Dr. Thomas Müller, Frankfurt am Main

Datenschutz-Grundverordnung (DSGVO) – Umsetzung in der betrieblichen Praxis*

Am 4.5.2016 veröffentlichte die Europäische Union (EU) die Endfassung der seit 2012 verhandelten DSGVO. Sie gilt nach einer gut zweijährigen Übergangsfrist ab dem 25.5.2018 und hebt die Richtlinie 95/46/EG (Datenschutzrichtlinie) auf.

Bis zum 25.5.2018 müssen alle in Europa ansässigen Unternehmen ihre Verarbeitungspraxis an die neuen Regeln anpassen. Diese äußerst ungewöhnliche Breitenwirkung resultiert aus der Rechtsform, die der europäische Gesetzgeber für das Datenschutzwerk gewählt hat. Als Verordnung gilt die DSGVO unmittelbar und ohne das Erfordernis eines Umsetzungsaktes der Mitgliedstaaten (Art. 288 Abs. 2 AEUV). Dadurch soll eine möglichst weitreichende Vereinheitlichung des Datenschutzrechtes in der gesamten EU erreicht werden[1].

Aufgrund der unmittelbaren Geltung für alle Unternehmen müssen auch Einrichtungen der betrieblichen Altersversorgung die Auswirkungen dieser Verordnung auf ihre Systeme prüfen. So werden u.a. intensive Dokumentationspflichten, die Implementierung weiterer technischer und organisatorischer Maßnahmen sowie die Berücksichtigung einer Vielzahl an Betroffenenrechten angeordnet. Die DSGVO sieht insbesondere folgende Neuerungen vor:

- Massiv erweiterte Sanktionen (bis 20 Millionen Euro oder bis zu 4 Prozent des weltweiten Vorjahresumsatzes)
- Erweiterte Haftungsrisiken
- Neue Fristen und Transparenzpflichten
- Verschärfte Notifikationspflichten bei Datenschutzverstößen (72-Stunden-Frist)
- Erfordernis einer auf einer Risikoanalyse basierenden Datenschutz-Folgenabschätzung
- „Privacy by Design" und „Privacy by Default"
- Neue Anforderungen an das Verfahrensverzeichnis
- Erweiterte Informations- und Hinweispflichten
- Erweiterte Betroffenenrechte (z.B. Recht auf Portabilität der Daten)
- Neue Anforderungen an die Einwilligung
- Neue Anforderungen an die Auftragsverarbeitung

Im Einzelfall müssen ggf. umfassende neue Strukturen und Prozesse geschaffen werden, um den Vorgaben der DSGVO zu entsprechen.

* Vortrag gehalten auf der Tagung der Fachvereinigung Pensionskassen am 21.9.2017 in Mannheim.

1 Vgl. Erwägungsgrund 9 DSGVO.

27 vgl. hierzu *Berenz*, a.a.O. (Fn. 8), Rn. 4-6 zu § 8.

I. Überblick über die Vorschriften der DSGVO

Das *erste Kapitel* (Art. 1-4 DSGVO) beschäftigt sich mit Gegenstand und Ziel der Verordnung sowie dem sachlichen und räumlichen Anwendungsbereich und enthält in Art. 4 DSGVO wichtige Legaldefinitionen. Im *zweiten Kapitel* (Art. 5-8 DSGVO) werden die Grundsätze der Verordnung erläutert. Die zentrale Bestimmung ist hier Art. 5 DSGVO, der die Grundsätze für eine rechtmäßige Datenverarbeitung festlegt und zur Auslegung unbestimmter Rechtsbegriffe heranzuziehen ist. Das sind u.a. Rechtmäßigkeit der Datenverarbeitung (Verbot mit Erlaubnisvorbehalt), Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie die Rechenschaftspflicht.

Eine weitere bedeutsame Vorschrift im zweiten Kapitel ist der Art. 6 DSGVO. Dieser enthält die wichtigsten Erlaubnistatbestände im Umgang mit personenbezogenen Daten. Sofern sensitive Daten betroffen sind (besondere Kategorien), ist Art. 9 DSGVO einschlägig. Dieser stellt einen eigenständigen Erlaubnistatbestand für die Verarbeitung von Daten dar[2]. Art. 7 bestimmt die näheren Voraussetzungen für die Einwilligung des Betroffenen. Sie muss grundsätzlich ohne Zwang abgegeben werden und ist nunmehr frei widerrufbar. Das *dritte Kapitel* beschreibt die Rechte der betroffenen Personen (Art. 12-23 DSGVO). Das sind u.a. transparente Information und Kommunikation gegenüber betroffenen Personen (Art. 12 DSGVO), Informationspflichten bei Datenerhebung (Art. 13, 14 DSGVO), Auskunftsrechte der betroffenen Personen (Art. 15 DSGVO), das Recht auf Berichtigung (Art. 16 DSGVO), das Recht auf Löschung (Art. 17 DSGVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO), das Recht auf Datenübertragbarkeit (Art. 20 DSGVO), Widerspruchsrechte (Art. 21 DSGVO), Profiling und andere automatisierte Einzelentscheidungen (Art. 22 DSGVO). *Kapitel vier* beschäftigt sich mit Verantwortlichen und Auftragsverarbeitern (Art. 24-43 DSGVO). Die Übermittlung personenbezogener Daten in Drittländer findet sich im *fünften Kapitel* (Art. 44-50 DSGVO). Die Aufgaben, Rechte und Pflichten der Aufsichtsbehörden sind in den *Kapiteln sechs und sieben* (Aufsichtsbehörden Art. 51-76 DSGVO) verortet. *Kapitel acht* (Art. 77-84 DSGVO) listet Regelungen zu Rechtsbehelfen, Haftung und Sanktionen auf. Das *Kapitel neun* (Art. 85-91 DSGVO) enthält Vorschriften für besondere Verarbeitungssituationen, z.B. zur Verarbeitung personenbezogener Daten und zur Freiheit der Meinungsäußerung sowie der Informationsfreiheit gem. Art. 85 DSGVO. Die Befugnisse der Kommission zum Erlass delegierter Rechtsakte und von Durchführungsrechtsakten finden sich in *Kapitel zehn* (Art. 92, 93 DSGVO). Das *elfte Kapitel* (Art. 94-99 DSGVO) enthält die Schlussbestimmungen. Hier ist vor allem Art. 99 DSGVO von Bedeutung, der bestimmt, dass die Verordnung ab dem 25.5.2018 verbindlich gilt.

II. Anwendungsbereich

1. Sachlicher Anwendungsbereich

Gem. Art. 2 Abs. 1 DSGVO gilt die Verordnung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden[3]. Unerheblich ist, ob die Verarbeitung vollständig oder nur teilweise automatisiert stattfindet. Schutzgut sind damit auch weiterhin „personenbezogene Daten", die Art. 4 Nr. 1 DSGVO definiert als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen".

Zudem findet die Verordnung auf die nichtautomatisierte Verarbeitung von personenbezogenen Daten Anwendung, die bereits in einer Datei gespeichert sind oder noch gespeichert werden sollen. Unter Verarbeitung wird nach der Definition in Art. 4 Nr. 2 DSGVO jeder personenbezogene Daten betreffende Vorgang erfasst, beginnend mit der Erhebung und der mit dem Löschen bzw. Vernichtung endet. Damit ist der sachliche Anwendungsbereich der Verordnung in der Praxis weit gefasst.

2. Räumlicher Anwendungsbereich

Art. 3 DSGVO normiert den räumlichen Anwendungsbereich der DSGVO. Gem. Art. 3 Abs. 1 DSGVO ist der Geltungsbereich der DSGVO eröffnet, wenn ein Verantwortlicher oder Auftragsverarbeiter eine Niederlassung in der Union unterhält und im Rahmen der Tätigkeit dieser Niederlassung personenbezogene Daten verarbeitet. In Art. 3 Abs. 2 DSGVO wird darüber hinaus das sog. Marktortprinzip eingeführt. Danach gilt die DSGVO auch für Unternehmen mit Sitz in einem Drittland, wenn diese Waren und Dienstleistungen in der EU anbieten oder das Verhalten von Privatpersonen in der EU verfolgen. Mit der Verhaltensbeobachtung (Art. 3 Abs. 2 a) DSGVO) sollen vor allem Tätigkeiten erfasst werden, bei denen Internetaktivitäten der betroffenen Personen nachvollzogen werden. Große Bedeutung hat diese Regelung bei Cloud-Angeboten. Ist ein Cloud-Anbieter außerhalb der EU niedergelassen und erbringt er für einen Cloud-Nutzer, der sich in der Union befindet, eine Dienstleistung, so gilt die DSGVO für den Cloud-Anbieter unmittelbar[4]. Die DSGVO entfaltet ihre Rechtswirkung selbst dann, wenn eine Rechtswahlklausel vorliegt, denn der räumliche Anwendungsbereich ist durch Rechtswahlklauseln nicht abdingbar[5].

III. Wichtige Änderungen im Überblick

1. Schadensersatzansprüche / Behördenvollzug der DSGVO

Gem. Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder den Auftragsverarbeiter. Art. 82 DSGVO ist ein eigenständiger, direkt geltender deliktsrechtlicher Anspruch, der dem allgemeinen zivilrechtlichen Regime unterliegt[6]. Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit der Verordnung nicht im Einklang steht, sind danach von dem Verantwortlichen oder dem hierfür verantwortlichen Auftragsverarbeiter zu ersetzen, es sei denn, dass diese von der Haftung befreit werden, weil sie nachweisen, dass sie in keiner Weise für den Schaden verantwortlich sind. Materielle Schäden sind alle zurechenbaren Nachteile, die der Geschädigte an seinem

2 *Steinhaus/Böhm* in: Wybitul, EU-Datenschutz-Grundverordnung, 2017, Art. 9 Rn. 6.

3 Im Unterschied zum BDSG (Bundesdatenschutzgesetz), bei dem der Schutz des Persönlichkeitsrechts lediglich ein gesetzgeberisches Ziel ausgibt (§ 1 Abs. 1 BDSG), verfolgt die EU seit jeher zwei Anliegen: Zum einen sind das der Schutz der Grundrechte und Grundfreiheiten und insbesondere der Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum anderen der freie Verkehr personenbezogener Daten zwischen den Mitgliedstaaten. Zahlreiche Erwägungsgründe der DSGVO verdeutlichen, dass die DSGVO in dieser Kontinuität zu diesen Anliegen steht; vgl. *Pötters* in: Gola, Datenschutz-Grundverordnung: DS-GVO, VO (EU) 2016/679, Kommentar, 2017, Art. 1 Rn. 1-4.

4 *Klar* in: Kühling/Buchner, DS-GVO, Kommentar, 2017, Art. 3 Rn. 88.

5 *Klar*, a.a.O. (Fn. 4), Art. 3 Rn. 105.

6 *Neun/Lubitzsch*, Die neue EU-Datenschutz-Grundverordnung – Rechtsschutz und Schadensersatz, BB 2017 S. 2563 ff. (2567).

Vermögen erlitten hat. Genannt wird z.B. die Verweigerung eines Kreditvertrages aufgrund falscher Bonitätswerte[7]. Mit dem in Art. 82 Abs. 1 DSGVO zusätzlich genannten Ersatz des immateriellen Schadens ist die Beeinträchtigung des Persönlichkeitsrechtes gemeint, etwa in Form von psychischen Auswirkungen. Seit dem sog. Herrenreiterurteil des BGH aus dem Jahre 1958[8] ist in Deutschland geltendes Recht, dass nicht jede Verletzung des Persönlichkeitsrechts zu einem Anspruch auf Geldentschädigung führt, sondern nur, wenn es sich um einen schwerwiegenden Eingriff handelt und die Beeinträchtigung nicht auf andere Weise befriedigend ausgeglichen werden kann. Ob diese Rechtsprechung weiterhin Bestand haben wird, bleibt abzuwarten. Art. 82 Abs. 3 DSGVO sieht hinsichtlich des Nachweises des Verschuldens eine Umkehr der Beweislast vor, d.h., das schuldhafte Verhalten wird vermutet, von dem sich der Verantwortliche oder der Auftragsverarbeiter entlasten kann, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Die DSGVO statuiert in Art. 58 Abs. 2 i) DSGVO die Befugnis der Aufsichtsbehörde zur Verhängung von Geldbußen „zusätzlich zu oder anstelle von" den übrigen dort genannten Maßnahmen[9]. Nach Art. 83 Abs. 1 DSGVO stellt die Aufsichtsbehörde sicher, dass die Verhängung von Bußgeldern in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. Die Geldbußen werden (Art. 83 Abs. 2 S. 1 DSGVO) je nach den Umständen des Einzelfalles verhängt. Art. 83 Abs. 2 S. 2 DSGVO legt Kriterien fest, die bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag im Einzelfall zu berücksichtigen sind. Das sind Art, Schwere und Dauer von Verstößen, Zahl der betroffenen Personen sowie ob vorsätzliches oder fahrlässiges Handeln vorlag. Ein weiteres Kriterium ist der Umfang der Zusammenarbeit mit den Aufsichtsbehörden. Dies verdeutlicht, dass das Verhältnis zwischen Aufsichtsbehörde und Verantwortlichen von Mitwirkung und Kooperation geprägt sein sollte[10]. Art. 83 Abs. 3 DSVO legt als Adressat der Geldbuße den Verantwortlichen oder den Auftragsverarbeiter fest. Als tauglicher Täter kommen neben natürlichen auch juristische Personen in Betracht, was sich aus den Definitionen der Begriffe „Verantwortlicher" sowie „Auftragsverarbeiter" (Art. 4 Nr. 7, 8 DSGVO) ableitet. Aus europäischer Sicht erfolgt keine Trennung zwischen der Tatbestandsseite und dem Haftungsadressaten auf der Rechtsfolgenseite, sodass die Haftung dem gesamten Unternehmen zugewiesen und in Form von Geldbußen auferlegt werden kann[11]. Der maximale Geldbetrag kann bis zu 20 Millionen Euro oder bis zu 4% des gesamten weltweit erzielten Jahresumsatzes des Unternehmens im vorangegangenen Geschäftsjahr liegen, je nachdem, welcher Wert der höhere ist.

2. Accountability (Nachweispflicht)

Eine der bedeutsamen Neuregelungen im Datenschutzrecht steht in Art. 5 Abs. 2 DSGVO. Der Verantwortliche ist für die Einhaltung (der Grundsätze für die Verarbeitung personenbezogener Daten) des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (Rechenschaftspflicht). Ergänzt wird der Grundsatz der Rechenschaftspflicht durch die Regelungen des Art. 24 Abs. 1 S. 1 DSGVO. Dieser schreibt vor: *„Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert."* Datenverarbeitende Unternehmen sind mithin zur Implementierung risikoangemessener technisch-organisatorischer Datenschutz- und Datensicherheitsmaßnahmen verpflichtet.

Die in diesen Bestimmungen statuierte Rechenschaftspflicht führt zu einer Umkehr der Beweislastverteilung im Verhältnis zu den Aufsichtsbehörden und betroffenen Personen. Im Rahmen eines aufsichtsbehördlichen Verfahrens oder bei einem Gerichtsprozess muss künftig nicht die Behörde oder der Kläger den Nachweis führen, dass das Unternehmen die Daten ohne die erforderliche Rechtsgrundlage verarbeitet oder unzureichende Sicherheitsvorkehrungen etabliert hat, sondern es ist das Unternehmen, das ausreichende Belege für sein datenschutzkonformes Verhalten vorlegen muss[12].

Um die in den Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO geforderten Nachweise erbringen zu können, ist es erforderlich, alle datenschutzrelevanten Vorgänge im Unternehmen sorgfältig zu dokumentieren und Datenschutz im Unternehmen zu organisieren. „Ziel muss es sein,

- alle datenschutzrelevanten Vorgänge im Unternehmen und die daraus resultierenden Datenschutzrisiken zu identifizieren,
- risikoangemessene Sicherheitsmaßnahmen und Handlungsanleitungen zu implementieren,
- die Einhaltung und Umsetzung dieser Maßnahmen und Anleitungen effektiv zu kontrollieren und
- Defizite in der Datenschutzorganisation frühzeitig zu erkennen und zu beseitigen"[13].

Vor diesem Hintergrund empfiehlt es sich, ein Datenschutzmanagementsystem nach dem Vorbild von Compliance-Management-Systemen zu implementieren.

3. Rechte der betroffenen Personen

Ein wichtiges weiteres Ziel der Neuregelung des europäischen Datenschutzrechts ist der Ausbau der Betroffenenrechte. Unter Betroffenenrechten – oder unter „Rechten der betroffenen Person" (so der Terminus der DSGVO) –, versteht das Datenschutzrecht die Rechte jedes Einzelnen gegenüber den für die Verarbeitung Verantwortlichen.

Die Grundverordnung sieht in den Art. 13 DSGVO (Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person) und Art. 14 DSGVO (Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden) erweiterte, teilweise über die bisherigen Pflichten des BDSG erheblich hinausgehende Informationspflichten vor. So hat der Verantwortliche bei Direkterhebung der Daten gem. Art. 13 DSGVO u.a. über die Zwecke und Grundlagen der Datenerhebung zu informieren.

Der für die Verarbeitung Verantwortliche hat ferner über die Dauer der Speicherung oder falls dies nicht möglich ist, über die Kriterien der Festlegung der Dauer zu informieren. Zu informieren ist zudem über Betroffenenrechte wie Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs- und Widerspruchsrechte sowie das Recht auf Datenübertragbarkeit. Der Betroffene muss bei Erteilung der Einwilligung darauf hingewiesen werden, dass er diese jederzeit widerrufen kann, ohne dass die Rechtmäßigkeit der bis dahin

7 *Gola/Piltz* in: Gola, a.a.O. (Fn. 3), Art. 82 Rn. 11.
8 BGH, Urteil vom 14.2.1958, I ZR 151/56.
9 Insgesamt 26 konkrete Befugnisse wie etwa der Verwarnung etc.
10 *Neun/Lubitzsch*, EU-Datenschutz-Grundverordnung- Behördenvollzug und Sanktionen, BB 2017 S. 1538 ff. (1541).
11 *Neun/Lubitzsch*, a.a.O. (Fn. 10), S. 1541.
12 *Hamann*, Europäische Datenschutz-Grundverordnung – neue Organisationspflichten für Unternehmen, BB 2017 S. 1090 ff. (1092).
13 *Hamann*, a.a.O. (Fn. 12), S. 1092.

vorgenommenen Verarbeitung entfällt. Er ist zudem über seine Beschwerderechte bei der Aufsichtsbehörde in Kenntnis zu setzen. Möchte der für die Verarbeitung Verantwortliche Daten für einen anderen Zweck weiterverarbeiten, als er die Daten ursprünglich erhoben hat, so muss er ab Geltung der Verordnung die betroffenen Personen vor der Weiterverarbeitung über diesen anderen Zweck informieren.

Art. 15 DSGVO regelt die Auskunftsrechte der betroffenen Person. Die betroffene Person hat ein Recht zu erfahren, ob ein für die Verarbeitung Verantwortlicher sie betreffende personenbezogene Daten verarbeitet. Soweit dies der Fall ist, hat die betroffene Person weiter ein Recht auf Auskunft über die Umstände der Datenverarbeitung. Art. 15 DSGVO erweitert den Anspruchsumfang auf die geplante Dauer der Speicherung, die Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden, und das Vorliegen einer automatisierten Entscheidungsfindung einschließlich Profiling.

In Art. 17 DSGVO ist das Recht auf Löschung beschrieben. Gemäß Abs. 1 hat die betroffene Person das Recht, von dem Verantwortlichen zu verlangen, dass die betreffenden personenbezogenen Daten unverzüglich gelöscht werden, sofern einer der folgenden Gründe zutrifft[14]:

- die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder in sonstiger Weise verarbeitet wurden, nicht mehr notwendig (Abs. 1a);
- die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gem. Art. 6 Abs. 1 a) DSGVO stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung (Abs. 1b);
- Widerspruch gegen die Verarbeitung und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor (Abs. 1c);
- die personenbezogenen Daten wurden unrechtmäßig verarbeitet (Abs. 1d);
- die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt (Abs. 1e);
- die personenbezogenen Daten wurden in Bezug auf angebotene Dienste einer Informationsgesellschaft gem. Art. 8 Abs. 1 DSGVO erhoben (Abs. 1f).

Auslegungsbedürftig ist im Rahmen des Art. 17 DSGVO, was mit „unverzüglicher" Löschung gemeint ist. Zum Teil wird die Auffassung vertreten, dass das Tatbestandsmerkmal „unverzüglich" eine Verschärfung gegenüber den allgemeinen Bestimmungen des Art. 12 Abs. 4 DSGVO darstelle, folglich müsse grundsätzlich ein Tätigwerden innerhalb von zwei Wochen erfolgen. Die wohl überwiegende Meinung geht von einer Frist von einem Monat aus, wobei diese in komplexen Fällen um zwei Monate verlängert werden könne (Art. 12 Abs. 3 S. 2 DSGVO)[15].

Die Löschrechte in Abs. 1 werden durch Abs. 2 ergänzt, indem der zur Löschung verpflichtete Verantwortliche im Falle der Veröffentlichung von personenbezogenen Daten angemessene Maßnahmen zu ergreifen hat, um Dritte über das ihnen gegenüber bestehende Löschungsverlangen der betroffenen Person in Kenntnis zu setzen[16].

Art. 20 DSGVO regelt das Recht auf Datenübertragbarkeit. Betroffene haben das Recht, die sie betreffenden personenbezogenen Daten, die sie einem für die Verarbeitung Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie haben das Recht, diese Daten einem anderen für die Verarbeitung Verantwortlichen ohne Behinderung durch den für die Verarbeitung Verantwortlichen, dem die Daten bereitgestellt wurden, zu übermitteln. Dieses Recht soll dann bestehen, wenn eine automatisierte Datenverarbeitung zur Durchführung eines Vertrags erfolgte oder auf einer Einwilligung basierte. Der Anspruch aus Art. 20 DSGVO beinhaltet darüber hinaus auch das Recht zu erwirken, dass die Daten direkt von einem für die Verarbeitung Verantwortlichen einem anderen für die Verarbeitung Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

Abgerundet wird das Kapitel der Betroffenenrechte in der DSGVO durch das Widerspruchsrecht in Art. 21, das Recht auf Einschränkung der Verarbeitung in Art. 18 und das Recht auf Berichtigung in Art. 16.

4. Datenschutz-Folgenabschätzung

Die DSGVO verpflichtet in Artikel 35 die Verantwortlichen, eine Datenschutz-Folgenabschätzung (DSFA) vorzunehmen, wenn ein „voraussichtlich hohes Risiko" mit der Verarbeitung von Daten verbunden ist. Sie ist ein Instrument, um die Risiken einzelner Datenverarbeitungsvorgänge für den Datenschutz von Betroffenen im Vorhinein zu identifizieren und zu bewerten[17].

Die Datenschutz-Folgenabschätzung (DSFA) ersetzt die bisherige Vorabkontrolle nach § 4d Abs. 5, 6 BDSG. Im Gegensatz zur Vorabkontrolle liegt die Datenschutzfolgeabschätzung in der Verantwortung der Unternehmensleitung und nicht beim Datenschutzbeauftragten. In Art. 35 Abs. 3 DSGVO werden einige Fälle aufgezählt, in denen in jedem Fall eine Datenschutz-Folgenabschätzung durchzuführen ist. In diesem Kontext ist auf ein wichtiges Arbeitspapier der Artikel-29-Datenschutzgruppe hinzuweisen. Dieses Arbeitspapier ist von großer Bedeutung, da die Artikel-29-Datenschutzgruppe sich aus Vertretern der Aufsichtsbehörden der Mitgliedstaaten zusammensetzt. Diese Behörden sollen durch die Erstellung von Positiv- und Negativlisten klarstellen, wann eine DSFA durchzuführen ist. Die Leitlinien sehen vor, dass die Verantwortlichen in bestimmten Fällen die unbedingte Pflicht haben, eine Folgenabschätzung durchzuführen. Diese Pflicht besteht *„where a processing is likely to result in a high risk to the rights and freedoms of natural persons"*. Um das Vorliegen eines solchen „hohen Risikos" zu konkretisieren, werden zehn Kriterien aufgelistet. Je mehr von diesen zutreffen, desto wahrscheinlicher ist das Vorliegen eines hohen Risikos. Als Faustregel dabei gilt, dass eine Folgenabschätzung bei Erfüllung von zwei oder mehr Kriterien durchgeführt werden muss[18]. Darüber hinaus sieht Art. 35 Abs. 4 DSGVO ein aufsichtsrechtliches Recht zur Erstellung einer Liste von Verarbeitungsvorgängen vor, für die Datenschutz-Folgeabschätzungen verpflichtend sind (Black-List). Art. 35 Abs. 5 DSGVO gibt den Aufsichtsbehörden auf der anderen Seite das Recht, Verarbeitungsvorgänge zu nennen, bei denen generell keine Datenschutz-Folgeabschätzung durchzuführen ist (White-List)[19]. In Zweifelsfällen ist die Aufsichtsbehörde zu kontaktieren (Art. 36 DSGVO).

14 Instruktiv hierzu *Hennemann*, Das Recht auf Löschung gem. Art. 17 Datenschutz-Grundverordnung, PinG 2016 S. 176 ff.
15 So etwa *Kamann/Braun* in: Ehmann/Selmayr, Datenschutz-Grundverordnung: DS-GVO, Kommentar, 2017, Art. 17 Rn. 37.
16 *Nolte/Werkmeister* in: Gola, a.a.O. (Fn. 3), Art. 17 Rn. 33.
17 Vgl. White Paper DATENSCHUTZ-FOLGENABSCHÄTZUNG. Ein Werkzeug für einen besseren Datenschutz.
18 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.
19 *Bausewein/Steinhaus* in: Wybitul, a.a.O. (Fn. 2), Art. 35 Rn. 5.

5. Auftragsverarbeiter

Die zentrale Vorschrift für Auftragsverarbeiter in der DSGVO ist Art. 28, wo in Absatz 1 zunächst die Prüfung der Geeignetheit eines Auftragsverarbeiters eingefordert wird. Der Verantwortliche darf danach nur Auftragsverarbeiter einsetzen, die hinreichende Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz vorhalten. Als Beleg solcher Garantien können genehmigte Verhaltensregeln des Auftragsverarbeiters nach Art. 40 DSGVO oder Zertifizierungen nach Art. 42 DSGVO dienen.

6. Verhaltensregeln und Zertifizierungen

Bekanntlich sah § 38a BDSG die Möglichkeit vor, mit der Datenschutzaufsichtsbehörde Verhaltensregeln abzustimmen. In der Praxis fand diese Regelung jedoch kaum Anwendung. Das dürfte sich mit der DSGVO ändern, da genehmigte Verhaltensregeln eine besondere Bedeutung erlangen. Die Verhaltensregeln sollen entsprechend den Besonderheiten der einzelnen Verarbeitungsbereiche zur ordnungsgemäßen Anwendung der DSGVO beitragen. Die DSGVO sieht im Art. 40 Abs. 2 DSGVO einen Katalog an Maßnahmen vor, der zu einer solchen Präzisierung führen kann. Dabei können Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder von Auftragsverarbeitern vertreten, solche Verhaltensregeln ausarbeiten, ändern oder erweitern und nach einem in Art. 40 Abs. 5 DSGVO festgelegten Verfahren von der Datenschutzaufsichtsbehörde genehmigen lassen.

Daneben gibt es die Möglichkeit der Zertifizierung. Zertifizierungsverfahren haben den Zweck, die Transparenz der Datenverarbeitung zu erhöhen, die Einhaltung der DSGVO zu verbessern und den betroffenen Personen einen raschen Überblick über das Datenschutzniveau von Produkten und Dienstleistungen zu geben. Zertifizierungen beziehen sich nicht auf das Unternehmen an sich, sondern jeweils nur auf einzelne Verarbeitungsvorgänge. Diesbezüglich können sie nachweisen, dass das Unternehmen die Anforderungen der DSGVO sowie der technisch organisatorischen Maßnahmen einhält.

Zertifizierungen werden entweder von der Datenschutzaufsichtsbehörde oder von Zertifizierungsstellen ausgestellt, die in einem in Art. 43 DSGVO festgelegten Akkreditierungsverfahren entweder von der zuständigen Datenschutzaufsichtsbehörde oder einer nationalen Akkreditierungsstelle im Sinne der EU-Akkreditierungs- und Marktüberwachungsverordnung akkreditiert wurden.

IV. Projektplanung

Um die DSGVO erfolgreich umzusetzen, sollte in einem ersten Schritt die Sammlung sämtlicher datenschutzrechtlich relevanter Dokumente, Prozesse oder IT-Systeme (Erhebung, Nutzung oder Speicherung von personenbezogenen Daten) erfolgen (Bestandsaufnahme). Dieser Schritt ist für den Verlauf des gesamten folgenden Projekts und die angestrebte Rechtskonformität mit der EU-DSGVO essentiell. In einem zweiten Schritt empfiehlt es sich, die gesammelten Dokumente, Prozesse und IT-Systeme rechtlich zu bewerten. Im Rahmen einer sog. GAP-Analyse sollte ein Soll-Ist-Vergleich erfolgen, um ggf. erforderlichen Anpassungsbedarf herauszuarbeiten. Ein möglichst aktuelles Verarbeitungsverzeichnis kann ein wertvoller Ausgangspunkt zur Identifizierung sein. Wegen des gegenüber dem BDSG deutlich stärker risikobasierten Ansatzes der DSGVO kommen neben der Nutzung bereits bestehender Datenschutzstrukturen auch die Adaption von Prozessen und Strukturen eines bestehenden Compliancemanagements oder Qualitätsmanagementsystems in Betracht. Vor allem aufgrund der steigenden Bußgeld- und Reputationsverlustrisiken sowie künftig drohender Schadensersatzforderungen betroffener Personen ist eine auf das gesamte Unternehmen und die einzelnen Geschäftsbereiche bezogene Risikoanalyse empfehlenswert. Schließlich erfolgt die konkrete Umsetzung des identifizierten Anpassungsbedarfs. Im Rahmen der Projektplanung ist ausreichend Zeit für diesen Schritt einzuplanen. Die betroffenen Abteilungen im Unternehmen sind zur Mitarbeit anzuhalten. Ziel ist es, zum 25. Mai 2018 den Anforderungen der EU-DSGVO zu genügen.