEGATED ACTS AND IMPLEMENTING ACTS	CHAPTER X DELEGATED ACTS AND IMPLEMENTING ACTS	CHAPTER X DELEGATED ACTS AND IMPLEMENTING ACTS[471]	
Article 86	***Article 86***	***Article 86***	
Exercise of the delegation	***Exercise of the delegation***	***Exercise of the delegation***	
1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	
	Amendment 200		
2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 336), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3)	2. The ~~delegation of power~~ ***power to adopt delegated acts*** referred to in ~~Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3),~~ ***Article 13a(5),*** Article 17(9), ~~Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 336), Article 34(8), Article 35(11), Article 37(2),~~ ***Article 38(4),*** Article 39(2), ***Article 41(3), Article 41(5),***	2. The delegation of power referred to in ~~Article 6(5),~~ Article 8(3), ~~Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 336), Article 34(8), Article 35(11), Article 37(2),~~ Article 39***a***(~~2~~7), ***[***Article 43(3), ~~Article 44(7),~~ Article 79a(~~6~~4), ~~Article 81(3), Article 82(3) and~~	

[471] ***COM reservation on the deletion of empowerments for delegated acts or implementing acts.***

shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.	Article 43(3), ~~Article 44(7), Article 79(6)~~***Article 79(7)***, Article 81(3)~~,~~ ***and*** Article 82(3) ~~and Article 83(3)~~ shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.	~~Article 83(3)~~ shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.	
	Amendment 201		
3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date	3. The delegation of power referred to in ~~Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3),~~ ***Article 13a(5),*** Article 17(9), ~~Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2),~~ ***Article 38(4),*** Article 39(2), ***Article 41(3), Article 41(5),*** Article 43(3), ~~Article 44(7), Article 79(6)~~***Article 79(7)***, Article 81(3)~~,~~ ***and*** Article 82(3) ~~and Article 83(3)~~ may be revoked at any time by the European Parliament or by the Council. A decision ~~of revocation~~ ***to revoke*** shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the	3. The delegation of power referred to in ~~Article 6(5),~~ Article 8(3), ~~Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2),~~ Article 39a(~~2~~7),***[*** Article 43(3)***]***, ~~Article 44(7),~~ Article 79a(~~6~~4), ~~Article 81(3), Article 82(3) and Article 83(3)~~ may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European*	

specified therein. It shall not affect the validity of any delegated acts already in force.	decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	*Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	
	Amendment 202		
5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the	5. A delegated act adopted pursuant to ~~Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3),~~ ***Article 13a(5),*** Article 17(9), ~~Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2),~~ ***Article 38(4),*** Article 39(2), ***Article 41(3), Article 41(5),*** Article 43(3), ~~Article 44(7), Article 79(6),~~ ***Article 79(7),*** Article 81(3)~~,~~***and*** Article 82(3) ~~and Article 83(3)~~ shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of	5. A delegated act adopted pursuant to ~~Article 6(5),~~ Article 8(3), ~~Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2),~~ Article 39a(~~2~~7),***[*** Article 43(3)***],*** ~~Article 44(7),~~ Article 79a(~~64~~), ~~Article 81(3), Article 82(3) and Article 83(3)~~ shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and	

Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.	~~two~~***six*** months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by ~~two~~ ***six*** months at the initiative of the European Parliament or ***of*** the Council.	the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.	
Article 87	***Article 87***	***Article 87***	
Committee procedure	***Committee procedure***	***Committee procedure***	
1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	
	Amendment 203		
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.	***deleted***	3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.	

CHAPTER XI FINAL PROVISIONS	CHAPTER XI FINAL PROVISIONS	CHAPTER XI FINAL PROVISIONS	
Article 88	***Article 88***	***Article 88***	
Repeal of Directive 95/46/EC	***Repeal of Directive 95/46/EC***	***Repeal of Directive 95/46/EC***	
1. Directive 95/46/EC is repealed.	1. Directive 95/46/EC is repealed.	1. Directive 95/46/EC is repealed.	
2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.	2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.	2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.	
Article 89	***Article 89***	***Article 89***	
Relationship to and amendment of Directive 2002/58/EC	***Relationship to and amendment of Directive 2002/58/EC***	***Relationship to and amendment of Directive 2002/58/EC***	
1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in	1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in	1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in	

connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.	connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.	connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.	
	Amendment 204		
2 Article 1(2) of Directive 2002/58/EC shall be deleted.	2. ~~Article~~***Articles*** 1(2)***, 4 and 15*** of Directive 2002/58/EC shall be deleted.	2 Article 1(2) of Directive 2002/58/EC shall be deleted.	
	Amendment 205		
	2a. The Commission shall present, without delay and by the date referred to in Article 91(2) at the latest, a proposal for the revision of the legal framework for the processing of personal data and the protection of privacy in electronic communications, in order to align the law with this Regulation and ensure consistent and uniform legal provisions on the fundamental right to protection of personal data in the European Union.		

	Amendment 206		
	Article 89a (new)		
	Relationship to and amendment of Regulation (EC) No 45/2001		
	1. The rules set out in this Regulation shall apply to the processing of personal data by Union institutions, bodies, offices and agencies in relation to matters for which they are not subject to additional rules set out in Regulation (EC) No 45/2001.		
	2. The Commission shall present, without delay and by the date specified in Article 91(2) at the latest, a proposal for the revision of the legal framework applicable to the processing of personal data by the Union institutions, bodies, offices and agencies.		
		Article 89a	
		Relationship to previously concluded Agreements	
		International agreements involving the transfer of personal	

		data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Regulation, and which are in compliance with Directive 95/46/EC, shall remain in force until amended, replaced or revoked[472].	
Article 90	***Article 90***	***Article 90***	
Evaluation	***Evaluation***	***Evaluation***	
The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in	The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in information technology and in the	The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in	

[472] ***COM reservation based on strong legal doubts on the legality of such proposal. COM refers to recital 79. DK, IT, RO and UK scrutiny reservation.***

information technology and in the light of the state of progress in the information society. The reports shall be made public.	light of the state of progress in the information society. The reports shall be made public.	information technology and in the light of the state of progress in the information society. The reports shall be made public.	
Article 91	***Article 91***	***Article 91***	
Entry into force and application	***Entry into force and application***	***Entry into force and application***	
1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.	1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.	1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Offi ial Journal of the European Union*.	
2. It shall apply from [*two years from the date referred to in paragraph 1*].	2. It shall apply from ~~[*two years from the date referred to in paragraph 1*]~~*…** . **** OJ: insert the date: two years from the date of entry into force of this Regulation***	2. It shall apply from [*two years from the date referred to in paragraph 1*].	
This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States.	
	Done at …,	***Done at Brussels***	
	For the European Parliament ***The President***	***For the European Parliament*** ***The President***	

	For the Council ***The President***	***For the Council*** ***The President***	

	Amendment 207		
	Annex (new)		
	Presentation of the particulars referred to in Article 13a		

1) Having regard to the proportions referred to in point 6, particulars shall be provided as follows:

ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data are **collected** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **retained** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **processed** for purposes other than the purposes for which they were collected	
	No personal data are **disseminated** to commercial third parties	
	No personal data are **sold or rented out**	
	No personal data are retained in **unencrypted** form	

COMPLIANCE WITH ROWS 1-3 IS REQUIRED BY EU LAW

2) The following words in the rows in the second column of the table in point 1, entitled "ESSENTIAL INFORMATION", shall be formatted as bold:

a) the word "collected" in the first row of the second column;

b) the word "retained" in the second row of the second column;

c) the word "processed" in the third row of the second column;

d) the word "disseminated" in the fourth row of the second column;

e) the word "sold and rented out" in the fifth row of the second column;

f) the word "unencrypted" in the sixth row of the second column.

3) Having regard to the proportions referred to in point 6, the rows in the third column of the table in point 1, entitled "FULFILLED", shall be completed with one of the following two graphical forms in accordance with the conditions laid down under point 4:

a)

b)

4)

a) If no personal data are collected beyond the minimum necessary for each specific purpose of the processing, the first row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

b) If personal data are collected beyond the minimum necessary for each specific purpose of the processing, the first row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

c) If no personal data are retained beyond the minimum necessary for each specific purpose of the processing, the second row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

d) If personal data are retained beyond the minimum necessary for each specific purpose of the processing, the second row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

e) If no personal data are processed for purposes other than the purposes for which they were collected, the third row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

f) If personal data are processed for purposes other than the purposes for which they were collected, the third row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

g) If no personal data are disseminated to commercial third parties, the fourth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

h) If personal data are disseminated to commercial third parties, the fourth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

i) If no personal data are sold or rented out, the fifth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

j) If personal data are sold or rented out, the fifth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

k) If no personal data are retained in unencrypted form, the sixth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

l) If personal data are retained in unencrypted form, the sixth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

5) The reference colours of the graphical forms in point 1 in Pantone are Black Pantone No 7547 and Red Pantone No 485. The reference colour of the graphical form in point 3a in Pantone is Green Pantone No 370. The reference colour of the graphical form in point 3b in Pantone is Red Pantone No 485.

6) The proportions given in the following graduated drawing shall be respected, even where the table is reduced or enlarged: