ePrivacy

Whitepaper

Was ist aus datenschutzrechtlicher Sicht

in Hinblick auf die zukünftige

Datenschutz-Grundverordnung

zu ändern?

ePrivacy GmbH, Hamburg, April 2017

Autoren: Prof. Dr. Christoph Bauer, Dr. Frank Eickmeier, Dr. Anna Täschner

Die Datenschutz-Grundverordnung, kurz „DSGVO“ ist ab dem 25.05.2018 europaweit geltendes Recht. Die DSGVO ersetzt zugleich die bislang geltenden nationalen Datenschutzvorschriften, in Deutschland insbesondere das Bundesdatenschutzgesetz (BDSG) und das Telemediengesetz (TMG). Beide Gesetze bleiben nur noch als Rumpfgesetze in Kraft. Die wesentlichen datenschutzrechtlichen Fragestellungen werden sich zukünftig aus der DSGVO ergeben. Für die Onlineunternehmen ist darüber hinaus die sogenannte ePrivacy-Verordnung zu beachten, die seit Januar 2017 als Entwurf vorliegt.

Was sind die wichtigsten Änderungen durch die DSGVO, die Unternehmen in der EU zukünftig berücksichtigen sollten?

1. **Neue Datenschutzerklärungen, neue Informationspflichten:**

   Die Art. 12 ff. DSGVO regeln neue Informationspflichten, die in weiten Teilen über die bisherigen Informationspflichten, die in einer Datenschutzerklärung abzubilden waren, hinausgehen. Falls noch nicht geschehen, muss die Datenschutzerklärung um folgende Punkte ergänzt werden:

   - Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters;
   - ggf. die Kontaktdaten des Datenschutzbeauftragten;
   - die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung;
   - wenn die Verarbeitung auf Art. 6 Abs. 1 f DSGVO beruht, die berechtigten Interessen, die von den Verantwortlichen oder einem Dritten verfolgt werden;
   - ggf. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
   - ggf. die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln;
   - die Dauer des Speicherung der Daten;
   - Informationen über das Bestehen eines Rechts auf Auskunft, Berichtigung oder Löschung;
   - Information darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist;
   - das Vorhandensein von sogenanntem „Profiling“ und in diesen Fällen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

ePrivacy Tipp: Prüfen Sie, ob ihre Datenschutzerklärung und ihr Verfahrensverzeichnis alle notwendigen Angaben enthalten, und ergänzen Sie sie gegebenenfalls.

2. Neue Definition der personenbezogenen Daten – und was haben Cookie-IDs damit zu tun?

Der Begriff der personenbezogenen Daten wurde in der DSGVO neu definiert. Prüfen Sie daher, welche Auswirkungen das auf Ihr Geschäftsmodell hat. Viele Daten, die früher als anonym galten, sind zukünftig Daten mit Personenbezug. „Personenbezogene Daten" im Sinne der DSGVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung durch

- einer Kennung wie einem Namen,
- einer Kennnummer,
- Standortdaten,
- einer Online-Kennung oder
- einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Wichtig für die Onlinebranche ist insoweit ein durch die DSGVO eingeführter Paradigmenwechsel. Während es früher umstritten war, ob Online-Identifier wie Cookie-IDs, User-IDs, MAC-Adressen u. ä. personenbezogene Daten waren, gelten sie nunmehr in der Regel als personenbezogen. Denn es handelt sich hierbei um eine „Online-Kennung" im oben erwähnten Sinne.

Die praktischen Auswirkungen sind erheblich. Denn wenn es sich bei Online-IDs um personenbezogene Daten handelt, dann bedarf jede Erhebung oder Nutzung dieser IDs – etwa im Rahmen von Online-Werbung – der Einwilligung des Nutzers. Deshalb gelangt in diesen Fällen der neue Art. 6 Abs. 1 f DSGVO zur Anwendung (siehe

unten 3.), der zukünftig für die Onlinewerbebranche von kaum zu überschätzender Bedeutung werden dürfte.

ePrivacy Tipp: Prüfen Sie, ob Sie Daten verarbeiten, die früher als anonym galten und in Zukunft als personenbezogen anzusehen sind, denn dann gilt die DSGVO.

3. Neue Regeln für Onlinewerbung

Durch die DSGVO hat sich am Grundprinzip im Datenschutzrecht nichts geändert: Die Verarbeitung von personenbezogenen Daten ist nur zulässig, wenn eine Einwilligung der betroffenen Person vorliegt oder das Gesetz eine Datenverarbeitung gestattet (sogenannter Erlaubnistatbestand).

Neu sind aber die Erlaubnistatbestände im Art 6 DSGVO. Insbesondere **Art. 6 Abs. 1 f DSGVO** enthält eine für die Praxis weitreichende und zum Teil neue Regelung. Danach ist die Verarbeitung von personenbezogenen Daten auch ohne ausdrückliche Einwilligung zulässig, wenn die Verarbeitung zur Wahrung der „berechtigten Interessen“ des Verantwortlichen (des Werbetreibenden) oder eines Dritten (z. B. eines Kooperationspartners) erforderlich ist, sofern nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Auch die Interessen der Werbeindustrie können ein berechtigtes Interesse darstellen. Sie sind damit nicht von vorneherein weniger wert, als die Interessen der Betroffenen, etwas die Besucher einer Website.

ePrivacy Tipp: Prüfen Sie dringend, welchen Einfluss die neuen Regeln zur Onlinewerbung für Ihr Unternehmen haben werden, und auf welcher Rechtsgrundlage Sie zukünftig personenbezogene Daten verarbeiten.

4. Neue Regeln für die Einwilligung von Kindern

Art. 8 DSGVO bestimmt zukünftig, dass die Einwilligung eines Kindes nur wirksam ist, wenn das Kind das 16. Lebensjahr vollendet hat. Hat das Kind noch nicht das 16. Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern durch die Eltern die Zustimmung erteilt wird.

ePrivacy Tipp: Prüfen Sie, ob Sie Daten von Kindern unter 16 Jahren verarbeiten, denn dafür benötigen Sie die Zustimmung der Eltern.

5. Neu: Profiling – und warum Nutzerprofile nicht darunter fallen

Neu ist in der DSGVO der Begriff des „Profilings". Jede Person sollte nach dem Willen des Gesetzgebers das Recht haben, nicht einer Entscheidung zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Dies könnte etwa die automatische Ablehnung eines Online-Kreditantrags oder ein Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen sein.

Zu einer derartigen Verarbeitung zählt auch das sogenannte „Profiling". Es meint jegliche Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlichen Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person.

Die gilt allerdings nur, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Im Klartext heißt das, dass jede Form von Nutzerprofilen im Rahmen der Onlinewerbung nicht darunter fallen. Denn diese haben in der Regel keine „rechtlichen Wirkungen".

ePrivacy Tipp: Prüfen Sie, ob sie nach der genannten Definition Profiling betreiben und ob sich dies rechtlich auf den Betroffenen auswirkt bzw. ihn erheblich beeinträchtigt. Falls ja, sollten sie rechtliche Expertise einholen.

6. Neue Regeln zur Auftragsverarbeitung

Es wird neue Regeln zur Auftragsdatenverarbeitung geben, die zukünftig schlicht „Auftragsverarbeitung" heißen wird. Zwar gelten viele Grundsätze, die in Deutschland

seit langem bekannt sind, auch zukünftig weiter. Es wird aber einige Änderungen geben, die eine Anpassung der „Auftragsverarbeitungsverträge“ erforderlich machen werden.

Die nach dem BDSG privilegierte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (§ 3 Abs. 8 Satz 3 und § 11 BDSG), wonach der per Auftrag eingesetzte Dienstleister nicht Dritter ist, sondern sozusagen ein „Innenverhältnis“ ohne Prüfschranken für eine Datenübermittlung gesetzlich bestimmt wird, findet sich in vergleichbarer Weise auch in der DSGVO wieder. Denn nach Art. 4 Nr. 10 DS-GVO ist ein Auftragsverarbeiter kein Dritter. Neu ist aber, dass die DSGVO keine Beschränkung der Privilegierung der Auftragsverarbeitung auf den EU-/EWR-Raum enthält, wie sich dies bisher aus der Eingrenzung in § 3 Abs. 8 Satz 3 BDSG ergab.

Allerdings legt die DSGVO den Auftragsverarbeitern künftig mehr Verantwortung und mehr Pflichten auf. Die zentrale Vorschrift für Auftragsverarbeiter in der DSGVO ist zukünftig Art. 28 DSGVO. Dort wird in Absatz 1 zunächst die Prüfung der Geeignetheit eines Auftragsverarbeiters eingefordert. Der Verantwortliche darf nach dieser Bestimmung nur Auftragsverarbeiter einsetzen, die hinreichend Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen („TOMs“) für einen ausreichenden Datenschutz haben.

Wie bisher muss mit dem Auftragsverarbeiter im Regelfall einen Vertrag über die Auftragsverarbeitung geschlossen werden, der schriftlich oder, und das ist neu, auch in elektronischer Form geschlossen werden kann.

Für alle Auftragsverarbeiter besteht zukünftig die neue Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO für alle Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung führen. Diese müssen der Aufsichtsbehörde auf Anfrage, z. B. bei Kontrollen, zur Verfügung gestellt werden.

Neu ist zukünftig auch der Begriff des „gemeinsamen Verantwortlichen“ (Joint Controller). Legen nach Art. 26 DSGVO zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie „gemeinsam Verantwortliche“. Sie legen dann in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere

was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten nachkommt.

ePrivacy Tipp: Falls Sie als Auftraggeber einen Dienstleister beauftragen, prüfen Sie noch einmal, ob Ihnen dessen TOMs vorliegen und ob sie ausreichend sind. Sind Sie als Auftragsverarbeiter tätig, beginnen Sie rechtzeitig damit, ein Verarbeitungsverzeichnis für die im Auftrag durchgeführten Tätigkeiten anzulegen.

7. Datenschutzfreundliche Voreinstellungen, Art. 25 DSGVO

Neu ist die Verpflichtung für alle Unternehmen, zukünftig datenschutzfreundliche Voreinstellungen vorzunehmen. Es besteht gemäß Art. 25 DSGVO die Pflicht, geeignete technische und organisatorische Maßnahmen vorzunehmen, die sicherstellen, dass durch die Voreinstellung grundsätzlich nur diejenigen personenbezogenen Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, auch wirklich verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

ePrivacy Tipp: Prüfen Sie, ob Ihre IT die genannten Anforderungen zukünftig erfüllt.

8. Überarbeiten Sie ihre Verfahrensverzeichnisse. Aber: Nicht mehr jeder braucht das Verzeichnis!

Art. 30 DSGVO legt neue Anforderungen für ein Verfahrensverzeichnis fest, dass zukünftig „Verzeichnis aller Verarbeitungstätigkeiten“ heißen wird. Nach Art. 30 DSGVO muss jeder Verantwortliche ein solches „Verzeichnis aller Verarbeitungstätigkeiten“ führen, sofer die Verarbeitungstätigkeit seiner Zuständigkeit unterliegt. Das Verzeichnis enthält zukünftig folgende Angaben:

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation;
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Das Verzeichnis ist schriftlich zu führen, was auch in elektronischer Form sein kann. Der Verantwortliche (oder der Auftragsverarbeiter, für den diese Regeln auch weitestgehend gelten) stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

ACHTUNG: Die genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn,

- die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen,
- die Verarbeitung erfolgt nicht nur gelegentlich oder
- es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10.

Da in der Onlinebranche viele Unternehmen eine Datenverarbeitung nicht nur „gelegentlich“ durchführen, sondern dies der Hauptzweck der geschäftlichen Tätigkeit ist, bedeutet dies für sie, dass sie von der Pflicht zur Erstellung des Verzeichnisses in der Regel nicht freigestellt sind. Jedes Unternehmen, das im Bereich der Onlinewerbung mit Themen wie Targeting, Nutzerprofilen, Cookie-IDs u. ä. befasst ist, ist nach wie vor zur Erstellung eines entsprechenden Verzeichnisses von Verarbeitungstätigkeiten verpflichtet.

ePrivacy Tipp: Prüfen Sie, ob Sie ein Verarbeitungsverzeichnis erstellen müssen, und beginnen Sie rechtzeitig damit. Sollten Sie bereits ein Verzeichnis führen, prüfen Sie, welche Ergänzungen Sie ggf. vornehmen müssen. Denken Sie daran, dass es in Zukunft strikter geahndet wird, falls Sie bei einer Prüfung durch die Behörde kein Verzeichnis vorlegen können.

9. Neu: Die sog. Datenschutzfolgenabschätzung

Neu eingeführt wurde die sog. Datenschutzfolgenabschätzung, Art. 35 DSGVO. Hat nach dieser Vorschrift eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich „ein hohes Risiko“ für die Rechte und Freiheiten betroffener natürlicher Personen zur Folge, so führt der Verantwortliche – also das Unternehmen - vorab „eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch“. Dabei ist der Rat des Datenschutzbeauftragten einzuholen (Art. 35 Abs.2 DSGVO).

Die Datenschutz-Folgenabschätzung ist insbesondere in folgenden Fällen erforderlich:

- Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die **Rechtswirkung** gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen,

- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Die Aufsichtsbehörden werden zudem zukünftig eine Liste der Verarbeitungsvorgänge veröffenltichen, für die immer eine Datenschutz-Folgenabschätzung durchzuführen ist.

Für die **Onlinebranche** enthält die oben erwähnte erste Voraussetzung eine wichtige Einschränkung. Denn danach bedarf eine automatisierte Verarbeitung von Daten – die in der Onlinebranche häufig vorkommt – nur dann einer Datenschutz-Folgenabschätzung, wenn diese entweder **Rechtswirkung** gegenüber natürlichen Personen entfaltet oder besonders sensible Daten verarbeitet werden. Die Auslieferung von programmatischer Werbung auf der Basis von möglicherweise erstellten Nutzerprofilen entfaltet aber in der Regel keine Rechtswirkung; in der Regel werden auch keine besonderen Arten personenbezogener Daten verarbeitet. In vielen Fällen der Onlinewerbung wird es deshalb nicht erforderlich sein, eine Datenschutzfolgenabschätzung vorzunehmen. Umso wichtiger ist es aber für das eigene Unternehmen festzustellen, ob die Voraussetzungen erfüllt sind oder nicht.

Ist eine Folgenabschätzung erforderlich, dann sollte sie zumindest folgendes enthalten (Art. 35 Abs. 7 DSGVO):

- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der vom Verantwortlichen verfolgten berechtigten Interessen,
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten

Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

ePrivacy Tipp: Prüfen Sie, ob Sie eine Datenschutzfolgenabschätzung durchführen müssen, indem Sie das Risiko für die Betroffenen einschätzen. Dies sollte in der Regel nicht der Fall sein, es sei denn, Sie betreiben Profiling oder verarbeiten besondere Arten von Daten. Halten Sie sich auf dem Laufenden, wann die Aufsichtsbehörden die Black- bzw. Whitelist herausgeben, und prüfen Sie dann, ob Ihr Verfahrenstyp dort aufgelistet ist.

10. Recht auf Löschung (Recht auf Vergessenwerden), Art. 17 DSGVO

Art. 17 DSGVO hat ein neues Recht, das sogenannte „Recht auf Vergessenwerden" eingeführt. Geblieben sind aber die üblichen Rechte auf Löschung der eigenen personenbezogenen Daten.

Insoweit bestimmt Art. 17 Abs. 1 DSGVO zunächst, dass jeder Betroffene das Recht hat, von dem jeweils Verantwortlichen zu verlangen, das ihn betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der nachfolgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung.
- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich.

ePrivacy Tipp: Bereiten Sie sich ggf. darauf vor, Daten auf Verlagen des Betroffenen hin zu löschen, und richten Sie einen entsprechenden Prozess ein.

11. Recht auf Datenübertagbarkeit

Neu ist auch das Recht auf Datenübertragbarkeit, Art. 20 DSGVO. Jede betroffene Person hat danach das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen – zum Beispiel Facebook - bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Ferner hat sie das Recht, diese Daten einem anderen Verantwortlichen (zum Beispiel Google +) ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln.

ePrivacy Tipp: Prüfen Sie, ob Sie ihr Geschäftsmodell von der Datenübertragbarkeit betroffen ist, und bereiten Sie diese ggf. rechtzeitig vor. Tauschen Sie sich evtl. mit anderen Unternehmen aus, wie diese die Anforderung umsetzen. Der Bitkom hat jüngst eine Stellungnahme zu diesem Thema veröffentlicht.

12. Neue Benachrichtigungspflicht bei Datenpannen

Wie schon bisher in § 42 a BDSG geregelt, besteht nach wie vor eine Informationspflicht bei unrechtmäßiger Kenntniserlangung bestimmter personenbezogener Daten.

Gem. Art. 33 DSGVO ist jeder Verantwortliche verpflichtet, im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich – und das ist neu – möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese bei der zuständigen Aufsichtsbehörde zu melden. Dies gilt nur dann nicht, wenn die Verletzung voraussichtlich nicht zu einem Risiko „für die Rechte und Freiheiten natürlicher Personen“ führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Neu ist auch die in Abs. 5 geregelte Verpflichtung, wonach der Verantwortliche sämtliche Verletzungen des Schutzes personenbezogener Daten dokumentieren muss. Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen von Art. 33 DSGVO ermöglichen.

Jede Meldung muss folgende Informationen enthalten:

- Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der

betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze,

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
- eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

ePrivacy Tipp: Prüfen Sie, ob Sie bereits einen Notfallplan für den Fall eines Datenabflusses definiert haben. Falls nicht, sollten Sie dies nachholen und ggf. die zuständigen Mitarbeiter in Kenntnis setzen. Bedenken Sie auch den Fall, dass es Freitagabends zu einer Datenpanne kommt, was bedeutet, dass die Meldung bis Montagabends erfolgt sein muss. Der Notfallplan kann z. B. Teil eines Datenschutz- und Datensicherheits-Konzepts Ihres Unternehmens sein.

13. Sicherheit der Datenverarbeitung

Die DSGVO verpflichtet auch zukünftig jeden Verantwortlichen dazu, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Datenschutzrisiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen müssen den Stand der Technik, die Implementierungskosten, die Art, den Umfang, die Umstände und der Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Die Maßnahmen können u. a. folgendes einschließen:

- Eine Pseudonymisierung und Verschlüsselung personenbezogener Daten.
- Die Fähigkeit, die Vertraulichkeit Integrität und Verfügbarkeit von Daten sicherzustellen.

- Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherstellen zu können.

- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

ePrivacy Tipp: Überprüfen Sie Ihre heute schon bestehenden technischen und organisatorischen Maßnahmen und stellen Sie sicher, dass zukünftig eine regelmäßige Überprüfung und die damit einhergehende Dokumentation für die Zukunft sichergestellt wird.

14. Neue Aufgaben und Pflichten des Datenschutzbeauftragten

Auch zukünftig wird es in Deutschland erforderlich sein, einen Datenschutzbeauftragten zu bestellen. Denn in Deutschland wird die Bestellpflicht eines Datenschutzbeauftragten abweichend zur DSGVO geregelt, und zwar im sog. Allgemeinen Bundesdatenschutzgesetz (ABDSG). Demnach muss ein Datenschutzbeauftragter bestellt werden, wenn mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. Auch der verschärfte Kündigungsschutz gilt, wie schon heute im BDSG geregelt, unverändert auch nach Geltung der DSGVO fort. Neu ist, dass Art. 37 Abs. 7 DSGVO vorsieht, dass der „Verantwortliche oder Auftragsverarbeiter“ die Kontaktdaten des Datenschutz-beauftragten veröffentlicht und diese Daten der Aufsichtsbehörde mitteilt.

Für die Verletzung dieser Pflichten kann nach der DSGVO zukünftig gem. § 83 Abs. 4 ein Bußgeld verhängt werden, und zwar in Höhe bis zu 10 Mio. Euro oder 2% des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist.

ePrivacy Tipp: Falls Sie bisher keinen Datenschutzbeauftragten bestellt haben, prüfen Sie, ob Sie das tun müssen, veröffentlichen Sie seine Kontaktdaten und teilen Sie sie der Aufsichtsbehörde mit.

15. Neue Bußgelder und Sanktionen

Der heutige Bußgeldrahmen des BDSG beläuft sich noch je nach Schwere des Verstoßes auf bis zu 50.000,00 Euro bzw. 300.000,00 Euro. Die DSGVO bringt hier in Art. 83 ff. weitreichende Verschärfungen. Der neue Bußgeldrahmen der DSGVO beläuft sich je nach Schwere des Verstoßes auf Geldbußen bis zu 10. Mio. Euro oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes, je nachdem, welcher der Beträge höher ist. Bei Verstößen gegen die Bestimmungen der Art. 5, 6, 7 und 9 – also insbesondere bei der Verarbeitung von personenbezogenen Daten – steigt der Bußgeldrahmen auf bis zu 20 Mio. Euro oder im Falle eines Unternehmens von bis zu 4 % seiner gesamten weltweit erzielten Jahresumsatzes.

ePrivacy Tipp: Machen Sie sich bewusst, dass Verstöße gegen das Datenschutzrecht künftig mit weitaus höheren Bußgeldern bewehrt sind als bisher, und informieren Sie ggf. auch ihre Mitarbeiter darüber.

16. Haftungserstreckung auf ausländische Unternehmen

Die Haftung nach der DSGVO trifft zukünftig auch vermehrt ausländische Unternehmen, selbst wenn sie keine eigene Filiale in einem Mitgliedsstaat der europäischen Union unterhalten. Gemäß Art. 3 DSGVO reicht es aus, dass ausländische Unternehmen entweder betroffenen Personen in der EU Waren oder Dienstleistungen anbieten oder – und das dürfte für die Onlinemarketingbranche wichtig sein – dass diese Unternehmen das Verhalten betroffener Personen „beobachten“, soweit ihr Verhalten in der EU erfolgt. Unternehmen der Onlinemarketingbranche, die also Techniken insbesondere zur Nachverfolgung von Internetaktivitäten, wie z. B. bei Tracking, Profiling und Targeting einsetzen, haften nach den Bestimmungen der DSGVO selbst dann, wenn sie keine eigene Niederlassung in der EU betreiben.

ePrivacy Tipp: Prüfen Sie, ob Sie mit Unternehmen zusammenarbeiten, auf die dies zutrifft, und informieren Sie diese ggf darüber. So erhöhen Sie die Bereitschaft.

17. Erweiterte Dokumentations- und Nachweispflichten

Die Datenschutzgrundverordnung sieht für Verantwortliche und Auftragsverarbeiter in vielen Fällen deutlich erweiterte Dokumentationspflichten vor. So schreibt Art. 5 Abs. 2 DSGVO vor, dass der für die Verarbeitung Verantwortliche nachweisen können muss, dass er die in Art. 5 Abs. 1 DSGVO geregelten Datenschutzgrundsätze einhält. Verstößt ein verantwortliches Unternehmen gegen diese Vorgabe, drohen Bußgelder wie oben erwähnt von bis zu 4 % des Umsatzes.

Nach Art. 24 Abs. 1 DSGVO muss der für die Verarbeitung Verantwortliche überdies nachweisen können, dass er personenbezogene Daten in Übereinstimmung mit der DSGVO verarbeitet. Auftragsverarbeiter müssen den Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, damit der Verantwortliche nachweisen kann, dass er seine in den Art. 32 ff. DSGVO geregelten Pflichten erfüllt.

ePrivacy Tipp: Prüfen Sie, ob Sie den erweiterten Dokumentationspflichten im Falle einer Anfrage durch die Aufsichtsbehörde nachkommen könnten. Hierzu gehört etwa die Dokumentation der Risikoeinschätzung im Zuge der Prüfung, ob eine Folgeabschätzung notwendig ist (siehe oben) u. a. Falls Sie als Auftragsverarbeiter tätig sind, müssen Sie damit rechnen, dass Ihr Auftraggeber Sie nach den entsprechenden Unterlagen wie etwa Verarbeitungsübersicht oder TOMs fragt.

18. Datenschutzmanagementsysteme

Die Anforderungen an die Unternehmen, an ihre Datenschutzorganisation und Datenschutzprozesse werden zukünftig stark steigen. Das liegt vor allem am sog. risikobasierten Datenschutz, der an vielen Stellen in der DSGVO etabliert wurde. Gerade die Anforderungen der Art. 24 und 25 DSGVO sowie der stark gestiegene Bußgeldrahmen werden es zukünftig in vielen Fällen erforderlich machen, sog. Datenschutzmanagementsysteme zu entwickeln. Unter einem Datenschutz-managementsystem versteht man die Gesamtheit aller dokumentierten und implementierten Regelungen, Prozesse und Maßnahmen, die dazu dienen, einen datenschutzkonformen Umgang mit personenbezogenen Daten im Unternehmen systematisch zu steuern.

ePrivacy Tipp: Prüfen Sie, ob die Einführung eines Datenschutzmanagement-systems für Sie sinnvoll sein könnte und wägen Sie alternative Optionen rechtzeitig und sorgfältig ab.