WHITEPAPER

BVDW
Wir sind das Netz

DATENSCHUTZMANAGEMENT IM E-COMMERCE

Vorwort

Dieses Whitepaper motiviert und sensibilisiert zum Thema Datenschutz-Management, es zeigt die notwendigen Eckpunkte eines modernen Datenschutz-Managements auf.

Das Dokument dient zur Orientierung und Einführung in das Thema Datenschutz-Management. Es soll und kann eine fundierte rechtliche und technische Beratung im Einzelfall nicht ersetzen.

Inhaltsübersicht

1. WARUM DATENSCHUTZ-MANAGEMENT?

Die Erhebung und Verarbeitung unterschiedlichster Informationen ist heute für jedes Unternehmen Realität. Häufig handelt es sich bei diesen Informationen aber nicht nur um Tabellen und Zahlenwerke. Kaum ein Unternehmen der digitalen Wirtschaft kommt ohne die Verwendung auch personenbezogener Daten – sei es der eigenen Beschäftigten oder der Nutzer der angebotenen Dienstleistungen – aus.

Unter den Begriff „personenbezogene Daten" fallen alle Einzelangaben über persönliche oder sachliche Verhältnisse (Name, Adresse, Mail-Adresse, Telefonnummer) einer bestimmten oder bestimmbaren natürlichen Person[1]. Derartige Daten genießen in Deutschland besonderen rechtlichen Schutz. Rechtliche Vorgaben zum Datenschutz müssen überall dort beachtet werden, wo personenbezogene Daten computergestützt, also unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden.

Die einschlägigen Bestimmungen zum Datenschutz finden sich vor allem in dem Bundesdatenschutzgesetz (BDSG), dem Telekommunikationsgesetz (TKG) sowie dem Telemediengesetz (TMG) und erlegen Ihnen als Verwender besondere Aufgaben im Umgang mit diesen auf. Die Vielzahl der zu beachtenden Reglungen erfordert demgemäß, dass geeignete Prozesse und Vorkehrungen eingerichtet werden, um den gesetzlichen Anforderungen umfassend gerecht zu werden (Datenschutz-Management).

2. WAS MUSS DAS DATENSCHUTZ-MANAGEMENT ABDECKEN?

Ein „Datenschutz-Management", d.h. ein aktives und zielgerichtetes Handeln zur Erreichung von gesetzlichen Datenschutz-Zielen, ist die Rahmenbedingung für die Erfüllung dieser gesetzlichen Auflagen bei der Entwicklung, der Planung, der Implementierung und dem Betrieb von Datenverarbeitungsverfahren, aber auch bei der Außerbetriebnahme von Verfahren und Anwendungen.

Zunächst sind hier die Regelungen über Art und Weise der Erhebung und Verarbeitung personenbezogener Daten von besonderer Relevanz. Es gilt generell, dass alles verboten ist, was nicht ausdrücklich erlaubt ist (das ist das sog. „Verbot mit Erlaubnisvorbehalt"). Eine Erfassung, Verarbeitung und Nutzung von personenbezogenen Daten ist nur dann zulässig, wenn hierzu entweder eine gesetzliche Erlaubnisnorm eingreift oder aber eine ausdrückliche und freiwillige Einwilligung des Betroffenen vorliegt.

Eine Einwilligung muss grundsätzlich schriftlich erteilt werden. Bei mündlicher Erteilung ist sie schriftlich zu bestätigen. Soweit die Einwilligung in elektronischer Form erklärt wird, sind die weiteren Anforderungen des TMG zu beachten. Die Erklärung muss protokolliert werden, für den Erklärenden ständig abrufbar und jederzeit widerruflich sein. Für den Nachweis einer wirksam erklärten Einwilligung ist der Diensteanbieter beweispflichtig. Betroffene haben daneben umfangreiche Auskunfts- und Löschungsansprüche bezüglich der von ihnen gespeicherten personenbezogenen Daten.

[1] Vgl. § 3 Abs. 1 BDSG

Ein umfassendes Datenschutz-Management muss also die Nachvollziehbarkeit und Zuordnung datenschutzrechtlich relevanter Vorgänge zu individuellen Nutzern unter Beachtung der gesetzlichen Anforderungen ermöglichen.

Datenschutz bedeutet aber auch, dass die Sicherheit der erhobenen Daten vom Verwender gewährleistet ist.

Gemäß § 9 BDSG müssen alle Stellen welche selbst oder im Auftrag personenbezogene Daten verarbeiten, auch technisch-organisatorische Maßnahmen treffen die erforderlich sind, um die Einhaltung der datenschutzrechtlichen Vorschriften zu gewährleisten. In der Anlage zu § 9 BDSG werden diese Anforderungen konkretisiert. Ein auf die technisch-organisatorischen Maßnahmen bezogenes Datenschutz-Management muss danach folgende Kategorien berücksichtigen:

- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle

Satz 1 der Anlage zu § 9 BDSG enthält einen Auftrag an die Einrichtung eines entsprechenden Datenschutz-Management: „Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird."

In dieser allgemeinen Form enthält das BDSG also die Pflicht zur Erstellung und Dokumentation eines Datenschutzmanagement-Konzeptes. Dieses Konzept ist übergeordnet zu einem IT- und Sicherheitskonzept zu sehen.
Ein systematisches Datenschutz-Management umfasst insgesamt alle Zuständigkeiten, vorgeschriebenen Verhaltensweisen sowie Abläufe (z.B. Vorabkontrollen, Auskunfts-, Benachrichtigungs- und Löschungsroutinen) und auch die Ressourcen (Betriebsmittel), die zur Erreichung des festgelegten Datenschutz-Ziels dienen.

Ein zum Datenschutz-Management angrenzender Prozess ist das Risiko-Management, so sollte der betriebliche Datenschutzbeauftragte im Idealfall auch standardmäßig in IT Sicherheitsthemen involviert sein und, soweit vorhanden, auch Mitglied im IT-Sicherheitsvorfall-Team.

Mit dem Datenschutz-Management verwandt ist das Informationsschutz-Management: während es beim Datenschutz-Management um den Schutz personenbezogener Daten geht, beschäftigt sich das Informationsschutz-Management mit dem Schutz von Daten ohne Personenbezug, z.B. Formeln und Konstruktionspläne.

Hier zeigt sich, dass Datenschutz und funktionierendes IT-Management Hand in Hand gehen, die Einführung von Datenschutz-Management wird zwangsläufig eine Verbesserung des IT-Managements mit sich bringen und umgekehrt.

3. FOLGEN BEI UNZUREICHENDEM DATENSCHUTZ-MANAGEMENT

Die Folgen einzelner datenschutzrechtlicher Verstöße können teilweise gravierend sein. Das BDSG sieht einen Bußgeldrahmen von 50- bis 300T€ im Falle von Verstößen gegen Datenschutzvorschriften vor. Zusätzlich soll der durch den Verstoß erreichte wirtschaftliche Vorteil abgeschöpft werden, was die eben genannten Beträge schnell überschreiten kann. Daneben droht bei bestimmten vorsätzlichen Verstößen überdies eine Freiheitsstrafe von bis zu zwei Jahren.

Die Anforderungen des BDSG müssen daher in jedem Unternehmen beachtet werden und – angemessen gewichtet – in die Unternehmensprozesse einfließen. Ein gut geführtes Datenschutzmanagement kann das Unternehmen vor scharfen Restriktionen und Sanktionen bewahren. Das Erreichen und Einhalten der Datenschutz-Standards ist heute für jedes Unternehmen elementar, um Gesetzesverstöße, Verlust wichtiger Unternehmensressourcen, persönliche Inanspruchnahme des Managements (z.B. KonTraG) und geschäftsschädigenden Vertrauensverlust von Kunden und Geschäftspartnern zu vermeiden. Die Bestellung eines fachkundigen Datenschutzbeauftragten kann die Geschäftsleitung vor persönlicher Inanspruchnahme schützen, gleichwohl trägt das Management natürlich auch weiterhin die unternehmerische Verantwortung für sein Handeln.

Ein ordnungsgemäßes Datenschutzmanagement dient ferner der Sicherung von Kundendaten. Der Verlust bzw. die unbeabsichtigte Offenlegung von Kundendaten gefährdet nicht nur Unternehmenswerte, sondern kann auch hohe Kosten und Rufschädigung zur Folge haben.
Nicht zuletzt vermeiden Sie, sich ggf. mit Abmahnungen auseinandersetzen zu müssen.

4. IHRE ERSTE CHECKLISTE ZUM DATENSCHUTZ-MANAGEMENT:

1. Arbeiten bei uns mehr als 10 Mitarbeiter in der automatisierten Datenverarbeitung personenbezogener Daten? Oder sind mindestens 20 Mitarbeiter auf andere Weise mit der Verarbeitung personenbezogener Daten beschäftigt?
   Wenn ja, haben wir einen Datenschutzbeauftragten bestellt? (§ 4f BDSG)?
   Für bestimmte Personenkreise ist wegen möglicher Interessenskonflikte die Bestellung zum Datenschutzbeauftragen nicht möglich, z.B. für den Geschäftsführer, den Leiter Personal, den Betriebsleiter, den Leiter der IT und den Leiter der Rechtsabteilung. Viele Firmen greifen daher auf einen externen Datenschutzbeauftragten zurück.
2. Gibt es ein öffentliches Verfahrensverzeichnis (§ 4g Abs.2 BDSG)?
   Die Anforderungen des BDSG nach einem Datenschutzbeauftragten und öffentlichen Verfahrensverzeichnissen stellen das „Fundament" des Datenschutzes dar und bilden damit die Grundlage für die Verankerung des Datenschutzes in Ihrem Unternehmen.

3. Gibt es eine Datenschutzerklärung in unserem Online-Auftritt (Verwendung für Marketing, Cookies etc.) und haben wir sie angemessen formuliert?
   Hier sollte jede Verwendung von Kundendaten, insbesondere wenn sie über den ursprünglichen Zweck (Bestellung, Vertragsabwicklung, Newsletter etc.) hinausgehen kann, beschrieben werden.
4. Werden neu eingestellte Mitarbeiter in Datenschutz und Datensicherheit eingewiesen? Werden sie gesondert (schriftlich) auf das Datengeheimnis verpflichtet?
5. Wird das zur Aufrechterhaltung des angestrebten Datenschutz-Niveaus notwendige Fachwissen und IT-Sicherheitswissen unserer Mitarbeiter regelmäßig nachgeschult?
6. Gibt es ein konventionelles oder elektronisches Datenschutzhandbuch (oder ein Wiki) für unsere Mitarbeiter?
7. Spielen die Prinzipien der Datenvermeidung und Datensparsamkeit (§3a BDSG) sowie der Zweckbindung bei uns schon eine Rolle?
   Brauchen wir alle Daten, die wir erheben und speichern, tatsächlich? Wie lange brauchen wir diese Daten (nur für eine Transaktion, für die nächste Aussendung, zur Bearbeitung von Rückfragen bzw. Reklamationen? Bei welchen Daten gibt es gesetzliche Anforderungen und Notwendigkeiten, bei welchen Daten ist die Speicherung ggf. verpflichtend, bei welchen nicht? Unterscheiden wir bei der Speicherung von Daten zwischen dem aktiven Bestand und Aufbewahrungsfristen (etwa gem. HGB)? Unterscheiden wir bei der Erhebung (Eingabe) zwischen Muss- und Kann-Feldern? Speichern wir ggf. Daten, deren Erhebung und Speicherung wir nicht begründen können? Was passiert bei uns mit den Daten eines Systems, das wir abschalten?
8. Ist die Nutzung von E-Mails und Internet rein zu Firmenzwecken oder auch zu privaten Zwecken erlaubt bzw. geduldet? Falls ja, ist eine Überwachung der Kommunikation verboten.
9. Wird Datenschutz bei der Auswahl, Neu- und Ersatzbeschaffung von Hardware und Software als Kriterium herangezogen? Spielt Verschlüsselung dabei schon eine Rolle?
10. Haben wir externe Stellen mit der Datenverarbeitung beauftragt? (§ 11 BDSG)
    Haben wir uns vorab von dem dort etablierten Datenschutz-Management und dessen Eignung überzeugt und eine (nachvollziehbare) entsprechend sorgfältige Auswahl getroffen? Führen wir dort regelmäßig anlassbezogene und anlassunabhängige Datenschutzkontrollen durch?
11. Sind die vertraglichen Verpflichtungen für Dienstleister, Unterauftragnehmer oder Erfüllungsgehilfen (z.B. für unseren Payment-Dienstleister, unsere Logistik, unser Webseiten-Hosting, den Katalog-/Mailingversand oder den Inkasso-Dienstleister) ausreichend und zeitgemäß?
12. Erheben wir besondere Arten personenbezogener Daten (z.B. zur ethnischen Herkunft, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit) und erfüllen wir – soweit eine Einwilligung nicht vorliegt – die gesetzlichen Ausnahmekriterien?
13. Sind Sperrung, Pseudonymisierung, Anonymisierung und Löschung von personenbezogenen Daten bei uns sichergestellt? Sind sie Teil der betrieblichen Praxis? Wann haben wir das zuletzt angewendet?
14. Ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten in unseren jeweiligen Geschäftsprozessen zulässig? (§ 4 BDSG und § 28 BDSG)
    Setzen wir z.B. bei der Registrierung von Newsletter-Abonnenten ein Double-Opt-In ein?

15. Wie gehen wir mit den IP-Adressen unserer Nutzer um? Kürzen wir bei der Benutzung von Webanalysetools die IP-Adressen=?
16. Wenn wir personenbezogene Daten an Dritte übermitteln, haben wir uns von der (gesetzlichen) Zulässigkeit überzeugt (§ 4 BDSG). Haben wir uns von der Angemessenheit des Schutzniveaus in einem anderen Staat als Deutschland überzeugt? (§ 28, 29 und §4b BDSG).
17. Werden bei der Übermittlung in Nicht-EU-Staaten Safe-Harbour Unternehmen ausgewählt oder ist die Geltung von EU-Komm-Standardverträgen vereinbart?
18. Sind die nach §9 BDSG notwendigen technischen und organisatorischen Maßnahmen bei uns umgesetzt? Können wir deren Umsetzung nachweisen? Überprüfen wir eine Anpassung der Maßnahmen, wenn wir unsere IT ändern? Gibt es Rollen- bzw. Zugriffskonzepte mit Einschränkung von Zugriffen bei Einsicht in und Veränderung von personenbezogenen Daten?
19. Gibt es regelmäßige interne oder externe Audits, mit denen wir die Wirksamkeit unseres Datenschutz-Managements auf die Probe stellen?
20. Gibt es ein eingeführtes und gelebtes Reporting zum Datenschutz?
21. Sind Berichts-, Eskalations- und Entscheidungswege bei besonderen Datenschutz-Vorkommnissen (Störfall bzw. Krisenfall) festgelegt und dokumentiert? Wie reagieren wir, wenn uns Externe auf vermutete Datenschutz-Probleme bei uns hinweisen? Wissen unsere Mitarbeiter, an wen sie sich wenden können?
22. Können wir auch die Anforderungen unseres Wirtschaftsprüfers, aber auch die Erwartungen unserer Kunden, an Datenschutz bei uns erfüllen?
23. Haben wir entsprechende Unternehmensprozesse etabliert?
24. Bestehen bereits Kontakte zu den zuständigen Aufsichtsbehörden? Wie kann der Aufbau solcher Kontakte aussehen und welche Zielrichtung diesbezüglich streben wir damit an?
25. Wie reagieren wir, wenn einer unserer Kunden Widerspruch gegen die Datenspeicherung einlegt? Können wir z.B. ausschließen, dass das Nutzungsverhalten eines bestimmten Kunden nicht mehr protokolliert und ausgewertet wird, wenn er dem widerspricht?

Ein etabliertes Datenschutz-Management bedeutet insbesondere, Chancen wahrzunehmen:

- Sie vermeiden Risiken (siehe oben)
- Sie können Wettbewerbsvorteile erzielen, denn Ihre Kunden und auch die Öffentlichkeit werden effektives Datenschutz-Management mit Vertrauen in die Kontrollierbarkeit Ihrer Datenverarbeitung honorieren
- Sie vermeiden Fehlinvestitionen bzw. teure Nachrüstungen
- Sie schaffen Transparenz, Nachvollziehbarkeit und Beweissicherheit für die Nutzer und
- sorgen für Überschaubarkeit in Ihren eigenen Verfahren und in Ihren betrieblichen Abläufen.

5. DATENSCHUTZ-MANAGEMENT… GETTING STARTED

Der Einstieg in das Datenschutz-Management enthält u.a. diese Punkte:

- Feststellung des Ist-Zustandes (wo werden personenbezogene Daten erhoben, gespeichert, verarbeitet und ggf. an Dritte weitergegeben)
- Welche (ggf. branchenabhängigen) Vorschriften außerhalb des BDSG sind außerdem zu erfüllen (z.B. TMG, TKG etc.)
- Einschätzung des Erfüllungsgrades der relevanten Vorschriften, d.h. Darstellung der Risiken
- Einschätzung der Erforderlichkeit bereits erhobener bzw. zu erhebender Daten
- Festlegung konkreter Zwecke für die jeweiligen Datenverarbeitungsvorgänge
- Erstellung einer anforderungsgerechten Datenschutzorganisation (Richtlinien, regelmäßige Mitarbeiterschulungen etc.), dazu gehört auch die
- Bestellung eines Datenschutzbeauftragten, er ist für die gesetzliche Aufgabe der Schulung, für die Beratung und Kontrolle, die Durchführung der Vorabkontrolle, das Führen des Verfahrensverzeichnisses sowie die Pflege des Kontaktes zur Datenschutzbehörde zuständig.
- Erstellung von Verfahrensverzeichnissen (§4g Abs. 2 BDSG)
- Erstellung eines Maßnahmenkatalogs zur Erfüllung gesetzlicher Anforderungen nach § 9 BDSG (bzw. nach IT-Grundschutzhandbuch des BSI bzw. ISO 27001), d.h. Aufstellen eines Zeit- und Aufgabenplans)
- Definition und Aufbau von Datenschutzprozessen (z.B. Vorabkontrolle, Auskunftsroutinen, Prüfung der Rechtsmäßigkeit von Datenverarbeitung) und die Erstellung datenschutzrechtlich relevanter Dokumente (Mitarbeiterverpflichtungen, Betriebsvereinbarungen, Vertragsvorlagen etc.).
  Hier sind insbesondere die in der Anlage zu § 9 BDSG ausgeführten Anforderungen zu beachten:
  - **Zutrittskontrolle**
    Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt durch z.B. Ausweisleser, elektronische Schlüsselsysteme etc.
  - **Zugangskontrolle**
    Datenverarbeitungssysteme können von Unbefugten nicht genutzt werden durch (z.B. Passwortschutz, Verschlüsselung).
  - **Zugriffskontrolle**
    Die zur Benutzung eines Datenverarbeitungssystems Berechtigten können ausschließlich nur auf die ihrer eigenen Zugangsberechtigung unterliegenden Daten zugreifen, so dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können durch (mehrstufige Firewall-Systeme, Protokollierung, Passwortschutz, Berechtigungs- und Betreiberkonzepte)

- **Weitergabekontrolle**
  Personenbezogene Daten können bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Dabei wird überprüft und festgestellt, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Verschlüsselung, Regelung des Kommunikationsverkehrs, Protokollierung)
- **Eingabekontrolle**
  Es kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Sicherungssoftware, Protokollierung, Berechtigungskonzept).
- **Auftragskontrolle**
  Personenbezogene Daten, die im Auftrag verarbeitet werden, können nur entsprechend den Weisungen des Auftraggebers verarbeitet werden (schriftliche Weisungen des Auftraggebers, Betreiberkonzept, Protokollierung).
- **Verfügbarkeitskontrolle**
  Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust geschützt (Sicherungskopien an einem anderen Ort, Maßnahmen zum Katastrophenschutz/ Notfallvorsorge).
- **Trennungskontrolle**
  Zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet (logische Trennung, Benutzerprofile, Berechtigungen, Mandanten- und Betreiberkonzept).

➔ Überprüfung des Schriftverkehrs (Außendarstellung und Außenwirkung)

Für den Beginn und die Aufrechterhaltung dieses Prozesses müssen Ressourcen bereitgestellt werden, das sind vorrangig Personalressourcen (Arbeitszeit). Eine IT-Unterstützung durch z.B. softwaregestütztes Prozess- und Dokumenten-Management ist erst ab einer bestimmten Betriebsgröße bzw. Verfahrenskomplexität relevant.

Genau wie ein funktionierender IT-Sicherheitsprozess ist der Datenschutz-Prozess zyklisch, d.h. er wird permanent überprüft und ggf. angepasst.

Die Aufrechterhaltung des einmal geschaffenen angemessenen Datenschutz-Niveaus im laufenden Betrieb dient dazu, auf Änderungen und Störungen in den Verfahren, mit denen personenbezogene Daten verarbeitet werden, zu reagieren.

Das sind vor allem:

➔ Änderungen im Datenschutzrecht
➔ Änderungen in den eigenen (IT-)Verfahren/technischer Fortschritt
➔ Störungen in den operativen Betriebsabläufen, die als IT-Sicherheitsvorfall zu klassifizieren sind (hier entsteht der Querbezug zum Risikomanagement und der Unternehmenskommunikation)

Ernsthaft umgesetztes Datenschutz-Management sorgt für Überschaubarkeit in Ihren Verfahren und Ihren betrieblichen Abläufen.

AUTOREN

Michael Neuber
Rechtsanwalt, Justiziar, Bundesverband Digitale Wirtschaft (BVDW) e.V.

Kirsten Pedd
Rechtsanwältin, Chef-Syndika, EOS Gruppe Deutschland

Jan Pohle
Rechtsanwalt, DLA Piper, Stv. Vorsitzender der Fachgruppe E-Commerce im BVDW

Siebo Woydt
Geschäftsführer, Creditreform Boniversum
Stv. Leiter der Unit Payment & Risikomanagement der Fachgruppe E-Commerce im BVDW

IMPRESSUM

Datenschutzmanagement im E-Commerce

Erscheinungsort und -datum
Düsseldorf, 25. Oktober 2012

Herausgeber
Bundesverband Digitale Wirtschaft (BVDW) e.V.
Berliner Allee 57
40212 Düsseldorf
Telefon: 0211 600456-0
Telefax: 0211 600456-33
E-Mail: info@bvdw.org
Internet: www.bvdw.org

Geschäftsführerin
Tanja Feller

Präsident
Arndt Groth

Vizepräsidenten
Christoph N. v. Dellingshausen, Matthias Ehrlich, Harald R. Fortmann, Ulrich Kramer, Burkhard Leimbrock

Kontakt
Fachgruppe E-Commerce im BVDW
Ramona Laughton, Fachgruppenmanagerin
E-Mail: laughton@bvdw.org

Vereinsregisternummer
Vereinsregister Düsseldorf VR 8358