Council of the European Union
General Secretariat

Brussels, 18 August 2017

WK 8705/2017 INIT

LIMITE

TELECOM
COMPET
MI
DATAPROTECT
CONSOM

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

REQUEST FOR CONTRIBUTION

From:	General Secretariat of the Council
To:	Delegations
Subject:	ePrivacy - DE comments (doc. 5358/17)

Delegations will find in the annex the DE comments on ePrivacy (doc. 5358/17) .

- Draft -

Comments by the German government for the Estonian Presidency relating to the proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

1. The General Data Protection Regulation and the ePrivacy Regulation: respective scopes of application

a) The General Data Protection Regulation and the ePrivacy Regulation

We are in favour of upholding a dedicated set of data protection rules for electronic communications. We also agree that it makes sense to regulate this field by way of a Regulation, particularly now that the General Data Protection Regulation is about to enter into force. It is important that any future ePrivacy Regulation be carefully aligned with the General Data Protection Regulation and that the two follow the same logic as far as the underlying principles are concerned. Germany feels that there is need for additional clarification in this regard: The Commission states in the recitals and in Article 1 para. 3 that the ePrivacy Regulation is to complement and particularise the provisions of the General Data Protection Regulation (GDPR). Germany welcomes the fact that the GDPR is to applied in a subsidiary capacity in those areas for which the ePrivacy Regulation does not set out any specific provisions. However, there are only very few references to the GDPR, which means that this underlying principle is not entirely obvious. We suggest the following wording for Article 1 para. 3:

(3) Unless anything to the contrary is stipulated in this Regulation, the provisions of Regulation (EU) 2016/679 shall apply.

b) Scope of application

Article 5 of the ePrivacy Regulation provides for the confidentiality of electronic communications data. The proposal does not explicitly state where the scope of this protection ends and the provisions of the GDPR start to apply. It is important to clearly define the respective scopes of application of the GDPR and ePrivacy Regulation, and to do this in the text of the ePrivacy Regulation (for example, the start and end of the communication process).

c) Specifying the scope of application

It should be clarified to what extent closed communications services in the area of legal and administrative authorities” and the “financial and customs authorities and their operators are not subject to the scope of application of the E-Privacy Regulation.

2. Tracking by means of cookies (Article 8)

Article 8 provides for the protection of terminal equipment from access by third parties. It is Germany's view that the provisions suggested in Article 8, para. 2 of Article 9, and Article 10 need to be carefully reviewed and be discussed in much more detail. These are provisions that are highly significant for both companies and private individuals alike. These provisions need to protect the right to informational self-determination. At the same time, they must not preclude the development and use of legitimate business models;
this notably applies to business models that ensure access to information that is influential on user's opinion. The relevant provisions ought to be practical and reflect the interests of users and service providers alike. This will require further assessment.

3. Browser software (Article 10)

Article 10 of the Commission's proposal imposes specific obligations (privacy settings preventing third-party access to terminal equipment; information obligations during installation) on manufacturers of browser software (software permitting electronic communication) which thus includes data protection issues in a user-friendly manner (privacy by default).

Germany is wondering whether legal requirements might be beneficial to large browser providers and their strong market position whilst discriminating against third-party providers. This could happen if browser providers define access rights of their own in their terms and conditions, leaving third-party providers without access to the end user. For this reason, Article 10 ought to be worded in such a way as to ensure that third-party providers are not discriminated against. This calls for a practical solution, and one that also makes reference to Article 8, which is related to this provision.

4. Offline Tracking (Article 8 para. 2)

Offline tracking is a process that involves the collection and identification of smartphone data such as terminal equipment. As this represents a substantial infringement of the right to informational self-determination, Germany would like to make this subject to the user's consent. We therefore suggest the following wording for Art. 8 para. 2 lit. b):

"The collection of information emitted by terminal equipment to enable it to connect to another device and/or to network equipment shall be prohibited, except if

[…]

b) the end user has given his or her consent."

This would mean that paras. 3 and 4, which make reference to para. 2 lit. b) of the old version, would be deleted.

5. Directories (Article 15)

Under Article 15, providers of directories that are publicly available will be required to obtain the consent of end users. We feel that this provision of Article 15 is not realistic, unlike the previous provision on directories. It is Germany's view that the previous procedure set out in Article 12 of Directive 2002/58/EC ought to continue to be used. This would mean that operators of electronic communication services are free to seek users' consent.

6. Supervision (Article 18)

We are supportive of the goal of strengthening supervision where data protection rules are concerned. Member States should, however, continue to have discretion to differentiate between different supervisory functions and assign these accordingly.

[7. [Issues around security]

a) General remarks

It is Germany's view that it is necessary to amend the wording of this Regulation to deliver legal certainty around the fact that necessary supportive action taken by operators of electronic communication networks and services to enable ac-

tivities which fall within the scope of Article 2 para. 2 lit. d) are also excluded from the scope of application of this Regulation.

b) Appointment of representatives pursuant to Article 3

The role to be played by the representative in situations where the authorities have made legitimate requests for information is mentioned as early in the document as recital 26 (end of para.). It is, however, necessary for the role of the representative to be described in a way that is unequivocal and clearer than this wording, particularly with regard to these information obligations.
In principle, we welcome the fact that the Regulation provides for comprehensive possibilities for companies to manage data processing and storage on a cross-border basis. However, there is a possibility that this may result in situations where the supervisory authorities are almost entirely cut off from possibilities to gather data pursuant to the relevant laws that apply in the Member States. This would notably be the case where a company chooses to store all of its data in such a way that it can only be accessed from outside a given Member State or even the European Union. To prevent this, there should be a provision stating that Member States' supervisory authorities must be given a point of contact.

This is why we suggest the following wording for Article 11 para. 2 Sentence 2:

"(2) [...] The operators or their representatives shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response."

- Entwurf -

Stellungnahme der Bundesregierung für die estnische Ratspräsidentschaft zu dem Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)

1. Verhältnis Datenschutzgrundverordnung zur E-Privacy-Verordnung und Reichweite des Anwendungsbereiches

a) Verhältnis Datenschutz-Grundverordnung zur E-Privacy-Verordnung

Wir befürworten die Beibehaltung einer speziellen Datenschutzregelung für den Bereich der elektronischen Kommunikation. Auch das Ziel, den Bereich zukünftig im Wege einer Verordnung zu regeln, wird insbesondere mit Blick auf die Datenschutz-Grundverordnung für sinnvoll erachtet. Dabei ist es wichtig, dass eine zukünftige E-Privacy-Verordnung und die Datenschutz-Grundverordnung (DS-GVO) sorgfältig aufeinander abgestimmt sind und Kohärenz zwischen diesen beiden Verordnungen hergestellt wird. Hier besteht aus deutscher Sicht noch erheblicher Klärungsbedarf.

Die Kommission misst der E-Privacy-Verordnung entsprechend den Erwägungsgründen und Artikel 1 Absatz 3 eine ergänzende und präzisierende Funktion zur Grundverordnung zu. Deutschland begrüßt den Ansatz, dass die DS-GVO subsidiär neben der E-Privacy-VO zur Anwendung kommen soll, sofern in der E-Privacy-VO keine speziellen Regelungen enthalten sind. Wegen der

gewählten Verweisungstechnik, also der nur vereinzelten Verweise auf die DS-GVO, kommt dieses Verhältnis zur Grundverordnung jedoch nicht klar zum Ausdruck. Es wird daher vorgeschlagen, Artikel 1 Abs. 3 wie folgt zu fassen:

(3) Die Bestimmungen der Verordnung (EU) 2016/679 finden Anwendung, soweit in dieser Verordnung nichts anderes bestimmt ist.

b) Reichweite des Anwendungsbereiches

Artikel 5 der E-Privacy-Verordnung regelt den Schutz der Vertraulichkeit elektronischer Kommunikationsdaten. Im VO-Vorschlag ist unklar, wann dieser Schutz endet und der allgemeine Datenschutz nach der DSGVO Anwendung findet. Eine entsprechend klare Abgrenzung des Anwendungsbereichs der DS-GVO einerseits und der E-Privacy VO andererseits ist in der E-Privacy-VO notwendig (zum Beispiel Beginn und Ende des Kommunikationsvorgangs).

c) Klarstellung des Anwendungsbereichs

Es sollte geklärt werden, inwieweit geschlossene Kommunikationsdienste im Bereich der Justiz und der Verwaltung sowie der Finanz- und Zollbehörden und deren Betreiber nicht dem Anwendungsbereich der E-Privacy-VO unterfallen.

2. Tracking mittels Cookies (Artikel 8)

Artikel 8 enthält eine Regelung zum Schutz der Endeinrichtungen vor dem Zugriff Dritter. Aus deutscher Sicht sollten die in den Artikeln 8, 9 Absatz 2 und 10 vorgeschlagenen Regelungen besonders sorgfältig geprüft und noch deutlich ausführlicher diskutiert werden. Diese Regelungen sind sowohl für Unternehmen wie für Privatpersonen von erheblicher Bedeutung. Die Regelungen müssen das Recht auf Achtung des Privatlebens und der Kommunikation sowie das Recht natürlicher Personen auf Schutz der sie betreffenden personenbezogenen Daten sicherstellen. Zugleich dürfen legitime Geschäftsmodelle nicht unterbunden werden; dies gilt unter anderem für Geschäftsmodelle, die den Zugang zu meinungsbildenden Informationen sicherstellen. Es sollten für Nutzer und Diensteanbieter insoweit praktikable Regelungen vorgegeben werden, die den Interessen aller Beteiligten Rechnung tragen. Hierzu sind weitere Prüfungen erforderlich.

3. Browsersoftware (Artikel 10)

Der Vorschlag der Kommission enthält in Artikel 10 eine Regelung, die den Herstellern von Browsersoftware (Software, die elektronische Kommunikation ermöglicht) besondere Pflichten auferlegt (Voreinstellungen zur Verhinderung des Zugriffs auf Endeinrichtungen und Informationspflichten bei der Installation) und die so datenschutzrechtliche Belange in nutzerfreundlicher Art und Weise beinhaltet (Privacy by default).

Aus deutscher Sicht besteht die Frage, ob gesetzliche Anforderungen die starke Marktstellung großer Browseranbieter verfestigen und Drittanbieter diskriminieren, indem Browseranbieter in ihren Geschäftsbedingungen eigene Zugriffsrechte festlegen, während Drittanbieter keinen Zugang zum Endnutzer mehr erhalten. Artikel 10 sollte daher so gefasst werden, dass Drittanbieter nicht diskriminiert werden. Hier gilt es praktikable Lösungen zu finden, die auch Artikel 8 miteinbeziehen, da zwischen beiden Regelungen ein Sachzusammenhang besteht.

4. Offline Tracking (Artikel 8 Absatz 2)

Beim Offline Tracking werden Daten von Endeinrichtungen, wie zum Beispiel Smartphones erhoben und identifiziert. Mit Blick auf den erheblichen Eingriff in das informationelle Selbstbestimmungsrecht sollte aus deutscher Sicht ein Einwilligungsvorbehalt normiert werden. Es wird daher vorgeschlagen, Artikel 8 Absatz 2 lit. b) wie folgt zu fassen:

„Die Erhebung von Informationen, die von Endeinrichtungen ausgesendet werden, um sich mit anderen Geräten oder mit Netzanlagen verbinden zu können, ist untersagt, außer

[…]

b) der Endnutzer hat seine Einwilligung gegeben.“

Die auf Absatz 2 lit. b) a. F. Bezug nehmenden Absätze 3 und 4 werden folglich gestrichen.

5. Verzeichnisse (Artikel 15)

In Artikel 15 werden zukünftig die Betreiber öffentlich zugänglicher Verzeichnisse dazu verpflichtet, die Einwilligung der Endnutzer einzuholen. Die Regelung in Artikel 15 erscheint gegenüber der bisherigen Regelung zu Teilnehmerverzeichnissen nicht praktikabel. Aus deutscher Sicht sollte sichergestellt werden, dass das bislang praktizierte Verfahren nach Artikel 12 der Richtlinie 2002/58/EG weiterhin beibehalten wird, wonach die Betreiber elektronischer Kommunikationsdienste die Einwilligung der Nutzer einholen können.

6. Aufsicht (Artikel 18)

Wir begrüßen das Anliegen, die Rolle der Datenschutzaufsicht zu stärken. Allerdings sollte den Mitgliedstaaten die Möglichkeit erhalten bleiben, Aufsichtsfunktionen differenziert zu vergeben.

7. Sicherheitsfragen

a) Allgemeines

Aus deutscher Sicht wird für erforderlich gehalten, dass in der Verordnung rechtsklar geregelt ist, dass erforderliche Unterstützungshandlungen von Betreibern elektronischer Kommunikationsnetze und -dienste für Tätigkeiten, die nach Artikel 2 Absatz 2 vom Anwendungsbereich der Verordnung ausgenommen sind, diesem ebenfalls nicht unterfallen.

b) Vertreterregelung

In Erwägungsgrund 26 a. E. wird bereits auf die Rolle des Vertreters bei der Auskunftserteilung an Sicherheitsbehörden eingegangen. Es ist aber erforderlich, die Rolle des Vertreters insbesondere hinsichtlich dieser Auskunftsverpflichtungen eindeutiger und klarer zu definieren.
Die Verordnung schafft umfangreiche und grundsätzlich positive Möglichkeiten für Unternehmen, die Datenverarbeitung und -haltung grenzübergreifend zu organisieren. In Folge kann es aber dazu kommen, dass Sicherheitsbehörden von Möglichkeiten zur Datenerhebung nach den jeweils für sie geltenden Gesetzen der Mitgliedstaaten weitgehend abgeschnitten werden. Dies wäre insbesondere dann der Fall, wenn ein Unternehmen die Datenhaltung so organisiert, dass nur noch eine Stelle außerhalb des Mitgliedstaates oder gar

außerhalb der Union über den Datenzugriff verfügen würde. Deshalb sollte zur Kompensation eine Regelung geschaffen werden, die den Sicherheitsbehörden der Mitgliedstaaten eine Ansprechstelle zur Verfügung stellt.

Es wird deshalb vorgeschlagen, Artikel 11 Absatz 2 Satz 2 wie folgt zu fassen:

„(2) […] <u>Die Betreiber oder ihre Vertreter</u> stellen der zuständigen Aufsichtsbehörde auf Anfrage Informationen über diese Verfahren, die Zahl der eingegangenen Anfragen, die vorgebrachten rechtlichen Begründungen und ihre Antworten zur Verfügung und geben sonstige in der Gesetzgebungsmaßnahme vorgesehene Auskünfte.“