Cybersecurity
Progress. Protected.

Die Europäische Datenschutz-Grundverordnung

ESET Best Practise 2.0

Leitfaden für Unternehmen und Behörden



Progress. Protected.

ESET.DE | ESET.AT | ESET.CH

INHALTSVERZEICHNIS

Vorwort **3**

Überblick **4**

DSGVO für Spätstarter **7**

Die Antreiber 7

Informationspflichten 9

Datenschutzorganisation 13

DSGVO für Einsteiger **15**

Grundlagen 15

Folgende Grundsätze sind nach der DSGVO einzuhalten 15

Datenschutzbeauftragter 17

Verzeichnis von Verarbeitungstätigkeiten 19

Auftragsverarbeitung 21

Sicherheit der Verarbeitung 22

Meldepflichten 22

Betroffenenrechte 24

DSGVO für Fortgeschrittene **25**

Datenschutz-Folgenabschätzung 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen 25

Kontakt 25

Über ESET **26**

Cybersecurity
Progress. Protected.

VORWORT

Seit dem 25.05.2018 gilt die EU-Datenschutzgrundverordnung (DSGVO). In unseren Seminaren und bei Vorträgen lassen sich sehr unterschiedliche Beobachtungen zum Status der Umsetzung der DSGVO bei Unternehmen und Behörden machen. Einige Unternehmen sind sehr weit fortgeschritten und bemühen sich, die neuen gesetzlichen Regelungen anzuwenden. Nach unserer Wahrnehmung, die auch von verschiedenen Umfragen bestätigt wird, hat die überwiegende Anzahl von Unternehmen und Behörden die neuen gesetzlichen Regelungen allerdings nur in sehr geringem Umfang oder noch gar nicht umgesetzt.

Dies ist in Anbetracht der mit den Datenschutzverstößen verknüpften finanziellen Bedrohungen kein guter Weg, auch wenn immer wieder das Argument zu hören ist, dass letztendlich die drohenden Bußgelder doch nicht so hoch ausfallen werden oder das Argument zitiert wird, dass am Ende doch nicht so heiß gegessen wie gekocht wird.

Bemerkenswert ist auch die Rolle der Aufsichtsbehörden. Nachdem zwei Jahre lang die neuen gesetzlichen Regelungen schon bekannt waren, kamen erst in den letzten Wochen vor dem Inkrafttreten der DSGVO Hinweise der Aufsichtsbehörden. Hier konnte man sich des Eindrucks nicht erwehren, dass auch für die Aufsichtsbehörden die neuen gesetzlichen Regelungen in gewisser Weise überraschend kamen. Dies führt in der Praxis zu Anwendungsschwierigkeiten, da in vielen Einzelfragen und in der konkreten Anwendung der DSGVO wichtige praktische Hinweise der Aufsichtsbehörden dringend benötigt werden. Hier besteht die Hoffnung, dass in Zukunft eine deutlichere Positionierung der Aufsichtsbehörden erfolgt.

Im Gesetzgebungsverfahren und in den Diskussionen um die DSGVO kam die Frage auf, ob eine Selbstbestimmung über die eigenen Daten im digitalen Zeitalter noch möglich ist. Der politische Wille der Europäischen Union ist hier eindeutig. Alle Bürger sollen über ihre personenbezogenen Daten und deren Verarbeitung und Verwendung selber bestimmen.

Es bleibt spannend, ob dies tatsächlich noch möglich ist oder ob letztendlich die gelebte Praxis und der Umgang eines jeden Einzelnen mit den personenbezogenen Daten zu einer Aushöhlung oder gar Missachtung der neuen datenschutzrechtlichen Regelungen führt.

Thomas Feil
Fachanwalt für IT- und Arbeitsrecht und externer Datenschutzbeauftragter bei Unternehmen und Behörden

Michael Schröder
Manager of Security Business Strategy ESET Deutschland GmbH und Datenschutzbeauftragter (DSC Standard)

ÜBERBLICK

Mit der seit dem 25.05.2018 geltenden EU-Datenschutzgrundverordnung (DSGVO) gelten neue datenschutzrechtliche Regelungen. Das Gesetz wurde bereits am 25.05.2016 veröffentlicht und gilt sowohl für Unternehmen als auch für Behörden. Auf nationaler Ebene werden damit das bisher geltende Bundesdatenschutzgesetz (BDSG) und auch alle Landesdatenschutzgesetze abgelöst. In Österreich ist die DSGVO als europäisches Recht ebenfalls zu beachten. Schweizer Unternehmen, die mit anderen europäischen Ländern Leistungen austauschen, werden ebenfalls mit der DSGVO konfrontiert. Bei zukünftigen Fragen zum Datenschutz werden Anwender in Unternehmen und Behörden zuerst in die DSGVO schauen.

An vielen Stellen hat der europäische Gesetzgeber aber Öffnungsklauseln vorgesehen. Auf Basis dieser Öffnungsklauseln hat der nationale Gesetzgeber die Möglichkeit, eigene Regelungen zu schaffen. Aus diesem Grund hat der Bundestag mit Zustimmung des Bundesrates ein Gesetz zur Anpassung des Datenschutzrechtes an die EU-Gesetzgebung vorgesehen. Mit dem etwas sperrigen Titel „Datenschutz-Anpassungs- und Umsetzungsgesetz EU DSAnpUG-EU" hat der deutsche Gesetzgeber versucht, die entsprechenden Lücken auszufüllen. Das Datenschutz-Anpassungs- und Umsetzungsgesetz EU hat dabei drei Teile. Im ersten Teil sind die gemeinsamen Bestimmungen vorgesehen, im zweiten Teil die Durchführungsbestimmungen für die DSGVO und im dritten Teil wird eine Richtlinie umgesetzt, die datenschutzrechtliche Regelungen für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten und deren zuständige öffentliche Stellen vorsieht. Wichtig ist dabei in der Praxis, dass alle Regelungen nach § 45 bis § 48 BDSG neu, wie das Datenschutz-Anpassungs- und Umsetzungsgesetz EU abgekürzt genannt wird, nicht als Ergänzung zur DSGVO gelten, sondern einen eigenen Regelungsbereich betreffen. *Für Unternehmen und Behörden, die der DSGVO unterliegen, sind in Deutschland daher nur die §§ 1 bis 44 BDSG neu relevant.*

Nicht alle Bundesländer haben es geschafft, rechtzeitig zum 25.05.2018 für das Landesrecht datenschutzrechtliche Regelungen vorzusehen. Es ist aber davon auszugehen, dass zeitnah alle Bundesländer entsprechende Regelungen schaffen.

Die Rangfolge ist in der Rechtsanwendung allerdings von Bedeutung. *Die DSGVO ist höherrangiges Recht. Nationale Vorschriften, sei es im BDSG neu oder in Landesdatenschutzgesetzen, dürfen den Regelungen der DSGVO nicht widersprechen.* Gleiches gilt für nationale Regelungen in Österreich oder anderen europäischen Ländern. In diesem Zusammenhang gibt es bereits Diskussionen rund um die Neuregelung zur Videoüberwachung, die in § 4 BDSG neu vorgesehen ist. Die Datenschutzkonferenz, der Zusammenschluss der Bundes- und Landesdatenschutzbeauftragten, hält die Regelung in § 4 BDSG neu für europarechtswidrig und empfiehlt den Anwendern, nicht die vom Bundesgesetzgeber veröffentlichte Regelung anzuwenden. Hier gewinnt die Frage der Rangfolge und der Normenhierarchie praktische Bedeutung. *Da im Zweifel die Aufsichtsbehörden auch die zuständigen Stellen sind, die Bußgelder verhängen, empfehlen wir in der praktischen Anwendung, sich eher der Rechtsauffassung der Datenschutzkonferenz anzuschließen.*

Die Datenschutzgrundverordnung enthält am Beginn insgesamt 173 Erwägungsgründe. Hier ist der politische Wille für einzelne Regelungen und Artikel in der DSGVO festgehalten. Mittlerweile gibt es diverse Veröffentlichungen, die die Erwägungsgründe konkret verschiedenen Artikeln zuordnen.

In Kapitel 1, den Allgemeinen Bestimmungen, finden sich die Regelungen zum Anwendungsbereich der DSGVO und die Begriffsbestimmungen.

In Artikel 1 DSGVO sind der Gegenstand und die Ziele der DSGVO festgelegt. Dort heißt es in Abs. 1:

„Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten."

Hier wird das Spannungsfeld deutlich, in dem die DSGVO steht. Zum einen geht es um den Schutz der personenbezogenen Daten bei der Verarbeitung, zum anderen soll aber auch der freie Verkehr von Daten sichergestellt werden. Im Gesetzgebungsverfahren gab es eine schlagwortartige Formulierung mit dem Hinweis, dass Daten das neue Öl einer Informationsgesellschaft sind. Der europäische Gesetzgeber hat sich deutlich anders positioniert als beispielsweise die USA. Im Vordergrund der DSGVO steht der Schutz personenbezogener Daten. Im Zweifel wird diesem Schutz Priorität vor dem freien Verkehr von Daten gegeben. In den USA ist der politische Ansatz deutlich anders und setzt den Schwerpunkt auf den freien Verkehr der Daten. Langfristig ist sicherlich in globaler Hinsicht von Bedeutung, wie sich die asiatischen Staaten beim Datenschutz positionieren. Aktuell lässt sich aber beobachten, dass aufgrund des großen europäischen Marktes die neuen datenschutzrechtlichen Regelungen weltweit Wirkung entfalten.

Beim sachlichen Anwendungsbereich ist die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung von persönlichen oder familiären Tätigkeiten von der Anwendung der DSDGVO ausgenommen (Art. 2 Abs. 2 lit.c DSGVO). Beim räumlichen Anwendungsbereich sind zunächst alle Unternehmen und Behörden betroffen, die ihren Sitz in der Europäischen Union haben. *Daneben sieht Art. 3 Abs. 2 DSGVO vor, dass bei der Verarbeitung personenbezogener Daten von in der EU aufhältigen Personen ebenfalls eine Anwendung der DSGVO erfolgt, wenn betroffenen Personen in der EU Waren oder Dienstleistungen angeboten werden oder wenn das Verhalten betroffener Personen beobachtet wird, die sich in der EU aufhalten.* Dies führt zu einem sehr weiten Anwendungsbereich der DSGVO und trifft beispielsweise alle Handy-Apps, die im europäischen Markt angeboten werden oder auch alle Internetseiten, die beispielsweise Waren und Dienstleistungen im europäischen Markt anbieten.

Auf der Internetseite www.dsgvo-gesetz.de finden sich die Regelungen der europäischen Verordnung, die jeweils passenden Erwägungsgründe und zugeordnet auch der passende Paragraf des BDSG neu.

Praxistipp

Bei den Begriffsbestimmungen in Art. 4 sind zwei Definitionen zunächst herauszugreifen. In Art. 4 Ziff. 1 DSGVO ist der Begriff „personenbezogene Daten" definiert. Dabei werden als personenbezogene Daten alle Informationen gesehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Bei der Frage, wann eine Person identifizierbar ist, wird auf direkte oder indirekte Möglichkeiten der Zuordnung zu einer Kennung, wie einem Namen, einer Kennnummer oder Standortdaten, abgestellt. Weitere Aspekte können zur Identifikation hinzugenommen werden. Insgesamt ist, auch mit Blick auf die europäische Rechtsprechung, die beispielsweise IP-Adressen als personenbezogene Daten sieht, von einem weiten Anwendungsbereich auszugehen. *Nach unseren Beobachtungen durchziehen personenbezogene Daten die meisten Bereiche eines Unternehmens und fast alle Bereiche einer Behörde.* Bei Behörden wird in fast jedem Kontext mit Bürgerdaten oder Daten von Mitarbeitern hantiert. Aus datenschutzrechtlicher Sicht ist dabei nicht von Bedeutung, ob es um wenige oder viele Daten geht. *Die DSGVO sieht keine Mindestmenge vor, ab der es zu einer Anwendung der neuen datenschutzrechtlichen Regelungen kommt. Bereits kleinste Datenmengen und Datensammlungen führen zu einer Anwendung der DSGVO.*

Die zweite Begriffsbestimmung, die, abweichend von der bisherigen deutschen Rechtslage, neue Aspekte aufruft, ist die Definition der „Verarbeitung" in Art. 4 Ziff. 2 DSGVO. Die DSGVO geht von einem umfassenden Verarbeitungsbegriff aus. *Eine Verarbeitung ist nicht nur die konkrete Nutzung, das Erheben, das Erfassen oder die Organisation und Ordnung von personenbezogenen Daten. Auch die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung sowie das Löschen und die Vernichtung sind eine Verarbeitung.* Auch hier gibt es die politische Zielrichtung, möglichst alle Verwendungen und Verwendungsarten von personenbezogenen Daten der DSGVO zuzuordnen. In der praktischen Umsetzung führt jede Nutzung von personenbezogenen Daten durch die Informationstechnologie und die EDV zu einer Verarbeitung. *Auch die strukturierte Datenverarbeitung in Papierform unterliegt der DSGVO.*

Eine Verarbeitung ist nicht nur die konkrete Nutzung, das Erheben, das Erfassen oder die Organisation und Ordnung von perso-nenbezogenen Daten.

Auszug

DSGVO FÜR SPÄTSTARTER

Die Antreiber

Wer bisher keine Umsetzungsmaßnahmen oder nur erste kleine Schritte in Richtung Umsetzung DSGVO unternommen hat, für den- oder diejenige sind die nachfolgenden Hinweise vorgesehen. *In diesem Abschnitt soll vorgestellt werden, warum die DSGVO zu beachten ist und welche Sofortmaßnahmen notwendig sind, um rechtliche und wirtschaftliche Risiken aus der Anwendung der neuen Datenschutzregelungen zu vermeiden.*

Der erste Antreiber für die Umsetzung der DSGVO sind die in Art. 83 festgelegten Geldbußen. *Dabei fordert der Gesetzgeber in Art. 83 Abs. 1 DSGVO, dass Geldbußen zukünftig wirksam, verhältnismäßig und abschreckend sein sollen.* Die Formulierung „abschreckend" ist in Zusammenhang mit Geldbußen ungewöhnlich. Vermutlich hätte es einen Aufschrei gegeben, wenn beispielsweise der Begriff „abschreckend" in Zusammenhang mit Bußgeldern nach dem Straßenverkehrsrecht vom Gesetzgeber formuliert worden wäre. Hier wird deutlich, dass der europäische Gesetzgeber mit der bisherigen Bußgeldpraxis der Aufsichtsbehörden unzufrieden ist und eine erhebliche Änderung fordert.

Daneben ist der Bußgeldrahmen in Art. 83 Abs. 4 und Art. 83 Abs. 5 DSGVO deutlich geändert worden. Bei Verstößen gegen die Bestimmungen der DSGVO können Geldbußen von bis zu 10 Mio. oder 20 Mio. Euro festgesetzt werden. *Im Falle eines Unternehmens sind auch Geldbußen von bis zu 2 % oder 4 % des gesamten weltweit erzielten Jahresumsatzes möglich. Dies ist der Bußgeldrahmen und es ist nicht zu erwarten, dass die Aufsichtsbehörden gleich am Beginn entsprechend hohe Bußgelder festsetzen werden.* Die Kombination des relativ weiten Bußgeldrahmens mit der Forderung nach abschreckenden Bußgeldern macht aber deutlich, dass entgegen der bisher üblichen Praxis mit mehr Bußgeldern zu rechnen ist und auch mit deutlich höheren Geldbußen als bisher.

Ohne anderweitige nationale Regelungen gelten die Bußgeldvorschriften auch für Behörden. Art. 83 Abs. 7 DSGVO sieht aber vor, dass der nationale Gesetzgeber für Behörden Ausnahmeregelungen bei den Geldbußen festlegen kann. Davon hat der Bundesgesetzgeber im BDSG neu Gebrauch gemacht. Gem. § 43 Abs. 3 BDSG neu sollen gegen Behörden und sonstige öffentliche Stellen keine Geldbußen verhängt werden. Öffentliche Stellen sind beispielsweise auch bundesunmittelbare Körperschaften oder Anstalten sowie Stiftungen des öffentlichen Rechts. Eine weitergehende Begriffsbestimmung erfolgt in § 2 Abs. 1 BDSG neu. Entsprechende Ausnahmeregelungen für die Verhängung von Bußgeldern gegen Behörden und sonstige öffentliche Stellen müssen Landesgesetze vorsehen, um die Landesverwaltung und die Kommunen aus dem Anwendungsbereich der DSGVO herauszunehmen. *Gibt es entsprechende Regelungen nicht oder werden diese verspätet eingeführt, ist bis zum Inkrafttreten einer entsprechenden Ausnahmeregelung die DSGVO mit der Bedrohung der abschreckenden Bußgelder auch auf Landesbehörden und Kommunen anwendbar.*

Unsere Beobachtung in Seminaren und Vorträgen ist aber, dass eine gewisse Lethargie in Anbetracht der hohen und abschreckenden Bußgelder eintritt. Vielfach hören wir das Argument von Unternehmensseite, dass bei Bußgeldern in Millionenhöhe eine so starke wirtschaftliche Bedrohung eintritt, dass das Unternehmen im Zweifel geschlossen werden muss. *Diese Argumentation ist nach unserer Einschätzung zu kurzsichtig. Geldbußen müssen immer verhältnismäßig sein, also auch zur wirtschaftlichen Tätigkeit des jeweiligen Unternehmens passen. Ein kleiner Handwerksbetrieb wird sicherlich keine Geldbuße in Höhe von 1 Mio. Euro erhalten.* Wichtig ist aus unserer Sicht für die aktuelle Anwendung der datenschutzrechtlichen Regelung, dass anders als bisher nicht grundsätzlich davon ausgegangen werden kann, bei Datenschutzverstößen gäbe es keine oder nur sehr geringe Bußgelder. *Die bisher vielfach anzutreffende Argumentation, dass es billiger sei, ein Bußgeld in Kauf zu nehmen, als Datenschutz tatsächlich im Unternehmen umzusetzen, verliert damit an Berechtigung.*

Der zweite Antreiber ist vermutlich in der Zukunft von erheblich größerer Bedeutung. *In Art. 82 Abs. 1 DSGVO ist festgelegt, dass bei Verstößen gegen die Verordnung nicht nur ein materieller Schadenersatzanspruch besteht, sondern auch ein immaterieller Schaden geltend gemacht werden kann.* Dass Datenschutzverstöße zu einem Schmerzensgeldanspruch führen, ist neu. Nicht festgelegt ist, in welcher Höhe ein Schmerzensgeld festzusetzen ist. Hier gibt es allerdings im Hintergrund eine Rechtsprechung des Europäischen Gerichtshofs, der bei Schmerzensgeldfestsetzungen die Forderung aufstellt, dass die Höhe des Schmerzensgelds europäischen rechtlichen Regelungen auch zur Durchsetzung helfen soll. Damit entfallen Schmerzensgeldansprüche im niedrigschwelligen Bereich, die faktisch für Unternehmen und Behörden keine Auswirkung haben. Die Regelungen in Art. 82 Abs. 1 DSGVO gelten sowohl für Unternehmen als auch für Behörden. *Anders als bei den Geldbußen ist eine Ausnahmeregelung beim Schmerzensgeldanspruch für Behörden nicht gesetzlich gestattet.*

Vermutlich wird in Zukunft nicht der Einzelfall einer Schmerzensgeldforderung die wirtschaftliche Bedrohung sein. *Wenn allerdings in gleich gelagerten Fällen hundertfach oder tausendfach Schmerzensgeldansprüche geltend gemacht werden, entsteht dadurch durchaus eine wirtschaftliche Bedrohung.* Hier ist unsere Erwartung, dass datenschutzrechtliche Ansprüche zusätzlich zu anderen Forderungen ergänzend geltend gemacht werden. Hier muss man sich nur einmal vorstellen, welche wirtschaftlichen Auswirkungen ein durchsetzbarer Schmerzensgeldanspruch in Höhe von 500 Euro hat, wenn jeder durch die Diesel-Skandale geschädigte Autofahrer eine solche Forderung gegen den jeweiligen Autohersteller durchsetzen könnte.

Im Moment ist noch nicht abzusehen, in welcher Höhe die Gerichte einen immateriellen Schaden sehen und welches Schmerzensgeld letztendlich festgesetzt wird. Es ist aber zu erwarten, dass zeitnah im Zuge von rechtlichen Auseinandersetzungen das Thema „Schmerzensgeld" aufgrund von Datenschutzverstößen eine wirtschaftliche Bedeutung gewinnt und Unternehmen und Behörden sich mit solchen Forderungen auseinandersetzen müssen.

Der dritte Antreiber ergibt sich aus einem anderen Zusammenhang. Dieser Antreiber für die Umsetzung und Anwendung der DSGVO basiert nicht auf negativen finanziellen und wirtschaftlichen Folgen, sondern setzt bei Rechtspflichten an, die Personen auferlegt werden. *Gem. Art. 39 Abs. 1 lit. b DSGVO hat der Datenschutzbeauftragte eine gesetzliche Überwachungspflicht hinsichtlich der Einhaltung der Europäischen Datenschutznormen.* Für externe Datenschutzbeauftragte ergeben sich dadurch erhebliche Haftungsrisiken. Aber auch für angestellte Datenschutzbeauftragte verändert sich deutlich das Risiko, wegen Datenschutzverstößen in Haftung genommen zu werden. Im Rahmen der Arbeitnehmerhaftung kann eine Mitarbeiterin oder ein Mitarbeiter dann zur Rechenschaft gezogen werden, wenn ein Fall der groben Fahrlässigkeit vorliegt. Eine grobe Fahrlässigkeit liegt beispielsweise vor, wenn ein Datenschutzbeauftragter bestimmte Bereiche des Unternehmens oder einer Behörde datenschutzrechtlich nicht prüft und überwacht.

Die in der DSGVO festgelegten Pflichten bleiben unabhängig davon bestehen, ob nach den gesetzlichen Regelungen ein Datenschutzbeauftragter bestellt werden muss. Auch ohne Datenschutzbeauftragten bedarf es einer klaren Zuordnung der Verantwortlichkeiten für die Umsetzung der gesetzlichen Anforderungen zum Datenschutz.

Informationspflichten

Als Erstes sollte ein Unternehmen oder eine Behörde bei der Umsetzung der DSGVO die Bereiche bearbeiten, die von außen wahrgenommen werden. Es gibt einige Aspekte der DSGVO, bei denen sofort von außen erkennbar ist, ob Unternehmen oder Behörden Maßnahmen ergriffen haben, um die neuen datenschutzrechtlichen Regelungen anzuwenden.

Der europäische Gesetzgeber ändert mit der DSGVO ein Grundprinzip im Datenschutz. Bisher war es auf Basis der gesetzlichen Regelungen möglich, durch die Geltendmachung von Auskunftsansprüchen in Erfahrung zu bringen, wer welche personenbezogenen Daten eines Bürgers speichert und verarbeitet. Hier ist zukünftige Erwartungshaltung des europäischen Gesetzgebers, dass jede Stelle, sei es Unternehmen oder Behörde, unabhängig ob groß oder klein, den Betroffenen informiert, dessen personenbezogenen Daten verarbeitet werden.

Dies ist aus Sicht des Gesetzgebers der wesentliche Beitrag zur Umsetzung der gewünschten Selbstbestimmung über die Verwendung der personenbezogenen Daten.

Nach unserer Wahrnehmung ist dieser Aspekt leider erst sehr spät in das Bewusstsein der Unternehmen und Behörden gekommen. Vielfach sind die gesetzlich festgelegten Informationspflichten nach wie vor nicht im Fokus bei der Anwendung der DSGVO. *Dass es dem Gesetzgeber dabei durchaus sehr ernst ist, ergibt sich auch aus dem Umstand, dass die Umsetzung der Informationspflichten der zweiten Bußgeldstufe, sprich Geldbußen von bis zu 20 Mio. Euro oder 4 % des gesamten weltweit erzielten Jahresumsatzes, zugeordnet wird.* Aus dieser Klassifizierung ergibt sich deutlich, welche rechtlichen Regelungen dem Gesetzgeber besonders wichtig sind.

Nach Art. 12 Abs. 1 DSGVO soll der Verantwortliche, sprich das Unternehmen oder die Behörde, betroffenen Personen alle Informationen gem. Art. 13 und 14 DSGVO geben, damit diese über die Verwendung ihrer personenbezogenen Daten informiert sind. *Dabei stellt der Gesetzgeber die Forderung auf, dass eine solche Information in präziser, transparenter, verständlicher und leicht zugänglicher Form erfolgen soll und dabei eine klare und einfache Sprache verwendet werden soll.* Ein Unternehmen oder eine Behörde soll sich nicht durch komplizierte juristische Formulierungen oder durch versteckte Datenschutzhinweise der Verantwortung entziehen. „Transparente Informationen" sind eine der zentralen Forderungen der DSGVO.

Werden personenbezogene Daten, beispielsweise der Name eines Ansprechpartners, in ein Warenwirtschaftssystem oder ein CRM-System eingegeben, löst dies Informationspflichten aus. Der Betroffene, sprich der Ansprechpartner, muss dann über die Datenverarbeitung mit den gesetzlich festgelegten Einzelheiten informiert werden.

Praxistipp

Konkret sieht Art. 13 DSGVO verschiedene Einzelinformationen vor, die dem Betroffenen mitzuteilen sind. Dabei verweist Art. 13 DSGVO auf die direkte Erhebung bei einer betroffenen Person. Dies kann beispielsweise durch die Verarbeitung einer E-Mail durch die Software des Verantwortlichen erfolgen. Werden also personenbezogene Daten bei der betroffenen Person erhoben, so soll der Verantwortliche zum Zeitpunkt der Erhebung dieser Daten seinen Informationspflichten nachkommen. Der Begriff „Datenerhebung" ist nicht weiter definiert. In den juristischen Kommentierungen wird darauf abgestellt, dass eine Datenerhebung den Beginn eines Datenverarbeitungsprozesses darstellt. Mit der Datenerhebung wird erstmals zielgerichtet auf personenbezogene Daten zugegriffen, um diese weiterzuverarbeiten. Dies kann beispielsweise auch durch eine Löschung geschehen.

Die Informationspflichten gliedern sich in statische Informationen, die in allen Fällen gleich sind, und variable Informationen. Zu den statischen Informationen gehören beispielsweise der Name und die Kontaktdaten des Verantwortlichen und seines Vertreters sowie die Kontaktdaten des Datenschutzbeauftragten. *Weiterhin ist darüber zu belehren, dass es ein Recht auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie ein Recht auf Berichtigung und Löschung gibt.* Es soll auf ein Beschwerderecht bei der Aufsichtsbehörde hingewiesen werden, und für alle Inkassodienstleister von besonderer Bedeutung ist die Forderung, dass aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und angestrebte Auswirkungen von Datenverarbeitungen bereitgestellt werden sollen. Hier empfiehlt sich in der Praxis, dass eine Musterinformation erstellt wird, die für alle Fälle der Datenverarbeitung in einem Unternehmen oder Behörden diese statischen Informationspflichten entsprechend den Anforderungen des Art. 13 DSGVO genau umsetzt.

Daneben gibt es variable Bestandteile einer Information nach Art. 13 DSGVO. *Gem. Art. 13 Abs. 1 lit. c DSGVO soll dem Betroffenen mitgeteilt werden, für welche Zwecke die personenbezogenen Daten verarbeitet werden und auf Basis welcher Rechtsgrundlage die Verarbeitung erfolgt.* Auch sollen die Empfänger oder Kategorien von Empfängern mitgeteilt werden (Art. 13 Abs. 1 lit. e DSGVO). Gem. Art. 13 Abs. 2 lit. a DSGVO ist daneben über die Dauer, für die die personenbezogenen Daten gespeichert werden, oder ggf. die Kriterien für die Festlegung der Dauer zu informieren.

Diskutiert wird aktuell, in welchem Detaillierungsgrad eine entsprechende Information erfolgen soll. Genügt es beispielsweise, für die Angabe der Rechtsgrundlage anzugeben, welche genaue rechtliche Regelung nach Art. 6 Abs. 1 DSGVO gilt? In Art. 6 Abs. 1 DSGVO ist im Einzelnen dargelegt, wann eine Verarbeitung von personenbezogenen Daten rechtmäßig ist. Genügt es also, die europäischen Regelungen der DSGVO lediglich zu zitieren oder wörtlich wiederzugeben? Teilweise wird die Auffassung vertreten, dass eine betroffene Person damit keine Möglichkeit hat, ihre rechtliche Position gegenüber der Datenverarbeitung einzuschätzen. *Die Erlaubnistatbestände in Art. 6 Abs. 1 DSGVO sind sehr offen formuliert. Um die Informationspflicht korrekt umzusetzen, wird gefordert, einzelfallbezogen und vollständig die jeweilige Rechtslage darzulegen. Der Verantwortliche soll die Rechtsgrundlage so erläutern, dass die betroffene Person deren Anwendung nachvollziehen kann.* Hierzu haben sich bisher die Aufsichtsbehörden nicht deutlich positioniert. Es bleibt also abzuwarten, mit welchem Detaillierungsgrad die Rechtsgrundlage anzugeben ist. Im ersten Schritt genügt vermutlich erst einmal der Verweis auf Art. 6 Abs. 1 DSGVO. Die zukünftigen rechtlichen Diskussionen werden hoffentlich an dieser Stelle Klarheit bringen.

Eine Behörde oder ein Unternehmen erhält eine Bewerbung. Dann ist „zum Zeitpunkt der Erhebung" dem Bewerber eine Information gem. Art. 13 DSGVO zu übermitteln. Dies unabhängig von der weiteren Bearbeitung der Bewerbung. Hier empfehlen wir, beispielsweise bei auf den Webseiten veröffentlichten E-Mail-Adressen für Bewerbungen sicherzustellen, dass sehr kurzfristig, möglichst innerhalb eines Tages, eine erste Antwort und Rückmeldung dem Bewerber übermittelt wird. Andernfalls besteht die Gefahr, dass Bewerber, die abgelehnt werden, im Nachgang nicht nur Forderungen nach dem AGG, sondern auch Forderungen wegen Datenschutzverstößen und Schmerzensgeldansprüchen geltend machen.

Praxistipp

Auch bei der Speicherdauer genügt nicht ein pauschaler Hinweis, dass die gesetzlichen Regelungen über die Speicherung und Archivierung eingehalten werden. Die Information soll gem. Art. 12 DSGVO vollständig und präzise sein. Insoweit bedarf es einer konkreten Angabe und beispielsweise dem Hinweis, nach wie vielen Monaten oder Jahren personenbezogene Daten gelöscht werden.

In der praktischen Anwendung dieser gesetzlichen Vorschrift ergeben sich nach unserer Erfahrung vielfältige Diskussionen, da bei Unternehmen und Behörden abschließend festgelegt werden muss, wann beispielsweise personenbezogene Daten gelöscht werden müssen oder können. Eine konkrete Festlegung mit Blick auf den Zweck der Verarbeitung und den gesetzlichen Anforderungen ist häufig nicht einfach.

Es ergibt sich in der Praxis sowohl für Unternehmen als auch für Behörden eine besondere finanzielle und wirtschaftliche Bedrohung. *Eine fehlende Information oder auch beispielsweise eine fehlerhafte Festlegung der Speicherdauer kann bei den Betroffenen Schmerzensgeldansprüche auslösen.* Es wäre also durchaus denkbar, dass bei einem E-Mail-Versand an eine Behörde oder ein Unternehmen im Nachgang eine Schmerzensgeldforderung aufgestellt wird, wenn nicht „zum Zeitpunkt der Erhebung" eine Information über die Rechtsgrundlage, den Empfänger der Daten oder die Speicherdauer übermittelt wird. Hierbei ist noch unklar, welcher Zeitrahmen mit der Formulierung „zum Zeitpunkt der Erhebung" gemeint ist. Allerdings ist davon auszugehen, dass ein wochenlanges Warten mit der Informationspflicht nicht im Sinne des Gesetzes ist.

Art. 13 DSGVO sieht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person nur eine einzige Ausnahme in Art. 13 Abs. 4 DSGVO vor. Nur wenn die betroffene Person bereits über die entsprechende Informationen verfügt, muss keine erneute Information erfolgen. Andere Argumente, wie beispielsweise der Verweis auf einen unverhältnismäßigen Aufwand oder andere Arten der technischen oder organisatorischen Unmöglichkeit, sind bei Art. 13 DSGVO unbeachtlich. Die Erwartungshaltung des Gesetzgebers ist, dass alle Behörden und Unternehmen diese Informationspflicht einhalten und umsetzen. *Die Informationspflicht nach Art. 13 DSGVO gilt im Übrigen auch für die Kommunikation per Brief oder Telefon.*

Art. 13 DSGVO führt auch dazu, dass alle Datenschutzhinweise auf den Internetseiten zu ändern sind. *Auch hier gilt das Prinzip, dass die Rechtsgrundlage der Verarbeitung und beispielsweise die Speicherdauer von IP-Adressen genannt werden muss. Werden Daten beispielsweise an Analyse-Tools weitergegeben, ist darüber ebenfalls zu informieren.*

Seit dem 25.05.2018 ist also anhand der Datenschutzhinweise auf der Internetseite und auch anhand der Umsetzung der Informationspflichten bei der E-Mail-Kommunikation sehr schnell festzustellen, ob ein Unternehmen oder eine Behörde die Anforderungen der Datenschutz-Grundverordnung umgesetzt hat. *Noch einmal ist zu betonen, dass eine unvollständige oder fehlerhafte Umsetzung der Informationspflichten nach Art. 13 DSGVO sowohl ein abschreckendes Bußgeld nach sich ziehen kann als auch Schmerzensgeldansprüche der betroffenen Personen auslösen können.*

Neben den Informationspflichten nach Art. 13 DSGVO sieht Art. 14 DSGVO auch eine Informationspflicht vor, wenn personenbezogene Daten nicht bei der betroffenen Person erhoben werden. *Erhalten Unternehmen und Behörden beispielsweise im Rahmen von kaufmännischen oder technischen Abwicklungen Daten Dritter, bestehen grundsätzlich ebenfalls die Informationspflichten.* Der Ausnahmekatalog ist allerdings in Art. 14 Abs. 5 DSGVO deutlich weiter gefasst. Die verantwortliche Stelle, die personenbezogene Daten vermittelt erhält, muss nicht informieren, wenn die betroffene Person bereits über die Information verfügt. Auch besteht nach Art. 14 Abs. 5 lit. b DSGVO keine Informationspflicht, wenn sich die Erteilung der Information als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordert. Hier ist allerdings mit einer gewissen Vorsicht diese Ausnahmeregelung anzuwenden. Eine fehlerhafte Interpretation oder zu weite Auslegung dieser Ausnahmenvorschrift löst ebenfalls einen Bußgeldtatbestand der zweiten Bußgeldstufe und ggf. einen Schmerzensgeldanspruch aus. *Daher empfehlen wir in der Praxis eine gewisse Zurückhaltung bei der Anwendung der entsprechenden Ausnahmenregelung.*

Wenn nicht sichergestellt werden kann, dass der „Erstverarbeiter" der personenbezogenen Daten seinen Pflichten nach Art. 13 DSGVO nachgekommen ist, bleibt dem „Zweitverarbeiter" nichts anderes übrig, als selber die Informationspflichten umzusetzen. Der Inhalt der Informationspflichten ähnelt in Art. 14 DSGVO weitestgehend den Anforderungen in Art. 13 DSGVO. Ergänzend kommt die Information über die Kategorien der personenbezogenen Daten, die verarbeitet werden, hinzu. *Bei der Ersterhebung weiß der Betroffene, welche personenbezogenen Daten er übermittelt hat. Dies ist bei der Weitergabe von personenbezogenen Daten so nicht mehr sichergestellt. Daher muss hier auch über die Kategorien der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, informiert werden.* Es wird nicht gefordert, dass die einzelnen Daten oder Datensätze genannt werden. Bewusst fordert der Gesetzgeber ausschließlich die Angabe der „Kategorien".

Die Umsetzung der Informationspflichten sollte für alle Unternehmen und Behörden, die bisher noch keine Maßnahmen oder nur wenige Schritte in Richtung DSGVO unternommen haben, allererste Aufgabe sein. Viele andere Forderungen der DSGVO, die ebenfalls umgesetzt werden müssen, sind von außen nicht zu ersehen. Hier können Mitbewerber, die datenschutzrechtliche Abmahnungen beabsichtigen, oder Betroffene nicht erkennen, welchen Status die Umsetzung der Datenschutzregelungen hat. Bei den Informationspflichten ist dies sofort auf der Internetseite oder beispielsweise im Rahmen der E-Mail-Kommunikation zu erkennen. Wir empfehlen Sofortmaßnahmen, um eine transparente Information der betroffenen Personen zu erreichen.

Wir empfehlen allen Unternehmen und Behörden, in die E-Mail-Signatur einen entsprechenden Hinweis auf die Umsetzung der Informationspflicht nach Art. 13 DSGVO mit aufzunehmen. Es kann beispielsweise auf der Unternehmens- oder Behördenwebsite eine Unterseite eingerichtet werden, die die variablen und statischen Informationen nach Art. 13 DSGVO veröffentlicht. Mit einem entsprechenden Link erhält dann jeder Empfänger einer E-Mail eine transparente und leicht zugängliche Möglichkeit, sich zu informieren. Alternativ kann auch eine entsprechende Information beispielsweise bei Onlineshops im Rahmen der Neukundenregistrierung per E-Mail als PDF-Anhang übermittelt werden. Hier ist eine gewisse Kreativität in der organisatorischen Abwicklung notwendig. Wir haben die Erfahrung gemacht, dass Organisationsabläufe, die nicht individuell bearbeitet werden müssen, eine Umsetzung der gesetzlichen Anforderungen am besten sicherstellen.

Praxistipp

Datenschutzorganisation

Wenn die Informationspflichten im Rahmen des Projekts „DSGVO für Spätstarter" ausreichend umgesetzt wurden, sollte kurzfristig eine Datenschutzorganisation eingerichtet werden. Es gibt weitere vielfältige Anforderungen, die nachfolgend in den Kapiteln „DSGVO für Einsteiger" bzw. „DSGVO für Fortgeschrittene" näher beschrieben werden. Nach unserer Erfahrung kann dies nicht „nebenbei" von jemandem erledigt werden, sondern es sind bestimmte organisatorische Rahmenbedingungen zu schaffen. Die Mitarbeiterinnen und Mitarbeiter, die sich um das Thema „Datenschutz" kümmern sollen, brauchen ausreichende zeitliche und teilweise auch finanzielle Ressourcen, beispielsweise für Fortbildungen. Es ist die Entscheidung zu treffen, ob ein Datenschutzbeauftragter zu bestellen ist, und wenn ja, ob eine interne Lösung gesucht wird oder auch mit Blick auf die Haftungsrisiken ein externer Datenschutzbeauftragter bestellt werden soll. *Die datenschutzrechtlichen Pflichten, beispielsweise das Führen eines Verzeichnisses der Verarbeitungstätigkeit nach Art. 30 DSGVO oder die Umsetzung der Anforderungen für die Sicherheit der Verarbeitung gem. Art. 32 DSGVO sind aber unabhängig von der Bestellung eines Datenschutzbeauftragten.* Auch wenn der Schwellenwert zur Bestellung eines Datenschutzbeauftragten nicht überschritten wird, sind die entsprechenden gesetzlichen Anforderungen im Unternehmen oder in der Behörde anzuwenden. *Daher darf die Bestellung eines Datenschutzbeauftragten nicht darüber hinwegtäuschen, dass eine Datenschutzorganisation, sprich insbesondere eine Zuordnung von Zuständigkeiten und Aufgaben festgelegt werden muss.*

Da die DSGVO vielfältige Regelungen und Anforderungen an die IT-Sicherheit stellt, beispielsweise eine Erwartungshaltung der Verschlüsselung von personenbezogenen Daten deutlich im Gesetz formuliert, sind auch die Arbeitsbereiche und Verantwortlichkeiten des Datenschutzbeauftragten und des IT-Sicherheitsbeauftragten deutlich voneinander abzugrenzen und aufeinander abzustimmen. Hier sollten ein IT-Sicherheitsbeauftragter und der Datenschutzbeauftragte Hand in Hand arbeiten und insbesondere die Anforderungen des Art. 32 DSGVO umsetzen. Gerade mit Blick auf die Dokumentationspflichten in beiden Bereichen empfiehlt sich eine enge Verzahnung, um Doppelarbeiten und Reibungsverluste zu vermeiden.

Art. 32 DSGVO fordert eine Festlegung von Schutzzielen für die jeweiligen Datenverarbeitungen. Ausdrücklich wird als zentrale Maßnahme die Verschlüsselung personenbezogener Daten gefordert. Unternehmen und Behörden müssen dazu beispielsweise Festplatten und USB-Medien nachweislich verschlüsseln, um den Sicherheitsanforderungen der DSGVO Genüge zu tun. Nachweislich muss ein Unternehmen und eine Behörde auch sicherstellen, dass die Integrität der Daten gewahrt ist. Dies kann beispielsweise durch eine Zwei-Faktor-Authentifizierung der Mitarbeiter Zugänge oder privilegierte Logins erfolgen.

Weiterhin ist eine deutliche Positionierung der Leitungsebene mit Blick auf den Datenschutz notwendig. *Es sollte aus Sicht der jeweiligen Leitungsebenen deutlich gemacht werden, dass Datenschutz tatsächlich umzusetzen ist und die gesetzlichen Regelungen zu beachten sind.* Die Wahrnehmung von Mitarbeiterinnen und Mitarbeitern, dass eine Unternehmens- oder Behördenleitung kein Interesse an dem Thema „Datenschutz" hat oder selber die datenschutzrechtlichen Anforderungen ignoriert, ist in Anbetracht der zuvor beschriebenen Antreiber keine gute Idee.

Auch der Bereich des Risikomanagements und der internen Kontrollsysteme hinsichtlich der Risiken wird zukünftig das Thema „Datenschutz" mehr im Fokus haben. In Anbetracht der Bußgeldbedrohungen ist ein entsprechendes Risiko im Unternehmen zu bewerten. *Wir erwarten darüber hinaus, dass in Zukunft Rechnungshöfe, Wirtschaftsprüfer und auch die Banken zunehmend eine Dokumentation des Themas „Datenschutz" fordern.* Hier lässt sich häufig anhand der Dokumentationen schon erkennen, inwieweit ein Unternehmen die gesetzlichen Anforderungen ernst nimmt und darüber hinaus, wie es um das Thema „IT-Sicherheit" besteht. Unternehmen und Behörden, die IT-Sicherheit nicht ernst nehmen, gefährden die eigene wirtschaftliche und organisatorische Basis. *Dass Rechnungshöfe, Wirtschaftsprüfer und Banken dies zunehmend kritisch sehen, deutet sich bereits bei ersten Veröffentlichungen neuer Anforderungen an.* Auch Cyber-Versicherungen formulieren Anforderungen an die Datenschutzdokumentation für die Berechnung der Versicherungsprämien.

DSGVO FÜR EINSTEIGER

Grundlagen

Wenn personenbezogene Daten verarbeitet werden, ist seit dem 25.05.2018 die DSGVO zu beachten. Für eine rechtmäßige Datenverarbeitung formuliert die DSGVO verschiedene Anforderungen. Es wird dabei zwischen „normalen" personenbezogenen Daten und besonderen Kategorien personenbezogener Daten differenziert. Für „normale" personenbezogene Daten erwartet die DSGVO von dem Verantwortlichen, sprich von dem Unternehmen oder der öffentlichen Einrichtung, dass die in Art. 5 formulierten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. Dabei stellt das Gesetz in Art. 5 Abs. 2 klar, dass der Verantwortliche für die Einhaltung dieser Grundsätze verantwortlich ist und deren Einhaltung nachweisen können muss. Unter den Grundsatz „Rechenschaftspflicht" führt dies praktisch für alle Verantwortlichen zu einer neuen Situation. Bisher musste im Rahmen einer aufsichtsrechtlichen Überprüfung die Aufsichtsbehörde nachweisen, dass ein Verstoß gegen die datenschutzrechtlichen Vorschriften vorliegt. *Nunmehr muss entsprechend der gesetzlich formulierten Rechenschaftspflicht der Verantwortliche die Einhaltung nachweisen.* Dies erfordert eine erheblich bessere Dokumentation, als dies vielfach bisher zu finden ist. Die Nichteinhaltung der verschiedenen Grundsätze aus Art. 5 ist ein Bußgeldtatbestand. Insoweit erweitert das neue Datenschutzrecht die bisherigen Dokumentationspflichten und wird in der Praxis dazu führen, dass datenschutzrechtliche Maßnahmen und Überprüfungen genauer intern erfasst werden.

Folgende Grundsätze sind nach der DSGVO einzuhalten:

- Grundsatz der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben und der Transparenz
- Grundsatz der Zweckbindung
- Grundsatz der Datenminimierung
- Grundsatz der Richtigkeit
- Grundsatz der Integrität und
- Vertraulichkeit

In den Grundsätzen finden sich die bereits zuvor beschriebenen Informationspflichten wieder. Mit dem *Grundsatz der Transparenz* wird erwartet, dass personenbezogene Daten in einer für die betroffenen Personen nachvollziehbaren Weise verarbeitet werden. Überraschend ist auch der *Grundsatz der Richtigkeit*, der nunmehr eine Überprüfung der sachlichen Richtigkeit von Daten erwartet. Dies ist beispielsweise für Inkassounternehmen oder die Schufa eine nicht unerhebliche Herausforderung, gilt aber auch für alle Unternehmen und öffentliche Einrichtungen. Es sollen angemessene Maßnahmen getroffen werden, damit unrichtige Daten gelöscht oder berichtigt werden.

Vielfach finden sich in Unternehmen und in der öffentlichen Verwaltung noch „alte Programme" und Fachanwendungen, die keine Löschungsmöglichkeiten von personenbezogenen Daten vorsehen. Eine solche Situation verstößt gegen Art. 5 Abs. 1 lit. e DSGVO. Hier wird gesetzlich eine Speicherbegrenzung formuliert. Personenbezogene Daten dürfen nur solange gespeichert werden, wie dies für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Das heißt im Umkehrschluss, dass auf jeden Fall eine Löschung erfolgen muss. Software, die keine Löschung ermöglicht, ist zu ergänzen oder auszutauschen. Ein Verstoß gegen den *Grundsatz der Speicherbegrenzung* ist ebenfalls ein Bußgeldtatbestand und kann zu Schmerzensgeldansprüchen eines Betroffenen führen.

Neben den Grundsätzen ist in einer zweiten Stufe zu prüfen, ob nach Art. 6 DSGVO eine Rechtmäßigkeit der Verarbeitung stattfindet. Das Gesetz formuliert, dass die Verarbeitung von personenbezogenen Daten nur rechtmäßig ist, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- es liegt eine Einwilligung vor,
- die Verarbeitung ist für die Erfüllung, eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich,
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich,
- die Verarbeitung dient lebenswichtigen Interessen der betroffenen Person,
- die Verarbeitung dient zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt,
- die Verarbeitung dient zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten.

Hier ist ebenfalls konkret und im Einzelfall zu prüfen, auf Basis welcher Rechtsgrundlage eine Verarbeitung der personenbezogenen Daten erfolgt. Auch für diesen rechtlichen Aspekt gilt das Prinzip der Rechenschaftspflicht. Außerdem ist die korrekte Rechtsgrundlage im Rahmen der Informationspflichten nach Art. 13 und Art. 14 zu veröffentlichen.

Insbesondere die Anwendung des Art. 6 Abs. 1 lit. f DSGVO ist in der Praxis nicht einfach. Zwar gibt die DSGVO mit dieser gesetzlichen Vorschrift dem Verantwortlichen einen gewissen Rahmen, innerhalb dessen eine Datenverarbeitung zulässig ist. Es ist aber ein dokumentierter Abwägungsvorgang vorzunehmen zwischen den berechtigten Interessen des Verantwortlichen oder eines Dritten und den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person. Hier spricht die DSGVO insbesondere auch die Situation von Kindern an und erwartet eine genaue Prüfung, wessen Interessen hier Vorrang haben.

Wenn keine der o. g. Bedingungen erfüllt ist, ist die Datenverarbeitung unzulässig. Es braucht auf jeden Fall eine entsprechende Rechtsgrundlage. Andernfalls drohen auch hier Bußgelder und Schadensersatzansprüche. *Die Einhaltung der Grundsätze in Art. 5 und die Rechtmäßigkeit der Verarbeitung in Art. 6 DSGVO ist dem Gesetzgeber besonders wichtig, was auch in der Festlegung der zweiten Bußgeldstufe bei Verstößen seinen Widerhall findet.*

Für besondere Kategorien personenbezogener Daten, beispielsweise politische Meinungen, religiöse oder weltanschauliche Überzeugung oder Gesundheitsdaten sowie die weiteren in Art. 9 Abs. 1 DSGVO aufgeführten Fälle, gelten weitere Sonderregelungen. Hier ist im Einzelfall sehr genau zu prüfen, ob eine Verarbeitung zulässig ist. Art. 9 Abs. 1 DSGVO geht bei besonderen Kategorien und besonders schützenswerten personenbezogenen Daten davon aus, dass eine Verarbeitung grundsätzlich untersagt ist. Hier formuliert der Gesetzgeber bewusst schärfer und lässt dann in einem eng zu verstehenden Ausnahmekatalog gemäß Art. 9 Abs. 2 eine Datenverarbeitung zu. Auch hier empfehlen wir, mit Blick auf die Rechenschaftspflicht eine genaue Überprüfung der Rechtsgrundlagen vorzunehmen.

In vielen Mustern für die Dokumentation der datenschutzrechtlichen Vorgänge ist nicht ausdrücklich hinterlegt, dass die Grundsätze dokumentiert abgeprüft werden. Wir empfehlen dies aber im Hinblick auf die Rechenschaftspflicht und empfehlen auch eine ausdrückliche Bewertung sowie Betrachtung, wie konkret die Grundsätze in der Datenverarbeitung angewandt werden.

Praxistipp

Datenschutzbeauftragter

In den Art. 37 – 39 sieht die DSGVO Regelungen für die Benennung eines Datenschutzbeauftragten vor. Jede Behörde und öffentliche Stelle hat einen Datenschutzbeauftragten zu bestellen. Darüber hinaus sind in Art. 37 Abs. 1 weitere Fälle benannt, in denen Datenschutzbeauftragte zu benennen sind. Hier hat der Bundesgesetzgeber aber mit § 38 BDSG neu verschärfende Regelungen vorgenommen, die sich an der bisherigen Rechtslage orientieren. Bei nichtöffentlichen Stellen ist ein Datenschutzbeauftragter zu bestellen, soweit in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Dabei ist allein auf die Anzahl der „Köpfe" abzustellen. Auch freie Mitarbeiter und Auszubildende werden berücksichtigt. *Darüber hinaus ist ein Datenschutzbeauftragter zu bestellen, wenn Verarbeitungen vorgenommen werden, die einer Datenschutz-Folgenabschätzung nach Art. 35 unterliegen. Dann ist eine entsprechende Bestellung, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen, zu übernehmen.*

Es empfiehlt sich also in der Praxis, insbesondere mit Blick auf Art. 38 BDSG neu zu überprüfen, ob ein Datenschutzbeauftragter benannt werden muss.

Die Benennung eines Datenschutzbeauftragten ist unabhängig von der Durchführung der nach der DSGVO geforderten Maßnahmen. Wenn beispielsweise ein Kleinbetrieb gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen, sind u. a. die o. g. Grundsätze der Datenverarbeitung sowie die in dieser Broschüre geschilderten weiteren Anforderungen einzuhalten.

Gemäß Art. 37 Abs. 7 muss der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten veröffentlichen und diese Daten der Aufsichtsbehörde mitteilen. Zukünftig wollen alle Aufsichtsbehörden ein entsprechendes Online-Tool zur Verfügung stellen, um eine erleichterte Übermittlung dieser Daten zu ermöglichen.

In Art. 38 ist die Stellung des Datenschutzbeauftragten beschrieben. Er berichtet unmittelbar der höchsten Managementstufe und darf hinsichtlich seiner Aufgaben keine Weisungen erhalten. Es soll eine Unabhängigkeit des Datenschutzbeauftragten bei der Aufgabenerfüllung sichergestellt sein. Der Verantwortliche und der Auftragsverarbeiter sollen den Datenschutzbeauftragten unterstützen. Deutlich wird in Art. 38 Abs. 6 ausgeführt, dass ein Datenschutzbeauftragter auch andere Aufgaben und Pflichten wahrnehmen kann. Das Gesetz fordert keinen Vollzeit-tägigen Datenschutzbeauftragten. Allerdings bleibt es die Aufgabe des Verantwortlichen oder des Auftragsverarbeiters, Interessenkollisionen zu vermeiden. *Damit wird vermutlich die bisherige Praxis aufrecht erhalten bleiben, dass sich bestimmte Positionen im Unternehmen nicht mit der Position als Datenschutzbeauftragter vertragen, beispielsweise die Position eines IT-Leiters oder eines Personalchefs sowie Mitglieder der Geschäftsleitung.*

Bemerkenswert ist die Aufgabenbeschreibung in Art. 39 DSGVO, die kraft Gesetzes ab dem 25.05.2018 für alle Datenschutzbeauftragten gilt, unabhängig ob sie als betrieblicher oder behördlicher Datenschutzbeauftragter tätig sind. Gemäß Art. 39 Abs. 1 lit. b DSGVO ist es die Pflicht des Datenschutzbeauftragten, die Einhaltung der Verordnung und der anderen nationalen Datenschutzvorschriften zu überwachen. Weitere gesetzliche Überwachungspflichten kommen hinzu. Damit ist der behördliche oder betriebliche Datenschutzbeauftragte eine der wenigen Positionen, die eine ausdrücklich im Gesetz festgelegte Überwachungspflicht hat.

Dies führt in der Praxis zu neuen Haftungsrisiken sowohl für interne als auch für externe Datenschutzbeauftragte.

Ein Datenschutzbeauftragter muss beispielsweise, wenn ein Bußgeld gegen das Unternehmen oder die öffentliche Einrichtung festgesetzt wurde, nachweisen können, dass er ausreichend seinen Überwachungspflichten nachgekommen ist. Bei externen Datenschutzbeauftragten besteht ansonsten das Risiko, dass der Verantwortliche und Auftraggeber gegenüber dem externen Datenschutzbeauftragten Regressansprüche geltend macht. Ein externer Datenschutzbeauftragter kann sich dann nur entlasten, wenn er nachweist, die konkrete datenverarbeitende Situation überwacht zu haben, und dass trotz der Überwachung ein Datenschutzverstoß geschehen ist, der mit Überwachung nicht zu verhindern war. Nach unserer Beobachtung führt dies auf der einen Seite bei den Datenschutzbeauftragten zu einer erheblich intensiveren Dokumentationspflicht, zum anderen sind rechtswidrige datenschutzrechtliche Zustände sehr früh und genau an die Geschäfts- oder Behördenleitung zu adressieren. Auch für interne Datenschutzbeauftragte ergibt sich ein Haftungsrisiko, da beispielsweise im Fall einer groben Fahrlässigkeit oder im Fall eines Vorsatzes die im Arbeitsrecht formulierten Begrenzungen der Arbeitnehmerhaftung nicht oder nur in geringem Umfang greifen. *Ein Fall der groben Fahrlässigkeit liegt beispielsweise vor, wenn bestimmte Fach- oder Geschäftsbereiche vom Datenschutzbeauftragten nicht überprüft worden sind oder die Überprüfung nur oberflächlich erfolgte.*

Damit gerät ein interner oder externer Datenschutzbeauftragter durchaus in die Rolle eines „Wirtschaftsprüfers" oder „Rechnungshofes" und ist verpflichtet, sich die Datenverarbeitungsvorgänge genau anzuschauen und zu überprüfen.

Zwar können keine Bußgelder direkt gegen einen Datenschutzbeauftragten nach Art. 83 DSGVO festgesetzt werden. In Anbetracht der sonstigen Haftungsrisiken ist dies aber nur ein schwacher Trost.

Jeder behördliche oder betriebliche Datenschutzbeauftragter sollte in seinem Arbeitsbereich genau prüfen, ob mit dem bisherigen Zeitrahmen die gesetzlich geforderte Überwachungspflicht tatsächlich umgesetzt werden kann. Wir beobachten, dass insbesondere nebenberufliche Datenschutzbeauftragte vielfach ein viel zu geringes Zeitkontingent und damit faktisch keine Möglichkeit haben, die Überwachung zu praktizieren. Ein solcher Zustand ist gegenüber der Geschäfts- oder Behördenleitung deutlich anzusprechen. Sollte es keine kurzfristige Änderung bzw. Erweiterung des Zeitkontingents und keine ausreichende Unterstützung bei der Umsetzung der gesetzlichen Anforderungen geben, empfehlen wir, das Amt als Datenschutzbeauftragter sofort niederzulegen. Nur so können Haftungsrisiken vermieden werden.

Praxistipp

Verzeichnis von Verarbeitungstätigkeiten

Wie bereits oben ausgeführt, entstehen umfangreiche Dokumentationspflichten. Das Gesetz fordert in Art. 30 DSGVO, dass der Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten führt, die in seinem Zuständigkeitsbereich liegen. Bereits jetzt gab es eine gesetzliche Anforderung, dass ein sog. „Verfahrensverzeichnis" erstellt wird. Hier ist die Beobachtung, dass vielfach solche Verfahrensverzeichnisse nur im geringen Umfang vorhanden sind. Da die Einhaltung dieser Regelung bußgeldbewehrt ist, empfehlen wir, diese Dokumentationspflicht ernst zu nehmen. *Das Verzeichnis der Verarbeitungstätigkeiten muss, anders als bisher, Dritten nicht zugänglich gemacht werden, sondern dient allein der internen datenschutzrechtlichen Dokumentation. Bei einer aufsichtsrechtlichen Überprüfung ist nach unserer Erfahrung ein solches Verzeichnis der Verarbeitungstätigkeiten sofort vorzulegen.*

Der Gesetzgeber legt nicht fest, wie die Struktur der Verzeichnisse aller Verarbeitungstätigkeiten sein soll. Wir empfehlen aber in der Praxis, nicht eine zu grobe Struktur zu wählen, da aufgrund der Überwachungspflichten eine mindestens jährliche Überprüfung der verschiedenen Verarbeitungsvorgänge erfolgen soll. Wir haben die Erfahrung gemacht, dass die Überwachung von nicht so umfangreichen Verzeichnissen von Verarbeitungstätigkeiten in der Praxis erheblich leichter ist.

Der Gesetzgeber legt in Art. 30 Abs. 1 DSGVO fest, welche Einzelheiten in einem Verzeichnis der Verarbeitungstätigkeiten festzuhalten sind. Beispielsweise sind Kategorien der Empfänger zu benennen, an die die personenbezogenen Daten weitergegeben werden. Die vorgesehenen Fristen für die Löschung der Daten sowie die Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO sind in einem solchen Dokument auszuführen.

In Anbetracht der Rechenschaftspflicht empfehlen wir aber, weitere Aspekte in dem Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren. Zum einen ist dort eine Rubrik für die Überwachungsdokumentation des Datenschutzbeauftragten vorzusehen, zum anderen ist eine ausdrückliche Dokumentation der Prüfung der Grundsätze der Verarbeitung gemäß Art. 5 und der Einhaltung der Rechtmäßigkeit gemäß Art. 6 DSGVO vorzusehen. Auch die Überprüfung der Anforderungen nach Art. 25 DSGVO, eines Datenschutzes durch Technikgestaltung oder durch datenschutzfreundliche Voreinstellung, sollte dokumentiert werden.

Beispielsweise empfiehlt sich im Personalbereich nicht, nur ein Verzeichnis der Verarbeitungstätigkeiten für alle Verarbeitungsvorgänge in der Personalabteilung zu erstellen. Wir empfehlen, beispielsweise den Bereich Lohn- und Gehaltsabrechnung, das Bewerbungsmanagement, die „normale Personalarbeit" sowie ein betriebliches Eingliederungsmanagement jeweils eigenständig in einem Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren.

Praxistipp

Auch aus einem anderen Grund ist ein gutes Verzeichnis der Verarbeitungstätigkeiten mit entsprechender genauer Dokumentation wichtig. Hier finden sich alle notwendigen Informationen, die für die Umsetzung der Informationspflichten nach Art. 13 und Art. 14 DSGVO notwendig sind. Insoweit werden die entsprechenden Daten an anderer Stelle zur Umsetzung der datenschutzrechtlichen Pflichten benötigt.

Neu ist die Pflicht für Auftragsverarbeiter gemäß Art. 30 Abs. 2 DSGVO, ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten zu führen. Hier ist im Moment unklar, ob für jeden Kunden ein einzelnes Dokument erstellt werden muss, oder ob bei vielen gleichlautenden Verarbeitungen ein zentrales Dokument erstellt wer-den kann, das dann auf eine Kundenliste referenziert. Unabhängig davon ist aber ein eigenes Verzeichnis der Verarbeitungstätigkeiten zu führen, das u. a. eine genauere Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO enthält. Wir beobachten teilweise in der Praxis, dass Verantwortliche von ihren Auftragsverarbeitern genau dieses Dokument nach Art. 30 Abs. 2 DSGVO abfordern, um sich ihre eigenen Dokumentationspflichten zu erleichtern. Darauf sollten sich Auftragsverarbeiter, beispielsweise IT-Dienstleister und IT-Systemhäuser einstellen.

In Art. 30 Abs. 5 DSGVO ist eine Ausnahmeregelung vorgesehen. Diese Ausnahmeregelung ist aber so unglücklich formuliert, dass sie faktisch keine Anwendung findet. Zwar soll bei Unternehmen, die weniger als 250 Mitarbeiter beschäftigen, kein Verzeichnis der Verarbeitungstätigkeiten zu erstellen sein. Allerdings werden dann im Nachgang Gegenausnahmen formuliert. Wenn beispielsweise die Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen in sich trägt, ist dann doch ein Verzeichnis der Verarbeitungstätigkeiten zu erstellen. Auch wird erwartet, dass ein Verarbeitungsverzeichnis von Kleinunternehmen erstellt wird, wenn eine Verarbeitung öfter als nur gelegentlich erfolgt. Faktisch sind durch die Gegenausnahmen damit die meisten Unternehmen wieder mit umfasst. Nach unserer Beobachtung ist die praktische Auswirkung der Ausnahmeregelung in Art. 30 Abs. 5 DSGVO nicht vorhanden.

Wir haben die Erfahrung gemacht, dass die Informationssammlung für die Verzeichnisse der Verarbeitungstätigkeiten häufig Mühe macht und sich einige Zeit hinzieht. Kalkulieren Sie pro Verzeichnis der Verarbeitungstätigkeiten einen Zeitumfang von mindestens 4-8 Arbeitsstunden. Wenn Sie beispielsweise insgesamt 10 verschiedene Fachanwendungen im Unternehmen einsetzen, entsteht ein nicht unerheblicher Zeitbedarf, um eine den gesetzlichen Anforderungen genügende Dokumentation zu erstellen.

Praxistipp

Auftragsverarbeitung

Wenn eine Verarbeitung von personenbezogenen Daten im Auftrag eines Verantwortlichen stattfindet, ist gemäß Art. 28 DSGVO dies nur zulässig, wenn geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten vom Auftragsverarbeiter ergriffen werden. Hier erwartet das Gesetz eine schriftliche Vereinbarung, sprich einen Vertrag zur Auftragsverarbeitung. In Art. 28 Abs. 3 sind darüber hinaus verschiedene Pflichten definiert. Auch greift die wiederholt zitierte Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO. Eine Weitergabe personenbezogener Daten an einen Auftragsverarbeiter und eine Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ist rechtlich nur zulässig und legal, wenn eine ausreichende Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde. *Mit anderen Worten: Eine unzureichende vertragliche Grundlage führt zu einer illegalen Datenverarbeitung.*

Dies ist für Auftragsverarbeiter, beispielsweise Rechenzentren oder Hoster, ein neues Risiko. Betroffene können Rechte sowohl gegen den Verantwortlichen als auch gegen den Auftragsverarbeiter geltend machen, beispielsweise Schmerzensgeldansprüche. Daneben ist aufgrund der eigenen Verantwortung des Auftragsverarbeiters dieser auch im Fokus der Bußgeldvorschriften.

Die bayrische Landesdatenschutzaufsicht hat eine ↗Formulierungshilfe für die Auftragsverarbeitung herausgegeben. Die Formulierungen dokumentieren Anforderungen der Aufsichtsbehörden an einen rechtskonformen Auftragsverarbeitungsvertrag.

Dabei sind drei Aspekte besonders auffällig:

- In dem Muster-Dokument wird erwartet, dass eine auf die individuelle Situation abgestimmte Risiko-Bewertung Grundlage von datenschutzrechtlichen Maßnahmen ist. Erwartet offensichtlich die Aufsichtsbehörde eine individualisierte Betrachtung der jeweiligen Verarbeitungsvorgänge. Dies ist bisher in der Praxis nicht häufig so umgesetzt worden.
- Es wird erwartet, dass der Auftragnehmer ein Datenschutzkonzept vorlegt. Dieses soll Anlage zum Vertrag zur Auftragsverarbeitung werden.
- Der Auftragsverarbeiter soll die Einhaltung der gesetzlich geforderten Maßnahmen nachweisen. Die Aufsichtsbehörde erwartet eine mindestens einmal jährlich vorzunehmende Auditierung. Der Auftraggeber soll den vollständigen Auditbericht erhalten. Nur so kann überwacht werden, ob der Auftragsverarbeiter seine gesetzlichen Verpflichtungen einhält.

Es ist aktuell zu beobachten ist aktuell zu beobachten, dass die wenigsten Auftragsverarbeiter über eine individualisierte Risikobewertung, ein Datenschutzkonzept und eine regelmäßige Auditierung verfügen. Insoweit muss sich ein Auftraggeber und Verantwortlicher darauf einstellen, dass entsprechende Anforderungen nur mühsam durchgesetzt werden können.

Sicherheit der Verarbeitung

In Art. 32 DSGVO formuliert der Gesetzgeber seine Anforderungen an die Sicherheit der Verarbeitung personenbezogener Daten. Es wird erwartet, dass ein dem Risiko angemessenes Schutzniveau gewährleistet wird. Dabei sind verschiedene Aspekte zu berücksichtigen, beispielsweise der Stand der Technik, Implementierungskosten oder die Eintrittswahrscheinlichkeit und Schwere von Risiken für die Rechte und Freiheiten natürlicher Personen. Es findet sich die bereits bei der Auftragsverarbeitung angesprochene individuelle Risikobewertung.

Diese Risikobewertung äußert sich u. a. in einer Klassifizierung der jeweiligen Datenverarbeitung in verschiedene Schutzstufen. Diese Klassifizierung sollte in dem Verzeichnis der Verarbeitungstätigkeiten dokumentiert und begründet werden.

Beispielhaft zählt dann der Gesetzgeber auf, welche Maßnahmen er für angemessen hält. In Art. 32 Abs. 1 lit. a DSGVO erwartet er die Pseudonymisierung und Verschlüsselung personenbezogener Daten. Auch soll die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen, vorhanden sein. Weiterhin fordert der Gesetzgeber in Art. 32 Abs. 1, dass personenbezogene Daten im Fall eines technischen oder physischen Zwischenfalls rasch wiederhergestellt werden sollen. Erwartet wird eine regelmäßige Überprüfung, Bewertung und Evaluierung der verschiedenen Maßnahmen. Insgesamt wird ein umfassendes System zur IT-Sicherheit gefordert. Sollte dies nicht vorhanden sein, ist dies ein Bußgeldtatbestand. Auch sind die entsprechenden Maßnahmen zu dokumentieren, damit der Verantwortliche oder der Auftragsverarbeiter seiner Rechenschaftspflicht Genüge tun kann.

Meldepflichten

Ergänzend zu den Anforderungen aus Art. 32 DSGVO zur Sicherheit der Verarbeitung ist in Art. 33 und in Art. 34 DSGVO eine Meldepflicht bei Verletzung des Schutzes personenbezogener Daten vorgesehen. In Art. 4 Nr. 12 DSGVO ist festgelegt, wann ein solcher Fall der Verletzung des Schutzes personenbezogener Daten vorliegt. Dies tritt beispielsweise ein, wenn Daten unberechtigterweise vernichtet oder verändert werden. *Eine Verletzung des Schutzes personenbezogener Daten besteht aber auch dann, wenn eine unbefugte Offenlegung oder ein unbefugter Zugang zu personenbezogenen Daten erfolgte.* In Art. 33 DSGVO ist dann in der ersten Stufe eine Meldepflicht bei der Aufsichtsbehörde vorgesehen. Hier ist die Schwelle für eine Meldepflicht relativ gering. Es wird erwartet, dass nach einem Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden eine Meldung an die Aufsichtsbehörde abgesetzt wird. Es soll bei allen Aufsichtsbehörden entsprechende Online-Meldetools geben.

Nach Art. 34 ist der Betroffene ebenfalls unabhängig von der Meldung an die Aufsichtsbehörde zu informieren, wenn ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen besteht.

Eine Meldepflicht entfällt nur dann, wenn der Verantwortliche in seiner rechtlichen Bewertung dazu kommt, dass keine Risiken für den Betroffenen bestehen. Eine solche Bewertung sollte auf jeden Fall dokumentiert werden. Dies fordert Art. 32 Abs. 5 DSGVO. Die Dokumentation soll der Aufsichtsbehörde die Überprüfung der Einhaltung dieser Bestimmungen ermöglichen.

Eine nicht abgesetzte Meldung an die Aufsichtsbehörde oder den Betroffenen löst einen Bußgeldtatbestand aus.

Bei der Meldung ist zum einen zu beschreiben, um welche Art der Verletzung des Schutzes personenbezogener Daten es sich handelt, Name und Kontaktdaten des Datenschutzbeauftragten sind zu benennen und die wahrscheinlichen Folgen der Verletzung sind näher zu beschreiben. Abschließend sind dann die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung darzulegen. Faktisch ist dies die Einrichtung eines Informationssicherheitsmanagementsystems.

Beispiel:

Ein verloren gegangener USB-Stick oder ein verlorenes Notebook kann eine Meldepflicht auslösen, wenn unverschlüsselt auf dem USB-Stick oder dem Notebook personenbezogene Daten, beispielsweise Kundenlisten oder E-Mail-Adressen vorhanden waren. Hier kann ein Verantwortlicher mit der Meldung auch einen weiteren Datenschutzverstoß dokumentieren und ein weiteres Bußgeld auslösen. Wer beispielsweise eine Meldung an die Aufsichtsbehörde absetzt, dass ein unverschlüsseltes Notebook oder ein unverschlüsselter USB-Stick verloren gegangen ist, dokumentiert damit gleichzeitig, dass die Regelungen aus Art. 32 DSGVO zur Sicherheit der Verarbeitung und die in Art. 32 Abs. 1 lit. a DSGVO geforderte Verschlüsselung personenbezogener Daten nicht stattgefunden hat. Insoweit ist der Inhalt der jeweiligen Meldung vor Versendung an die Aufsichtsbehörde juristisch zu bewerten. All dies ist in 72 Stunden sicherzustellen.

Wenn ein Verantwortlicher oder ein Auftragsverarbeiter von den in Artikel 32 Absatz 1 DSGVO genannten Maßnahmen abweichen möchte, muss dies schriftlich dokumentiert und begründet werden. Ein Beispiel: Wird in einem Unternehmen oder einer öffentlichen Einrichtung auf die Verschlüsselung personenbezogener Daten verzichtet, muss erklärt werden, wie der Schutz dieser Daten trotzdem gewährleistet wird und warum keine Verschlüsselung eingesetzt wird. Die im Gesetz genannten Anforderungen sind zwar nur Beispiele, haben aber in der Praxis einen großen Einfluss.

Praxistipp

Betroffenenrechte

Neben den Informationspflichten nach Art. 13 und Art. 14 DSGVO sieht das neue Datenschutzrecht weitere Betroffenenrechte vor. *Nach Art. 15 hat ein Betroffener ein Auskunftsrecht über die personenbezogenen Daten und weitere in Art. 15 Abs. 1 DSGVO festgelegte Informationen. Gemäß Art. 12 Abs. 3 muss der Verantwortliche innerhalb eines Monats auf den Auskunftsanspruch einer betroffenen Person reagieren.* Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Dann ist allerdings der Betroffene zu informieren und die Gründe der Verzögerung sind darzulegen.

Weiterhin hat ein Betroffener ein Recht auf Berichtigung (Art. 16 DSGVO), ein Recht auf Löschung (Art. 17 DSGVO), ein Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) und ein Recht auf Datenübertragbarkeit (Art. 20 DSGVO).

Bei dem Recht auf Datenübertragbarkeit nach Art. 20 DSGVO ist aktuell noch unklar, welche praktischen Auswirkungen dies haben wird. Ein Betroffener kann seine personenbezogenen Daten herausverlangen und von dem Verantwortlichen eine Übermittlung an einen neuen Verantwortlichen fordern.

Beispiel:

Wenn ein Betroffener seine Autoversicherung wechselt, so kann von der alten Autoversicherung verlangt werden, dass alle Informationen aus dem Versicherungsverhältnis in einem strukturierten, gängigen und maschinenlesbaren Format direkt an die neue Autoversicherung von dem alten Autoversicherer übermittelt werden.

Wir empfehlen, die Meldepflichten ebenfalls sehr ernst zu nehmen. In der Praxis beobachten wir, dass Aufsichtsbehörden sehr verärgert reagieren, wenn Datenschutzpannen über Dritte bekannt werden und der Verantwortliche keine eigene Meldung abgesetzt hat.

Praxistipp

DSGVO FÜR FORTGESCHRITTENE

Datenschutz-Folgenabschätzung

Neben den bereits beschriebenen Herausforderungen erwartet die DSGVO, dass weitere Maßnahmen zur Umsetzung und Implementierung eines guten Datenschutzniveaus erfolgen. Unter der Bezeichnung „Datenschutz-Folgenabschätzung" wird in Art. 35 und Art. 36 DSGVO ein weiteres Verfahren festgelegt. *Wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, ist vorab eine Abschätzung der Folgen für den Schutz der personenbezogenen Daten durchzuführen.* Hier sind die Risiken genauer zu betrachten und zu bewerten. Auch muss der Verantwortliche deutlich machen, welche Abhilfemaßnahmen er ergreifen will, um die Risiken zu bewältigen. Ggf. ist gemäß Art. 35 Abs. 9 DSGVO der Standpunkt der betroffenen Person und ihrer Vertreter einzuholen.

Insgesamt ist die Datenschutz-Folgenabschätzung eine umfassende datenschutzrechtliche Bewertung im Vorfeld einer IT-Einführung.

Aktuell ist die Beobachtung zu machen, dass in vielen Beschaffungsvorgängen die datenschutzrechtliche Bewertung oberflächlich ausfällt oder nicht stattfindet. Diese Praxis ist vor dem Hintergrund der neuen gesetzlichen Herausforderungen nicht aufrecht zu erhalten.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

In Art. 25 DSGVO formuliert der europäische Gesetzgeber weitergehende Anforderungen für die Zukunft. *Erwartet wird, dass Datenschutz bereits bei der Entwicklung von Software und durch Technikgestaltung wirksam beachtet wird. Datenschutzfreundliche Voreinstellungen sollen dazu führen, dass letztendlich die datenschutzrechtlichen Vorgaben der DSGVO möglichst frühzeitig bedacht und beachtet werden.*

Hat ein Verantwortlicher gemäß Art. 5 Abs. 2 DSGVO eine Rechenschaftspflicht und ein Datenschutzbeauftragter muss gemäß Art. 39 Abs. 1 lit. b DSGVO die Einhaltung dieser gesetzlichen Vorgabe überwachen. Auch hier hat der Gesetzgeber mit einer Verankerung in den Bußgeldtatbeständen deutlich gemacht, dass ihm die Einhaltung des Art. 25 DSGVO wichtig ist. Hier wird sich in Zukunft zeigen, wie in der Praxis mit diesen Anforderungen umzugehen ist. Generell sollten in IT-Verträgen Regelungen aufgenommen werden, wie im Einzelnen Datenschutz durch Technikgestaltung oder durch datenschutzfreundliche Voreinstellungen umgesetzt wird oder werden kann.

Kontakt

Mail: info@eset.de

ESET Deutschland GmbH

Spitzweidenweg 32

07743 Jena

Deutschland

ÜBER ESET

Als europäischer Hersteller mit mehr als 35 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Organisationsgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihre Infrastruktur mithilfe von Cloud Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungslösungen unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen sowie Compliance-Maßnahmen.

Unsere Extended Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

3 VON ÜBER 500.000 ZUFRIEDENEN KUNDEN

BVB 09 CHAMPION PARTNER

Seit 2019 ein starkes Team auf dem Platz und digital

KLINIKUM LANDSHUT

Seit 2022 durch ESET geschützt Mehr als 1.450 Postfächer

ISP Security Partner seit 2008 2 Millionen Kunden

BEWÄHRT

Secur|ty made in EU
Trust Seal www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel „IT Security made in EU" verliehen

ISO 9001 SYSTEM CERTIFICATION SGS

ISO/IEC 27001 SYSTEM CERTIFICATION SGS

Unsere Lösungen sind nach den Qualitäts- und Informationssicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2022 zertifiziert

ESET IN ZAHLEN

110.000.000+
Geschützte Nutzer weltweit

500.000+
Geschützte Unternehmen

178
Länder & Regionen

12
Forschungs- und Entwicklungszentren weltweit

ESET BLOG