Datenschutzrechtliche Neuregelungen für Unternehmen

Gravierende Änderungen durch die Datenschutz-Grundverordnung

Dr. Thomas Söbbing

Am 25. Mai 2018 tritt die Datenschutz-Grundverordnung (DSGVO) in Kraft und löst das Bundesdatenschutzgesetz (BDSG) in seiner jetzigen Form ab. Dies führt zu einigen Änderungen, die bisher von vielen Unternehmen noch nicht berücksichtigt worden sind. Die Einhaltung der neuen Vorgaben ist für alle Unternehmen, die Waren oder Dienstleistungen in der Europäischen Union anbieten, zwingend. Andernfalls drohen finanzielle Sanktionen. Der Beitrag gibt einen Überblick über Aspekte der DSGVO, die für Unternehmen wichtig sind. (Red.)

Laut in einer Studie des Beratungshauses Carmao[1] erfüllen noch nicht einmal 38 Prozent der Unternehmen die bereits bestehenden Vorgaben des Bundesdatenschutzgesetzes. Und mehr als die Hälfte der befragten Unternehmen zweifelt daran, die Auflagen der europäischen Datenschutz-Grundverordnung fristgerecht erfüllen zu können. Umso wichtiger ist es, sich intensiv mit dem Thema DSGVO zu beschäftigen.

Die DSGVO ersetzt die aus dem Jahr 1995 stammende europäische Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Im Gegensatz zu dieser Richtlinie, die von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden musste, gilt die Datenschutz-Grundverordnung unmittelbar in allen EU-Mitgliedstaaten ab dem 25. Mai 2018, da es sich bei dem neuen Gesetz um eine europäische Verordnung handelt. Die nationalen Gesetzgeber werden lediglich neue Gesetze erlassen, um die nationalen Vorschriften, die durch die Verordnung ersetzt werden, aufzuheben.

DER AUTOR:


Quelle: Deutsche Leasing

Dr. Thomas Söbbing, Frankfurt am Main,

ist Fachleiter Recht bei der Deutsche Leasing AG. Zuvor war er in leitenden und beratenden Positionen bei IBM, KPMG und Siemens tätig. Ferner ist er Hochschuldozent an der German Graduate School (GGS).

E-Mail: Thomas.Soebbing@deutsche-leasing.com

Sachlicher Anwendungsbereich

Mit der DSGVO wird das Datenschutzrecht in der EU vereinheitlicht. Die DSGVO regelt dabei die Rechtsgrundlagen der Datenverarbeitung, die Rechte der davon Betroffenen, die Pflichten der dafür Verantwortlichen et cetera. Die bereits geltenden Betroffenenrechte aus dem BDSG werden erweitert und durch neue Rechte ergänzt.

So wurde zum Beispiel die Datenportabilität aufgenommen; in der Konsequenz soll der Betroffene nach Artikel 20 DSGVO seine personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format herausverlangen dürfen. Alternativ ermöglicht die Vorschrift dem Betroffenen auch, die Daten durch den Verantwortlichen zu einem neuen Verantwortlichen übermitteln zu lassen.

Aus dem Recht auf Vergessenwerden aus Artikel 17 DSGVO leitet sich das Recht ab, dass Personen von Verantwortlichen die Löschung ihrer personenbezogenen Daten verlangen können. Bei einem entsprechenden Antrag ist der Verantwortliche verpflichtet, solche Daten unverzüglich zu löschen, sofern sie für die Zwecke, für die sie erhoben und verarbeitet wurden, nicht mehr notwendig sind. Eine andere Möglichkeit ist, dass die betroffene Person ihre Einwilligung, auf die sich die Verarbeitung stützte, widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt. Ziel der DSGVO ist es, ein einheitliches Regelwerk in der ganzen EU zum Schutz personenbezogener Daten zu schaffen. Solche Daten sind nach Artikel 4 Nummer 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Räumlicher Anwendungsbereich

Der räumliche Anwendungsbereich der DSGVO ist im Vergleich zur Datenschutzrichtlinie 95/46/EG eine

1) Veröffentlicht in der Computerwoche vom 27. Juni 2017.

große Neuerung: Künftig gilt zusätzlich das Marktortprinzip. Werden personenbezogene Daten im Zusammenhang mit Angeboten von Waren oder Dienstleistungen in der Europäischen Union verarbeitet, muss sich die verarbeitende Stelle an die Vorgaben der DSGVO halten. Dadurch fällt der Kreis der Betroffenen deutlich größer aus. Denn gemäß Artikel 3 DSGVO findet die Verordnung Anwendung bei der Verarbeitung personenbezogener Daten, wenn sie im Rahmen der Tätigkeiten einer EU-Niederlassung eines Verantwortlichen oder seines Auftragsverarbeiters erfolgt, unabhängig davon, ob die eigentliche Datenverarbeitung in der EU stattfindet.

Diese Verordnung wird ebenfalls angewendet bei nicht in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeitern, wenn von der Datenverarbeitung Personen betroffen sind, die sich in der EU befinden. Dabei genügt es, dass die Datenverarbeitung im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen steht, unabhängig davon, ob von den betroffenen Personen eine Zahlung zu leisten ist; das Verhalten betroffener Personen ist dabei entscheidend, soweit ihr Verhalten in der EU erfolgt.

Verarbeitung von personenbezogenen Daten

Die allgemeinen Grundsätze nach Artikel 5 Absatz 1 DSGVO stellen dabei so etwas wie die Grundregeln für die Verarbeitung von personenbezogenen Daten dar; sie helfen bei der Auslegung von Regelungen der DSGVO. Diese Grundsätze der Datenverarbeitung muss jeder Verantwortliche einhalten und dies nachweisen können (sogenannte Rechenschaftspflicht).[2] Dafür eignet sich beispielsweise das Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 DSGVO.

Einer der wesentlichen Grundsätze der DSGVO ist die rechtmäßige Verarbeitung personenbezogener Daten. Die Rechtmäßigkeit ist in Artikel 6 Absatz 1 DSGVO geregelt. Es muss demnach immer eine Rechtsgrundlage zur Legitimation der Verarbeitung vorliegen. Je nach Zweck der Datenverarbeitung kann der Verantwortliche die Rechtmäßigkeit dabei auf verschiedene Tatbestände stützen. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig,

- wenn eine Einwilligung der betroffenen Person vorliegt,
- zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen,
- zur Erfüllung einer rechtlichen Verpflichtung,
- zum Schutze lebenswichtiger Interessen,
- zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt oder aufgrund einer Interessenabwägung erforderlich ist.

Auch die DSGVO kennt besondere Kategorien personenbezogener Daten, welche einen erhöhten Schutzbedarf aufweisen. Diese werden in Artikel 4 und 9 DSGVO aufgelistet und entsprechen weitgehend den aus dem BDSG bekannten besonderen Arten personenbezogener Daten. Hinzu kommen biometrische und genetische Daten.

Sanktionen

Die DSGVO sieht erhebliche Sanktionen vor. Als Höchststrafe für Verstöße können 20 Millionen Euro oder vier Prozent des Jahresumsatzes eines Unternehmens verhängt werden.[3] Dies zeigt, dass das Verschlafen der DSGVO kein Kavaliersdelikt ist, sondern sehr schmerzhaft sein kann.

Firmen sollten in wichtigen Datenverarbeitungsbereichen regelmäßige Datenschutz-Audits durchführen, um das Risiko kostenträchtiger Datenschutzverstöße zu minimieren und die Gefahr hoher Sanktionen zu vermeiden. Sie sollten eine Risikoanalyse und eine Folgenabschätzung durchführen und die Einhaltung der Regeln alle zwei Jahre durch einen externen Experten überprüfen lassen.

Betrieblicher Datenschutzbeauftragter

Die Artikel 34 bis 37 DSGVO regeln die Benennung eines Datenschutzbeauftragten, seine Stellung und seine Aufgaben. Die DSGVO enthält in Artikel 37 Regelungen zum Datenschutzbeauftragten. Demnach soll eine Verpflichtung zur Bestellung durch nicht öffentliche Stellen grundsätzlich nur dann bestehen, wenn die Kerntätigkeit des Unternehmens die Verarbeitung besonders sensibler Daten (zum Beispiel Gesundheitsdaten) oder eine systematische Überwachung von betroffenen Personen ist.

Eine zahlenmäßige Beschränkung der mit der Datenverarbeitung beschäftigten Personen gibt es im Vergleich zum geltenden Recht nicht. Die Bestellpflicht würde ohnehin schon für die meisten Betriebe entfallen. In Artikel 37 Absatz 4 DSGVO sieht eine Öffnungsklausel allerdings vor, dass die Mitgliedstaaten die Pflicht zur Bestellung eines Datenschutzbeauftragten ergänzend zu den oben genannten Fallkonstellationen auch weitergehend regeln können.

Von dieser Befugnis wird die Bundesrepublik Deutschland voraussichtlich Gebrauch machen. Die beiden bisher bekannten Entwürfe des Bundesministeriums des Inneren für ein neues BDSG sehen eine Bestellpflicht ähnlich wie beim jetzigen § 4 f BDSG vor.

Einwilligung zur Datenverarbeitung

Grundsätzlich dürfen personenbezogene Daten nur genutzt werden,

2) Vgl. Artikel 5 Absatz 2 D.SGVO.
3) Vgl. Artikel 83 DSGVO.

wenn eine freiwillig abgegebene, spezifische und informierte Einwilligung des Betroffenen vorliegt. Schweigen oder Inaktivität dürfen nicht als Einwilligung interpretiert werden. Was bisher aus dem § 28 Absatz 1 Nummer 1 BDSG bekannt ist, dass das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist, darf zukünftig auch gelten, ist nur enger zu sehen.

Nach Artikel 6 DSGVO ist die Verarbeitung nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben.
- Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen.

Die DSGVO räumt Betroffenen gemäß Artikel 13 DSGVO weitreichende Informationsrechte ein. Beispielsweise ist eine Informationspflicht über die Dauer der Datenspeicherung vorgesehen.

Die DSGVO führt für Unternehmen und Verantwortliche eine Reihe von neuen Informationspflichten ein. Dabei will der EU-Gesetzgeber einen Grundsatz der fairen und transparenten Datenverarbeitung schaffen. Die betroffenen Nutzer sollen zukünftig besser in der Lage sein, eine Datenerhebung, -verarbeitung oder -nutzung anhand der zur Verfügung gestellten Informationen zu überprüfen.

Die Grundverordnung regelt die Informationspflichten in den Artikeln 13 und 14 DSGVO in zwei sehr umfangreichen und über das bisher Erforderliche hinausgehenden Katalogen. Ergänzend dazu finden sich in einer Vielzahl der Erwägungsgründe der Datenschutz-Grundverordnung Anmerkungen und Hinweise, welche den Grundsatz der fairen und transparenten Verarbeitung stets hervorheben. Es wird unterschieden zwischen Informationspflichten bei der Erhebung personenbezogener Daten beim Betroffenen[4] sowie Informationspflichten für den Fall, dass die Erhebung nicht direkt bei dem Betroffenen erfolgt.[5]

Informationspflichten

Werden personenbezogene Daten beim Betroffenen erhoben, muss der Verantwortliche nach Artikel 13 Absatz 1 DSGVO folgende Informationen mitteilen:

- Identität des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Verarbeitungszwecke und Rechtsgrundlage
- berechtigtes Interesse
- Empfänger
- Übermittlung in Drittstaaten
- Dauer der Speicherung
- Rechte der Betroffenen
- Widerrufbarkeit von Einwilligungen
- Beschwerderecht bei der Aufsichtsbehörde
- Verpflichtung zur Bereitstellung personenbezogener Daten
- automatisierte Entscheidungsfindung und Profiling.

Werden personenbezogene Daten nicht beim Betroffenen erhoben, bestehen nach Artikel 14 DSGVO für den Verantwortlichen nahezu dieselben Informationspflichten, wie bei

4) Vgl. Artikel 13 DSGVO.
5) Vgl. Artikel 14 DSGVO.

der Erhebung direkt beim Betroffenen. Dabei muss der Betroffene nicht über eine etwaige Verpflichtung zur Bereitstellung informiert werden, da er selbst nicht über die Bereitstellung entscheiden kann.

Gemäß Artikel 14 Absatz 2f DSGVO 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. Nach Artikel 12 DSGVO 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.

Es wird explizit erwähnt, dass dafür auch sogenannte „standardisierte Bildsymbole" verwendet werden können, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln.

Anders als im BDSG wird es in der Datenschutz-Grundverordnung besondere Anforderungen an die Verarbeitung personenbezogener Daten von Kindern geben. In diesem Falle sollten nach Erwägungsgrund 58 der DSGVO aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann.

Bei der Direkterhebung muss der Betroffene nach Artikel 13 Absatz 1 DSGVO zum Zeitpunkt der Erhebung informiert werden. Werden die Daten nicht beim Betroffenen erhoben, muss der Verantwortliche die Informationen nach Artikel 14 Absatz 3 DSGVO 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. Bei der Direkterhebung kann nach Artikel 13 Absatz 4 DSGVO 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 gemäß Artikel 14 Absatz 5 DSGVO 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 satzungsgemäße Geheimhaltungspflicht.

Insgesamt lässt sich festhalten, dass die Fälle, in denen auf eine Information des Betroffenen verzichtet werden kann, im Vergleich zum BDSG eingeschränkt werden.

Managementsystem zum Datenschutz

Nach Artikel 30 DSGVO muss ein Unternehmen ein Verzeichnis aller Verarbeitungstätigkeiten von personenbezogenen Daten führen. Dies ist nur eine von mehreren neuen Vorgaben zur Dokumentationspflicht. Bei der Einhaltung aller gesetzlichen Vorgaben wird das Verzeichnis aber eine tragende Rolle spielen. Denn es enthält eine Dokumentation und Übersicht über alle eingesetzten Verfahren, bei denen personenbezogene Daten verarbeitet werden.

In der Datenschutz-Grundverordnung finden sich einige Normen, die eine Dokumentierung der getroffenen Datenschutzmaßnahmen fordern. Daneben schafft die DSGVO weitere Prozesse, die etabliert und Aufgaben, die wahrgenommen werden müssen. Bei dieser Vielzahl von Anforderungen empfiehlt es sich, ein Datenschutz-Managementsystem einzuführen, welches die Einhaltung aller Vorgaben systematisch plant, umsetzt und laufend kontrolliert.

Bisher war die Auftragsdatenverarbeitung in § 11 BDSG geregelt. Danach handelt der Auftragnehmer aus-

Pflichten an den Auftragsverarbeiter

DSGVO-Vorschrift	Inhalt
Artikel 27 Absatz 1	Die Pflicht zur Bestellung eines „Repräsentanten" betrifft auch den Auftragsverarbeiter.
Artikel 30 Absatz 2	Der Auftragsverarbeiter ist zur Führung von Verfahrensverzeichnissen verpflichtet.
Artikel 31	Die Pflicht zur Zusammenarbeit mit der Datenschutzaufsicht betrifft auch den Auftragsverarbeiter.
Artikel 32 Absatz 1	Die Pflicht zu technischen und organisatorischen Maßnahmen der Datensicherheit gilt auch für den Auftragsverarbeiter.
Artikel 37 Absatz 1	Die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten betrifft auch den Auftragsverarbeiter.
Artikel 44	Die Beschränkungen für den Datentransfer in Drittländer sind auch vom Auftragsverarbeiter zu beachten.

Quelle: Dr. Thomas Söbbing

schließlich nach den Weisungen des Auftraggebers.[6] Gemäß § 11 Absatz 4 BDSG ist der Auftragnehmer von der Einhaltung der Bestimmungen des Datenschutzrechts in weitem Umfang befreit. Die Verantwortung für eine rechtskonforme Datenverarbeitung bleibt nahezu vollständig beim Auftraggeber.

Verarbeitung von Auftragsdaten

Durch die DSGVO wird der Begriff des Verantwortlichen in Artikel 4 Nummer 7 DSGVO für die Europäische Union nun wie folgt definiert: „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden."

Der Auftragsverarbeiter wird in Artikel 4 Nummer 8 DSGVO wie folgt beschrieben: „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet." Dabei stellt die Definition des Artikels 4 Nummer 8 DSGVO lediglich auf ein Auftragsverhältnis ab, nicht jedoch auf Weisungsrechte und Verantwortlichkeiten. Ein eigenverantwortliches Handeln des Auftragsverarbeiters ist nach der Definition ebenso wenig ausgeschlossen wie Entscheidungsspielräume des Auftragsverarbeiters.

Die DSGVO verpflichtet den Auftragnehmer weitaus stärker zur Einhaltung des Datenschutzrechts, als dies nach dem BDSG der Fall ist. Während nach dem BDSG ausschließlich der Auftraggeber für die Datenverarbeitung verantwortlich ist, wird durch die DSGVO der Auftragnehmer für die Verarbeitung der Daten mitverantwortlich. So finden sich an zahlreichen Stellen der DSGVO selbstständige Pflichten, die sich an den Auftragsverarbeiter richten (siehe Abbildung, Seite 8).

Nach Artikel 29 DSGVO arbeitet der Auftragsverarbeiter ausschließlich bei der Datenverarbeitung auf Weisung des Verantwortlichen: „Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind."

Datentransfers ins Ausland

Grundsätzlich hat bereits das Bundesdatenschutzgesetz in § 4b ff. BDSG den Transfer von personenbezogenen Daten in Staaten außerhalb der EU oder des EWG (sogenannte Drittstaaten) erschwert. Dabei wurde vom Bundesdatenschutzgesetz unterstellt, dass in Drittstaaten generell kein angemessenes Datenschutzniveau herrscht.

An dieser Ansicht hat sich mit der DSGVO nichts geändert. Gemäß Artikel 44 DSGVO ist jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, nur dann zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel[7] niedergelegten Bedingungen einhalten und auch die sonstigen Bestim-

6) Vgl. § 11 Absatz 3 S. 1 BDSG.
7) Kapitel 5 Artikel 44 bis 50.

mungen dieser Verordnung eingehalten werden.

Dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Somit ist ein Datentransfer in Drittstaaten auch weiterhin nur dann zulässig, wenn zusätzliche Sicherheitsmechanismen dazu beitragen, ein angemessenes Datenschutzniveau zu gewährleisten oder wenn ein solches verbindlich festgestellt wurde.

Gemäß Artikel 45 DSGVO darf eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein/mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

Daneben bleiben auch die in der Datenschutz-Richtlinie geregelten weiteren Möglichkeiten des Datentransfers anwendbar. So ist es gemäß Artikel 49 DSGVO beispielsweise möglich, personenbezogene Daten auf Basis einer Einwilligung oder zur Erfüllung eines Vertrages zu übermitteln. Von der Kommission erlassene Beschlüsse über ein angemessenes Datenschutzniveau in einem bestimmten Land, welche auf der Grundlage der Datenschutz-Richtlinie entschieden wurden, bleiben ebenfalls in Kraft, bis sie durch einen Beschluss der Kommission, der nach einem in der Grundverordnung festgelegten Prüfverfahren erlassen wurde, geändert, ersetzt oder aufgehoben werden.

Folgenabschätzung

Mit dem Inkrafttreten der DSGVO sind Unternehmen unter bestimmten Voraussetzungen verpflichtet, eine Datenschutz-Folgenabschätzung (DSFA) vorzunehmen. Nach Artikel 35 Absatz 1 DSGVO ist eine DSFA grundsätzlich immer dann durchzuführen, wenn „(…) eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge“ hat.

Ferner werden in Artikel 35 Absatz 3 DSGVO Regelbeispiele genannt, bei denen eine Durchführungspflicht besteht:

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen,
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10,
- systematische, weiträumige Überwachung öffentlich zugänglicher Bereiche.

Diese Regelbeispiele ähneln stark der aus dem BDSG bekannten Vorabkontrolle. Aber der Text der DSGVO lässt weitgehend offen, wie und nach welchen Kriterien eine Datenschutz-Folgenabschätzung durchzuführen ist. Durch den relativ offenen Tatbestand des Artikels 35 Absatz 1 DSGVO wird aber auch Klärungsbedarf geschaffen, wann dieser denn nun genau erfüllt ist.

Die Aufsichtsbehörden müssen gemäß Artikel 35 Absatz 4 DSGVO im Rahmen ihres jeweiligen Zuständigkeitsbereichs eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die eine DSFA nach Absatz 1 durchzuführen ist. Artikel 35 Absatz 5 DSGVO enthält zudem eine Ermächtigung der Aufsichtsbehörden, eine Liste mit Arten von Datenverarbeitungsvorgängen zu erstellen und zu veröffentlichen, bei denen explizit keine Datenschutz-Folgenabschätzungen durchgeführt werden müssen. In Artikel 35 Absatz 7 DSGVO wird bestimmt, wie eine DSFA durchzuführen ist.

Umgang mit Datenpannen

Die DSGVO sieht eine verschärftere Meldepflicht bei Datenpannen („Data Breaches“) vor. In Artikel 33 DSGVO ist geregelt, wann eine Verpflichtung zur Meldung an die Aufsichtsbehörde beziehungsweise nach Artikel 34 DSGVO, wann eine Meldung an den Betroffenen zu erfolgen hat.

Zukünftig muss jede Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde gemeldet werden. Eine Beschränkung auf die oben bezeichneten Risikodaten kennt die DSGVO nicht.

Eine Ausnahme besteht nach Artikel 33 Absatz 1 DSGVO nur dann, wenn die Datenpanne voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Es ist also stets eine Risikoabwägung durchzuführen. Dabei sollte in jedem Falle der Risikokatalog des Erwägungsgrundes 75 DSGVO berücksichtigt und die Abwägung dokumentiert werden.

Ergibt die durchzuführende Risikoabwägung, dass durch die Datenpanne voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen besteht, sind diese Personen nach Artikel 34 DSGVO zu benachrichtigen. Ausnahmen von der Pflicht zur Benachrichtigung bestehen nach Artikel 34 Absatz 3 DSGVO, wenn

- geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen wurden, durch die die betroffenen Daten für Unbefugte nicht zugänglich sind (zum Beispiel Verschlüsselung),
- durch nachfolgende Maßnahmen sichergestellt wurde, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht,
- die direkte Information der Betroffenen mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall ist jedoch eine öffentliche Bekanntmachung gefordert.

Recht auf Vergessenwerden

Nach Artikel 17 Absatz 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden und der Verantwortliche ist dazu verpflichtet, sofern einer der folgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem EU-Recht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

Hat der Verantwortliche gemäß Artikel 17 Absatz 2 DSGVO die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so hat er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, zu treffen, um die datenverarbeitenden Einrichtungen und Personen darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

Die Rechtsnorm des Artikels 17 DSGVO knüpft an die Entscheidung des Europäischen Gerichtshofs (EuGH) zum Recht auf Vergessenwerden an[8], auch wenn der EuGH dieses Recht nicht erfunden hat, sondern er dies aus den allgemeinen Datenschutzgrundsätzen entwickelte.

Die Idee eines „digitalen Radiergummis“ hat sich jedoch nicht in der Form durchgesetzt, wie ursprünglich geplant. Somit werden mit der DSGVO einige gravierende datenschutzrechtliche Neuregelungen auf die Unternehmen zukommen. Der Gesetzgeber strebt eine Vereinheitlichung des Datenschutzstandards an, der für die EU-Mitgliedstaaten und unter gewissen Umständen auch für Nicht-EU-Staaten (zum Beispiel Großbritannien nach dem Brexit) bindend sein wird.

Es empfiehlt sich für verantwortliche Stellen, frühzeitig entsprechende Vorkehrungen zu treffen, um der neuen Rechtslage gerecht zu werden. Bei der Planung und Gestaltung der notwendigen Maßnahmen sollten Datenschutzbeauftragte, aber auch IT-Abteilungen eingebunden werden, um einen erfolgreichen Übergang zur DSGVO zu gewährleisten und sich vor den entsprechenden Sanktionen zu schützen. ◂

8) Vgl. EuGH C 131/12 vom 13. April 2016 „Google Spain“.