Die neue EU-Datenschutz-Grundverordnung

02/2018

Gliederung

I. Einleitung

Ab 25.05.2018 gilt die neue EU-Datenschutz-Grundverordnung (DS-GVO). Sie regelt den Umgang mit sensiblen personenbezogenen Daten (Kunden-, Patienten-, Mandantendaten usw.) und löst damit das Bundesdatenschutzgesetz ab.

Worum geht es in der Verordnung?

Mit der DS-GVO soll ein einheitlicher Datenschutzstandard innerhalb der EU geschaffen werden. Personenbezogene Daten sollen besser geschützt und der freie Datenverkehr innerhalb des Europäischen Binnenmarktes soll gewährleistet werden.

Wen betrifft die Verordnung?

Die Verordnung betrifft alle Unternehmen mit Hauptsitz in der Europäischen Union. Dabei ist es nicht ausschlaggebend, ob es sich um ein großes oder ein kleines Unternehmen handelt. Die Verordnung gilt grundsätzlich für alle Branchen.

II. Überblick

Was steht konkret in der Verordnung?

Da die Verordnung sehr umfangreich ist, können nicht alle Regelungen wiedergegeben werden. Zunächst werden lediglich die wichtigen Regelungen aufgezählt:

- Die Nutzung/Verarbeitung von personenbezogenen Daten soll durch eine eindeutige bestätigende Handlung erfolgen (Zustimmung)

- Nachweisführung für Einwilligung / Zustimmung der betroffenen Personen zur Verarbeitung von Daten
- Datentransparenz für natürliche Personen, damit diese sehen können, in welchem Umfang personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden
- Es sollen Modalitäten festgelegt werden, die einer betroffenen Person die Ausübung der Rechte, die ihr durch die Verordnung zustehen, erleichtern
- Es sollen Mechanismen festgelegt werden, die dafür sorgen, dass betroffene Personen unentgeltlich Zugang zu ihren personenbezogenen Daten erhalten
- Betroffenen Personen muss ein Recht auf Löschung und „Vergessenwerden“ eingeräumt werden
- Anträge auf Zugang oder Löschung müssen leicht verständlich sein und in elektronischer Form bereitgestellt werden
- Jedem Betroffenen muss ein Widerrufsrecht hinsichtlich der Nutzung, Speicherung, Verwertung von personenbezogenen Daten zustehen
- Führen eines Verzeichnisses von Verarbeitungstätigkeiten
- Haftung und Recht auf Schadensersatz der betroffenen Personen wegen eines Verstoßes gegen diese Verordnung gegen Verantwortlichen
- Gegebenenfalls Einführung eines Datenschutzbeauftragten
- Meldepflichten für Verletzungen des Schutzes personenbezogener Daten

Was passiert wenn ich mich nicht an die Verordnung halte?

Ab Mai 2018 ist mit den ersten Datenschutzüberprüfungen der Landesdatenschutzbeauftragten zu rechnen. Es werden dafür Stellen eingerichtet, welche in Unternehmen den Vollzug der Verordnung kontrollieren, indem diese sich das Verzeichnis von Verarbeitungstätigkeiten vorlegen lassen. Sofern ein Verstoß gegen die Verordnung festgestellt wurde, können Bußgelder und Strafen bis zu 20 Mio. € bzw. bis zu 4 % des Bruttojahresumsatzes des Unternehmens drohen.

Sieben Schritte zur optimalen Vorbereitung

1. Erster Schritt:

   Bringen Sie Transparenz in Ihre Daten!

Vergleichen Sie Ihre aktuelle Vorgehensweise mit den Anforderungen der neuen Verordnung und überlegen Sie, was Sie verändern müssen, um die Vorgaben auf eine Weise zu erfüllen, die den Bedürfnissen Ihrer Organisation entspricht.

Denken Sie daran, dass die Erfüllung der Verpflichtungen lt. DS-GVO nicht nur die Richtlinien und Maßnahmen Ihres eigenen Unternehmens einbezieht, sondern auch

die jeglicher Anbieter, die in Ihrem Namen personenbezogene Daten verarbeiten.

2. Zweiter Schritt:

   Die Verantwortlichkeiten für den Datenschutz in Ihrem Unternehmen regeln.

Jedes Unternehmen, größenunabhängig, ist ab dem 25.05.2018 verpflichtet, Verfahren für Datenschutz-Compliance einzuführen. Nicht alle Unternehmen müssen jedoch einen Datenschutzbeauftragten ernennen.

3. Dritter Schritt:

   Die rechtliche Basis für die Datenverarbeitung prüfen.

Anhand der Übersicht über Ihre unterschiedlichen personenbezogenen Daten aus Schritt 1 sollten Sie prüfen, welche Rechtsgrundlagen aktuell für die Verarbeitung der verschiedenen Arten von personenbezogenen Daten gelten. Wenn Sie eine Zustimmung als Grundlage für die Datenverarbeitung nutzen, müssen Sie überlegen, wie Sie diese Zustimmung einholen, und in der Lage sein, klar zu zeigen, wie und wann diese Zustimmung erteilt wurde. Lag bisher keine Zustimmung für die Verarbeitung der jeweiligen personenbezogenen Daten vor, so ist diese rückwirkend einzuholen.

4. Vierter Schritt:

   Rechte des betroffenen Personenkreises prüfen.

Lt. der Verordnung genießt jede Person, deren Daten Sie verarbeiten, einen erweiterten Rechtsschutz dahingehend, auf die eigenen persönlichen Daten zuzugreifen, diese korrigieren, löschen oder elektronisch übertragen zu lassen.

Kann Ihr Unternehmen Kundendaten schnell und einfach finden, löschen und bewegen?

Hat Ihr Unternehmen und Dritte, mit denen Sie zusammenarbeiten, Aufzeichnungen darüber, wo sich Daten befinden, wie sie verarbeitet werden und wo sie geteilt wurden?

Auch hier hilft die Liste aus Schritt 1.

5. Fünfter Schritt:

   Denken Sie an Ihre Drittanbieter für die Datenverarbeitung.

Prüfen Sie, ob Ihre Datenverarbeitungsanbieter internationale Datenschutzstandards erfüllen, Erfahrungen im Datensicherheitsmanagement in großem Umfang haben und über Tools verfügen, die Ihre Rechtssicherheit verbessern und Verletzungsrisiken verringern. Überprüfen Sie bestehende Verträge und aktualisieren Sie Vereinbarungen mit Ihren Drittanbietern.

6. Sechster Schritt:

   Kommunizieren Sie wichtige Informationen intern wie extern.

Lt. der Verordnung sind Sie verpflichtet, die rechtlichen Grundlagen für die Verarbeitung Ihrer Daten mitzuteilen und sicherzustellen, dass Ansprechpartner und Behörden im Falle eines auftretenden Problemfalls bekannt sind. Stellen Sie also sicher, dass Ihre Online-Datenschutzerklärungen auf der Website sowie Ihre AGBs auf dem neuesten Stand sind.

Darüber hinaus sollten Sie alle Ihre Mitarbeiter über die neuen Rahmenbedingungen der Verordnung informieren und sie entsprechend aufklären.

Sensibilisieren und verpflichten Sie Ihre Mitarbeiter.

7. Siebter Schritt:

   Erstellen Sie einen Notfallplan für evtl. Datenschutzverletzungen.

Ihr Unternehmen muss über geeignete Richtlinien und Prozesse für den Fall von Datenschutzverletzungen verfügen. Stellen Sie dabei den Informationsfluss sicher:

Welche Behörden sind Ihr Ansprechpartner für Datenpannen?

Welche formalen Voraussetzungen, z. B. Fristen, müssen erfüllt werden?

Informieren Sie Ihr Management über diese Richtlinien und Prozessabläufe.

Es ist eine 72-Stunden-Frist einzuhalten.

III. Welche Rechte hat der Betroffene einer Datenverarbeitung

1. Informationsrecht

Welche Informationspflichten bestehen nach Art. 13 DS-GVO?

Werden personenbezogene Daten beim Betroffenen erhoben, muss der Verantwortliche nach Art. 13 Abs. 1 DS-GVO folgende Informationen mitteilen:

a) Identität des Verantwortlichen

Es ist über den Namen und die Kontaktdaten des Verantwortlichen zu informieren.

b) Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)

Neu ist die Verpflichtung der Mitteilung der Kontaktdaten des Datenschutzbeauftragten.

c) Verarbeitungszwecke und Rechtsgrundlage

Der Verantwortliche muss über die Zwecke der Datenverarbeitung sowie über die Rechtsgrundlage der Verarbeitung informieren. Diese neue Anforderung führt dazu, dass der Betroffene darüber aufgeklärt wird, auf welchen Erlaubnistatbestand (s. Art. 6 DS-GVO, z. B. Einwilligung oder Erfüllung eines Vertrages) der Verantwortliche die Datenverarbeitung stützen möchte.

d) Berechtigtes Interesse

Sollte die Verarbeitung personenbezogener Daten zur Wahrung berechtigter Interessen des Verantwortlichen nach Art. 6 Abs. 1f) DS-GVO erforderlich sein, beziehen sich die Informationspflichten auch auf eine Aufklärung über diese Interessen.

e) Empfänger

In allen Fällen, in denen personenbezogene Daten übermittelt werden sollen, sind die Betroffenen grundsätzlich über die konkreten Empfänger zu informieren. Ausnahmsweise reicht auch eine Information über Kategorien von Empfängern, wenn konkrete Unternehmen noch nicht bezeichnet werden können.

Nach Art. 13 Abs. 2 DS-GVO muss der Verantwortliche dem Betroffenen darüber hinaus weitere Informationen mitteilen, die insbesondre notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) Dauer der Speicherung

Es ist konkret anzugeben, für wie lange personenbezogene Daten gespeichert werden. Nur ausnahmsweise, wenn die Angabe einer konkreten Zeitspanne dem Verantwortlichen nicht möglich ist, reichen Kriterien für die Festlegung der endgültigen Dauer der Speicherung aus.

b) Rechte der Betroffenen

Die Betroffenen sind über ihre Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Bearbeitung, Widerspruch gegen die Verarbeitung sowie Datenübertragbarkeit hinzuweisen, die sich aus den Art. 15 bis 21 DS-GVO ergeben.

c) Widerrufbarkeit von Einwilligungen

Soweit die Verarbeitung auf einer Einwilligung des Betroffenen beruht, ist auch darauf gesondert hinzuweisen. Die entsprechende Informationspflicht ist nur erfüllt, wenn gleichzeitig darüber aufgeklärt wird, dass die Einwilligung jederzeit widerrufen werden kann und die Datenverarbeitung bis zum Zeitpunkt des Widerrufs rechtmäßig bleibt.

d) Beschwerderecht bei der Aufsichtsbehörde

Der Betroffene ist darüber aufzuklären, dass er sich gem. Art. 77 DS-GVO bei einer Aufsichtsbehörde beschweren kann, wenn er der Ansicht ist, dass die Verarbeitung seiner personenbezogenen Daten rechtswidrig erfolgt.

e) Verpflichtung zur Bereitstellung personenbezogener Daten

Der Verantwortliche muss den Betroffenen darüber informieren, ob die Bereitstellung seiner personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben, für einen Vertragsschluss erforderlich ist oder eine sonstige Verpflichtung besteht und

welche Folgen eine Nichtbereitstellung hätte.

f) Automatisierte Entscheidungsfindung und Profiling

Sobald der Verantwortliche Verfahren der automatisierten Entscheidung nach Art. 22 DS-GVO oder andere Profiling-Maßnahmen nach Art. 4 DS-GVO durchführt, muss der Betroffene über die besondere Tragweite und die angestrebten Auswirkungen solcher Verfahren informiert werden. Diese Informationspflicht erstreckt sich auch auf Angaben zu der dazu verwendeten Logik oder des Algorhythmus.

Welche Informationspflichten bestehen nach Art. 14 DS-GVO?

Werden personenbezogene Daten nicht beim Betroffenen erhoben, bestehen nach Art. 14 DS-GVO für den Verantwortlichen nahezu dieselben Informationspflichten wie bei der Erhebung direkt beim Betroffenen.

Logischerweise muss allerdings hier der Betroffene nicht über eine etwaige Verpflichtung zur Bereitstellung informiert werden, da er selbst nicht über die Bereitstellung entscheiden kann.

Nach Art. 14 Abs. 2f) DS-GVO muss der Verantwortliche den Betroffenen jedoch darüber aufklären, aus welcher Quelle die personenbezogenen Daten stammen und ob es sich dabei um eine öffentlich zugängliche Quelle handelt.

In welcher Form müssen die Informationen bereitgestellt werden?

Nach Art. 12 DS-GVO sind die oben dargestellten Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form zu erteilen. Dabei können sie schriftlich oder in elektronischer Form an den Betroffenen übermittelt werden.

Wann muss der Betroffene informiert werden?

Bei der Direkterhebung muss der Betroffene nach Art. 13 Abs. 1 DS-GVO zum Zeitpunkt der Erhebung, z. B. bei Bestellung eines Newsletters, informiert werden.

Werden die Daten nicht beim Betroffenen erhoben, muss der Verantwortliche die Informationen nach Art. 14 Abs. 2 DS-GVO grundsätzlich innerhalb einer angemessenen Frist, spätestens jedoch nach einem Monat, erteilen. Werden die Daten allerdings zur Kommunikation mit dem Betroffenen verwendet oder sollen sie an einen Empfänger übermittelt werden, ist die Information zwingend zum Zeitpunkt der Kontaktaufnahme oder ersten Übermittlung vorzunehmen.

Kann die Informationspflicht eingeschränkt sein?

Bei der Direkterhebung kann nach Art. 13 Abs. 4 DS-GVO auf die Information des Betroffenen nur dann verzichtet werden, wenn dieser bereits informiert wurde.

Soweit die Daten nicht beim Betroffenen erhoben werden, sind die Informationspflichten gem. Art. 14 Abs. 5 DS-GVO in drei weiteren Fällen entbehrlich:

- Die Information ist unmöglich oder unverhältnismäßig aufwendig
- Die Erhebung oder Übermittlung ist gesetzlich vorgeschrieben
- Es besteht ein Berufsgeheimnis oder eine sonstige satzungsmäßige Geheimhaltungspflicht

Was passiert bei Verstößen gegen die Informationspflicht?

Wenn Verantwortliche ihren Informationspflichten nicht nachkommen, droht gem. Art. 83 Abs. 5b DS-GVO ein Bußgeld. Der europäische Gesetzgeber sieht die Gewährleistung einer fairen und transparenten Datenverarbeitung mithilfe umfassender Informationen als elementar an und bedroht Verstöße in diesen Fällen mit dem hohen Bußgeldrahmen, der Bußgelder bis zu 20 Mio. € oder 4 % des Jahresumsatzes vorsieht.

2. Auskunftsrecht

Welche Informationen fallen unter das Auskunftsrecht nach Art. 15 DS-GVO?

- Zwecke der Datenverarbeitung
- Kategorien der Daten
- Empfänger oder Kategorien von Empfängern
- Dauer der Speicherung
- Rechte auf Berichtigung, Löschung und Widerspruch
- Beschwerderecht bei einer Aufsichtsbehörde
- Herkunft der Daten (wenn nicht beim Betroffenen erhoben)
- Bestehen einer automatisierten Entscheidungsfindung einschl. Profiling

Wie ist der Betroffene zu informieren bei Geltendmachung des Auskunftsrechts?

- Durch Kopie aller personenbezogenen Daten auf gängigem elektronischen Weg

3. Recht auf Berichtigung und Löschung (Vergessenwerden)

Was bedeutet das Recht auf Berichtigung nach Art. 16 DS-GVO?

Es gibt dem Betroffenen die Möglichkeit, die Vervollständigung seiner personenbezogenen Daten ohne unangemessene Verzögerung zu verlangen.

Wann sind personenbezogene Daten zu löschen?

Nach Art. 17 Abs. 1 DS-GVO sind personenbezogene Daten künftig unverzüglich zu löschen, wenn

- die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf

sonstige Weise verarbeitet wurden, nicht mehr notwendig sind,

- die betroffene Person ihre Einwilligung widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt,
- die betroffene Person Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen,
- die personenbezogenen Daten unrechtmäßig verarbeitet wurden,
- die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich ist.

Wie kann eine Löschung vorgenommen werden?

Ausreichend ist es

- die Datenträger physisch zu zerstören,
- Verknüpfungen oder Codierungen zu löschen,
- bei wiederbeschreibbaren Datenträgern (z. B. einer Festplatte) ggf. spezielle Löschsoftware einzusetzen.

Nicht ausreichend ist es,

- Datenträger einfach zu entsorgen, also in den Müll zu werfen,
- rein organisatorische Maßnahmen zu treffen.

Wird die Löschung abgelehnt, ist dies vom Verantwortlichen zu begründen. Auf die Möglichkeit zur Beschwerde bei einer Aufsichtsbehörde und auf einen gerichtlichen Rechtsbehelf ist hinzuweisen.

Wann ist zu löschen?

Die betroffenen Daten sind unverzüglich zu löschen, das bedeutet „ohne schuldhaftes Zögern“.

Bei einem Löschungsantrag des Betroffenen ist in jedem Fall zu beachten, dass spätestens innerhalb eines Monats nach Eingang des Löschungsantrags die betroffene Person über die ergriffenen Maßnahmen bzw. die Gründe der Ablehnung informiert werden muss.

Wann findet das Recht auf Vergessenwerden keine Anwendung?

- Wenn die Datenspeicherung der Erfüllung einer rechtlichen Verpflichtung dient
- Wenn das öffentliche Interesse im Bereich der öffentlichen Gesundheit überwiegt
- Wenn die Speicherung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist

Wann spielt das Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO eine Rolle?

- Wenn die Daten vom Betroffenen bestritten werden
- Wenn die Verarbeitung unrechtmäßig ist
- Wenn ein Widerspruch des Betroffenen nach Art. 21 DS-GVO vorliegt

Welche Mitteilungs- und Informationspflicht bestehen bei Löschung?

Der nach der Verordnung für die Verarbeitung Verantwortliche teilt allen Empfängern, an den die Daten weitergegeben wurden, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigem Aufwand verbunden.

Werden auch dem Betroffenen die Empfänger seiner weitergegebenen Daten bekannt gegeben?

Wenn der Betroffene dies wünscht, muss der für die Verarbeitung Verantwortliche die Informationen über die Empfänger, an die die Daten weitergegebenen wurden, mitteilen.

4. Recht auf Datenübertragbarkeit

Was bedeutet das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO?

Der Betroffene soll befugt sein, die von ihm zur Verfügung gestellten Daten von einer automatisierten Anwendung auf eine andere Anwendung zu übertragen. Betroffene sollen dadurch leichter von einem Anbieter zu einem anderen Anbieter wechseln können, ohne den Verlust ihrer Daten befürchten zu müssen.

IV. Welche Pflichten hat ein Unternehmen?

1. Technischer Datenschutz

Was bedeuten die Vorgaben des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen nach Art. 25 DS-GVO?

Der für die Verarbeitung Verantwortliche sollte intern Strategien festlegen und Maßnahmen treffen, die insbesondere dem Grundsatz des Datenschutzes durch Technik (data-protection by design) und durch datenschutzfreundliche Voreinstellungen (data-protection by default) sicherstellen.

Was sollte das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO beinhalten?

- Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen (ggf.

auch Vertreter und Datenschutzbeauftragter)

- Zwecke der Verarbeitung
- Kategorien von betroffenen Personen und personenbezogenen Daten
- Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden
- Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Verzeichnis von Verarbeitungstätigkeiten

Das Verzeichnis von Verarbeitungstätigkeiten nach der DS-GVO ist im Grundsatz nichts anderes als das altbekannte Verfahrensverzeichnis nach §§ 4g Abs. 2, 4e BDSG. Es handelt sich also um eine Dokumentation und Übersicht über Verfahren, bei denen personenbezogene Daten verarbeitet werden.

Welche Sanktionen drohen bei einem fehlenden Verzeichnis von Verarbeitungstätigkeiten?

Mit Einführung der Verordnung müssen Verantwortliche nun die Verzeichnisse von Verarbeitungstätigkeiten jederzeit und vollständig für die Aufsichtsbehörden vorhalten können, ansonsten droht ein Bußgeld (Art. 83 Abs. 4a DS-GVO). Der mögliche Rahmen bewegt sich hier bis zu 10 Mio. € oder bei Unternehmen bis zu 2 % des Jahresumsatzes.

Ist das Verzeichnis von Verarbeitungstätigkeiten öffentlich zu machen?

Während das alte Verfahrensverzeichnis in weiten Teilen noch auf Antrag jedermann zugänglich zu machen war, besteht diese Pflicht bei den Verzeichnissen von Verarbeitungstätigkeiten nur noch gegenüber den Aufsichtsbehörden.

Gibt es Ausnahmen von der Pflicht eines Verzeichnisses von Verarbeitungstätigkeiten?

Für Unternehmen oder Einrichtungen mit weniger als 250 Mitarbeitern gibt es zwar eine gewisse Erleichterung, die allerdings nur selten einschlägig sein dürfte. Hiernach sind diese nach Art. 30 Abs. 5 DS-GVO von der Führung eines Verzeichnisses befreit, außer

- die vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen (z. B. Scoring),
- die Verarbeitung erfolgt nicht nur gelegentlich oder
- es erfolgt eine Verarbeitung besonderer Datenkategorien gem. Art. 9 Abs. 1 DS-GVO (z. B. Gesundheitsdaten) bzw. die Verarbeitung von personenbezogenen

Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO.

In erster Linie die Ausnahme von der Ausnahme „die Verarbeitung erfolgt nicht nur gelegentlich“ unterwirft die meisten Unternehmen wieder der Pflicht, ein Verzeichnis führen zu müssen. Dies bedeutet zusätzlichen bürokratischen Aufwand für Kleinstunternehmer, wie etwa Handwerker und kleine Gewerbebetriebe, aber auch Arztpraxen und Apotheken. Diese waren nach der bislang geltenden Gesetzeslage regelmäßig nicht verpflichtet, Verfahrensverzeichnisse zu führen.

Neu ist, dass neben den verantwortlichen Stellen auch die Stellen, die nur im Auftrag der verantwortlichen Stellen Daten verarbeiten (Auftragsdatenverarbeiter), entsprechende Verzeichnisse führen müssen (Art. 30 Abs. 2 DS-GVO).

Im Falle von fehlender Datenschutzdokumentation muss zunächst ermittelt werden, in welchen Fällen personenbezogene Daten von z. B. Kunden, Lieferanten oder Beschäftigten erhoben und verarbeitet werden. Hierzu bietet es sich als erster Anhaltspunkt an, alle innerhalb der Systemlandschaft des Unternehmens eingesetzten Anwendungen und Tools aufzulisten, in denen personenbezogene Daten gespeichert werden. Dies hilft gleichsam bei der Ermittlung der Datenflüsse im Unternehmen und kann auch als Grundlage für das Verzeichnis von Verarbeitungstätigkeiten dienen. Dieses wird in der Praxis zwecks Übersichtlichkeit meist aus mehreren Verzeichnissen für verschiedene Verarbeitungsvorgänge (z.B. Zeiterfassungssysteme, CRM-Systeme etc.) bestehen.

2. Meldepflicht

Müssen Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde gemeldet werden?

Nach Art. 33 DS-GVO grundsätzlich Ja.

Gilt die Meldepflicht ausnahmslos immer?

Nein. Es entsteht keine Meldepflicht, wenn ein Risiko für Rechte und Freiheiten von Individuen unwahrscheinlich ist.

Gibt es eine Frist für die Meldepflicht?

Ja. Nach Art. 33 DS-GVO unverzüglich und ohne unangemessene Verzögerung. Möglichst binnen höchstens 72 Stunden, nachdem die Verletzung bekannt wurde.

Muss auch der Betroffene der Datenschutzverletzung benachrichtigt werden?

Nach Art. 34 DS-GVO grundsätzlich Ja. Der Betroffene muss dann nicht benachrichtigt werden, wenn technische oder organisatorische Maßnahmen, wie z. B. eine Verschlüsselung, die Kenntnisnahme von personenbezogenen Daten verhindern oder sichergestellt ist, dass kein hohes Risiko besteht.

Wie muss der Betroffene benachrichtigt werden?

Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten und so rasch wie nach allgemeinem Ermessen möglich geschehen.

3. Daten-Folgenabschätzung

Wann muss ein Unternehmen eine Daten-Folgenabschätzung nach Art. 35 DS-GVO vornehmen?

Dann, wenn eine Form der Verarbeitung wahrscheinlich ein hohes Risiko verursacht, insbesondere bei neuen Technologien oder aufgrund ihres Wesens, ihres Umfangs, ihres Kontextes oder ihrer Zwecke.

Was sind Beispiele für derartige neue Technologien?

- Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen aufgrund automatisierter Verarbeitung
- Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten
- Systematische weiträumige Überwachung öffentlich zugänglicher Bereiche

V. Was ist zu beachten bei einer Website?

Die für Website-Betreiber wichtigsten allgemeinen Rechtfertigungen einer Datenverarbeitung sind:

- Das Vorliegen einer Einwilligung des Betroffenen
- die Notwendigkeit der Datenverarbeitung für die Durchführung eines Vertrages und
- das legitime Interesse des Datenverarbeiters, sofern nicht die Rechte des Betroffenen überwiegen

Datenschutzerklärung

Bleiben die aktuellen Vorgaben zur Datenschutzerklärung bestehen?

Ja. Insofern ist weiterhin besonderer Wert auf datenschutzkonforme Erklärungen zu

- Webformulare
  (Kontaktformulare, Newsletter etc.)
- Cookies
  (Informationen zu Zweck, Empfänger der Daten etc.)
- Analysetools
  (wie etracker)

zu legen.

VI. Was sind die Anforderungen an eine rechtsgültige Einwilligung?

Die wichtigsten Anforderungen an eine rechtsgültige Einwilligung sind regelmäßig:

- Die freie Entscheidung des Betroffenen.
- Ausführliche, erkennbare und bestimmte Informationen des Betroffenen: Der Betroffene muss vor Abgabe der Einwilligungserklärung über den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten im Einzelnen informiert werden. Der Betroffene muss außerdem in der Lage sein, die Informationen leicht zu erkennen und auch als Einwilligung zu identifizieren. Im Bereich Erkennbarkeit der Einwilligung für den Betroffenen gibt Art. 7 Nr. 2 DS-GVO Vorgaben zur Erkennbarkeit, vor allem, wenn die Einwilligung zusammen mit anderen Erklärungen abgegeben werden soll. In diesem Fall muss die Einwilligung deutlich hervorgehoben werden. Im Falle der Verarbeitung von besonders sensiblen Arten von personenbezogenen Daten muss sich die Einwilligung ausdrücklich auf diese beziehen (Art. 9 Nr. 2a DS-GVO).
- Schriftform der Einwilligungserklärung: Grundsätzlich muss lt. § 4a Abs. 1 BDSG die Einwilligung in Schriftform erfolgen, nur in speziellen Ausnahmefällen darf davon abgewichen werden. Die Möglichkeit der einfachen elektronischen Einwilligung im Bereich Internet und E-Mail wird derzeit nur durch das Telemediengesetz (§ 13 Abs. 2 TMG) geschaffen, welches in diesen speziellen Fällen zur Anwendung kommt. In Erwägungsgrund 25 zur DS-GVO wird klargestellt, dass die Einwilligung nur durch eine eindeutige Handlung zustande kommen soll, die auch in elektronischer Form erfolgen kann. Damit ist regelmäßig eine aktive Handlung des Nutzers durch Opt-In (z. B. Setzen eines Häkchens) notwendig, andere Varianten, wie eine stillschweigende Zustimmung oder Opt-Out (z. B. Entfernen eines Häkchens), sind dagegen nicht mehr möglich.
- Widerruflichkeit der Einwilligungserklärung
  In Art. 7 Nr. 3 DS-GVO ist bestimmt, dass der Betroffene vor Abgabe der Einwilligung über sein Widerrufsrecht aufgeklärt werden muss und der Widerruf der Einwilligung genauso leicht möglich sein muss, wie die Abgabe selbst.

VII. Wann besteht eine Bestellpflicht für einen Datenschutzbeauftragten?

Aufgrund der Verordnung wird es ab 2018 erstmals eine europaweit geltende Pflicht zur Bestellung eines Datenschutzbeauftragten geben (Art. 35 ff. DS-GVO). Diese ist bindend, sofern ein Unternehmer einer Tätigkeit nachgeht, die aus datenschutz-

rechtlicher Sicht einer besonderen Kontrolle bedarf. Darüber hinaus kann jedes Unternehmen einen Datenschutzbeauftragten freiwillig bestellen.

Nach Art. 37 Abs. 2 DS-GVO ist ein betrieblicher Datenschutzbeauftragter unter bestimmten Bedingungen zu benennen:

> *„(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn […]*
>
> *b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder*
>
> *c) die Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Art. 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 besteht.“*

Unter „Kerntätigkeit“ ist nach der Stellungnahme der Art. 29-Datenschutzgruppe jede Tätigkeit zu verstehen, die essenziell für die Erreichung der Ziele des Unternehmens sind. Als Beispiel sei hier die Verarbeitung von Gesundheitsdaten in einem Krankenhaus genannt.

Ziff. b) dürfte dabei insbesondere für Unternehmen, deren Kerntätigkeit der Handel mit personenbezogenen Daten ist („Daten als Ware“), Auskunfteien oder Adresshändler gelten.

Die Art. 29-Datenschutzgruppe führt einige Faktoren auf, die maßgeblich für das Merkmal „umfangreiche Verarbeitung“ im Sinne der Ziff. b) und c) sind:

- Anzahl der Betroffenen,
- die Menge der betroffenen Daten und/oder
- die Vielzahl der verschiedenen Datensätze,
- die Dauer der Datenverarbeitung,
- die geografische Reichweite der Datenverarbeitung

Auch hier werden zahlreiche Beispiele zur Verdeutlichung genannt, u. a. die Verarbeitung von Gesundheitsdaten in einem Krankenhaus oder die Verarbeitung von personenbezogenen Daten für Werbezwecke durch Suchmaschinen für verhaltensbedingte Werbevorschläge.

Unter dem Merkmal „Umfangreiche regelmäßige und systematische Überwachung“ kann man alle Arten des Internettrackings und –profilings verstehen.

In Art. 37 Abs. 7 DS-GVO ist geregelt, dass „der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und

diese Daten der Aufsichtsbehörde mitteilt „,sofern eine „Benennungspflicht“ besteht.

Auf der Website eines Unternehmens ist es ausreichend, wenn man beispielsweise eine Hotline oder spezifische Kontaktdaten veröffentlicht. Nicht erforderlich ist die Kundgabe des Namens des Datenschutzbeauftragten.

Interner oder externer Datenschutzbeauftragter?

Grundsätzlich kann ein Unternehmen wählen, ob die Position des betrieblichen Datenschutzbeauftragten intern oder extern besetzt wird (Art. 37 Abs. 6 DS-GVO).

Viele Unternehmen bedienen sich heutzutage der Möglichkeit, einen externen Datenschutzbeauftragten zu bestellen, um ihre eigenen internen Recourcen besser nutzen zu können und von den Vorteilen des spezifischen Fachwissens eines externen Datenschutzbeauftragten zu profitieren.

Welche Sanktionen drohen bei fehlender Bestellung eines Datenschutzbeauftragten?

Die vorsätzliche oder fahrlässige Versäumung, einen betrieblichen Datenschutzbeauftragten zu bestellen, diesen nicht in der vorbeschriebenen Weise oder nicht rechtzeitig zu bestellen, stellt gem. § 43 Abs. 1 Nr. 2 BDSG bereits heute eine Ordnungswidrigkeit dar, die mit einem Bußgeld in Höhe von bis zu 50.000 € belegt werden kann. Die Verordnung teilt diese Auffassung und sieht ein Bußgeld von bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes vor, je nachdem, welcher Betrag höher ist (Art. 83 Abs. 4 lit.A DS-GVO).

Welche Kriterien muss ein Datenschutzbeauftragter erfüllen?

Art. 37 Abs. 5 DS-GVO fordert

- eine gewisse berufliche Qualifikation,
- das Fachwissen auf dem Gebiet des Datenschutzes und der Datenschutzpraxis und
- die Fähigkeiten zur Erfüllung der gesetzlich definierten Aufgaben

Durch stetige Neuentwicklungen werden Datenschutzbeauftragte ständig gefordert, sodass eine stete Weiterbildung im IT- und juristischen Bereich unerlässlich ist, um den immer komplexeren Fragestellungen gerecht werden zu können.

Spätestens mit der Anwendbarkeit der noch komplexeren DS-GVO sollte der Faktor der juristischen Qualifikation eines betrieblichen Datenschutzbeauftragten nicht unterschätzt werden.

Haftung des Datenschutzbeauftragten?

Die Art. 29-Datenschutzgruppe stellt in ihrer Stellungnahme zwar eindeutig klar, dass das Unternehmen – ob Verantwortlicher oder Auftragsverarbeiter – selbst für die Einhaltung der Regelungen nach Art. 24 Abs. 1 DS-GVO verantwortlich ist.

Trotzdem haftet der Datenschutzbeauftragte in seinem Verantwortungsbereich für Datenschutzverletzungen.

Welche Aufgaben und Pflichten hat ein Datenschutzbeauftragter nach der DS-GVO?

Die Aufgaben und Pflichten eines betrieblichen Datenschutzbeauftragten sind in Art. 39 DS-GVO geregelt und umfassen:

- Unterrichtung und Beratung der Verantwortlichen, der Auftragsverarbeiter und der Beschäftigten,
- Überwachung und Einhaltung der DS-GVO und nationaler Sonderregelungen,
- Sensibilisierung und Schulung,
- Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung,
- Zusammenarbeit mit der Aufsichtsbehörde

Was sollten Unternehmen jetzt tun?

Grundsätzlich empfiehlt sich unabhängig von einer etwaigen Bestellpflicht einen betrieblichen Datenschutzbeauftragten zu bestellen, um so die Umsetzung der Datenschutzgrundverordnung in Ihrem Unternehmen auf die effektivste Weise voranzutreiben und startklar für Mai 2018 zu sein.

VIII. Fazit

Wichtig ist zunächst, dass Unternehmen sich erst einmal bewusst werden, wie die personenbezogenen Kundendaten behandelt werden, sodass zunächst eine Bestandsanalyse durchzuführen ist. Dann sollte die Behandlung der Daten entsprechend der Verordnung geregelt werden und gegebenenfalls neue technisch-organisatorische Maßnahmen zur Realisierung der DS-GVO-Anforderungen ergriffen werden. Diese Maßnahmen und die üblichen Abläufe müssen sodann niedergeschrieben werden, ein sog. Verzeichnis von Verarbeitungstätigkeiten ist anzulegen. Das Verzeichnis von Verarbeitungstätigkeiten muss auf Anfrage der Aufsichtsbehörde unverzüglich eingereicht werden.

Vermeiden Sie Abmahnungen aufgrund falscher oder fehlender Datenschutzerklärungen

Eine wesentliche Änderung der Verordnung ist es, dass Sie als Unternehmen eine Informationspflicht haben und auf Ihrer Website und möglichst allen Online-Kanälen erklären, wie Sie in Ihrem Unternehmen den Datenschutz handhaben. Je nachdem, welche Daten Sie über Ihre Online-Kanäle von Besuchern oder Kunden erfassen, kann eine solche Erklärung sehr umfangreich werden und einige Punkte sind dabei zu beachten. Die Deutsche Gesellschaft für Datenschutz (DGD) unterstützt Unternehmen mit einem Daten-

schutzerklärung-Generator. Dieser generiert Ihnen über einen Fragebogen die für Ihr Unternehmen passende Datenschutzerklärung (www.dgd-datenschutz.de/muster/datenschutzerklaerung/).

Insbesondere müssen die Kontaktdaten des evtl. Datenschutzbeauftragten veröffentlicht werden.

Gerne unterstützen wir Sie bei der Erstellung der Datenschutzerklärung.

Information:
Der Inhalt dieser Information wurde nach bestem Wissen und Kenntnisstand erstellt. Mit Rücksicht auf die Komplexität der angesprochenen Themen und den ständigen Wandel der Rechtsmaterie bitten wir um Verständnis, wenn wir unsere Haftung und Gewährleistung auf Beratungen in individuellen Einzelaufträgen nach Maßgabe unserer Auftragsbedingungen beschränken und sie i. Ü., d. h. für diese Informationen ausschließen.