Whitepaper Datenschutzgrundverordnung

Inhalt

1. Einleitung

Die EU-Datenschutzgrundverordnung (**DSGVO**) tritt am 25. Mai 2018 als unmittelbar in den Mitgliedsstaaten geltendes Recht in Kraft und löst die Richtlinie 95/46/EG (**Datenschutzrichtlinie 1995**) vollständig ab. Mit der DSGVO wird das europäische Datenschutzrecht stark vereinheitlicht, es bleiben aber auch relevante Spielräume für die Mitgliedsstaaten zur Ergänzung der Regelungen durch nationale Datenschutzregelungen. Diese sind in der DSGVO in zahlreichen Öffnungsklauseln vorgesehen, etwa für den Beschäftigtendatenschutz.

Die DSGVO entwickelt das europäische Datenschutzrecht auf Grundlage der Datenschutzrichtlinie 1995 weiter, ohne es zu revolutionieren. Viele Anforderungen der DSGVO sind daher vor dem Hintergrund der aktuellen deutschen Regelung im Bundesdatenschutzgesetz (**BDSG-alt**) für den Rechtsanwender im Grundsatz bekannt. Die beste Vorbereitung auf die DSGVO ist daher aus der Perspektive des deutschen Adressaten eine funktionierende Datenschutz-Organisation auf Basis des BDSG-alt, die allerdings längst nicht in allen deutschen Unternehmen vollständig vorhanden ist.

Zudem gibt es relevante Neuerungen in der DSGVO, so dass eine Überprüfung und Anpassung der aktuellen Datenschutz-Organisation für jedes Unternehmen dringend angezeigt ist. Dies gilt besonders, wenn das Thema Datenschutz bisher noch nicht sehr hoch auf der Agenda steht. So werden mit der DSGVO insbesondere Informations-, Dokumentations- und Rechtfertigungspflichten verschärft. Es empfiehlt sich daher, die DSGVO zum Anlass zu nehmen, um das Thema Datenschutz für das eigene Unternehmen bzw. die eigene Behörde zu priorisieren.

2. Anwendungsbereich der DSGVO und nationales Datenschutzrecht

Neu und wichtig	Das ist zu tun
• Die DSGVO ersetzt das BDSG-alt und die Datenschutzrichtlinie 1995. • Der Anwendungsbereich des europäischen Datenschutzrechts wird erweitert. • Mitgliedsstaaten können nationale Regelungen schaffen, um Öffnungsklauseln zu konkretisieren. • In Deutschland ist dafür das Datenschutz Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU (**BDSG-neu**) verabschiedet worden.	• Prüfen, ob das eigene Unternehmen in den Anwendungsbereich der DSGVO fällt (insbesondere Unternehmen außerhalb der Union). • Änderungen datenschutzrechtlicher Anforderungen durch DSGVO und nationale Regelungen analysieren. • Die Datenschutz-Organisation an neue Regelungen anpassen.

2.1. Anwendungsbereich der DSGVO

Die DSGVO findet Anwendung, wenn

- personenbezogene Daten durch verantwortliche Stellen oder deren Niederlassung innerhalb der Union verarbeitet werden, oder
- personenbezogene Daten über Personen in der Union verarbeitet werden, um ihnen Waren oder Dienstleistungen anzubieten (sog. Marktortprinzip) oder deren Verhalten zu beobachten.

Insbesondere das Marktortprinzip erweitert die Anwendbarkeit des europäischen Datenschutzrechts stark. Auch Unternehmen außerhalb der Union sollten daher prüfen, ob sie in den Anwendungsbereich der DSGVO fallen und eine DSGVO-konforme Datenschutz-Organisation benötigen.

2.1.1. Datenverarbeitung im Zusammenhang mit Niederlassungen in der EU

Wie ihre Vorgängerregelung findet die DSGVO Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese „im Rahmen der Tätigkeiten" einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der EU erfolgt (Art. 3 Abs. 1 DSGVO).

Der Begriff "im Rahmen der Tätigkeiten" wurde durch den Europäischen Gerichtshof (**EuGH**) im Urteil "Google Spain" (Aktenzeichen C-131/12) weit ausgelegt. Der EuGH vertrat in dieser Entscheidung die Auffassung, dass die Tätigkeiten der Google Inc. (USA) der spanischen Niederlassung von Google zuzurechnen sind, auch wenn diese Niederlassung nur für den Verkauf von Werbeflächen innerhalb des Suchmaschinendienstes zuständig und technisch nicht in die Suchmaschinenfunktion involviert ist. Angesichts dieses Urteils kann die Datenverarbeitung von Nicht-EU-Verantwortlichen schon unter die Datenschutzrichtlinie 1995 fallen. Dies gilt erst Recht für die DSGVO.

2.1.2. Verarbeitung von Daten über Personen in der Union (Marktortprinzip)

Auch wenn die Datenverarbeitung nicht durch einen Verantwortlichen oder eine Niederlassung in der Union ausgeübt wird, kann ein Verantwortlicher in den Anwendungsbereich der DSGVO fallen. Nach dem in Art. 3 Abs. 2 DSGVO verankerten Marktortprinzip ist die DSGVO anwendbar, wenn eine Datenverarbeitung Personen innerhalb der EU betrifft und im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen an diese Personen steht oder der Beobachtung eines Verhaltens in der Union dient. Diese Regelung zielt insbesondere auf Internetsachverhalte ab und wird etwa relevant, wenn eCommerce-Angebote in der Union unterbreitet werden oder das Surfverhalten europäischer User getrackt wird.

2.2. Nationales Datenschutzrecht und DSGVO

Die DSGVO wird die aktuellen nationalen Datenschutzgesetze der Mitgliedstaaten weitgehend ersetzen, so dass hinsichtlich der Verarbeitung personenbezogener Daten die Regelungen der DSGVO grundsätzlich vorrangig sind.

Die DSGVO enthält jedoch auch Öffnungsklauseln, die den Mitgliedstaaten Spielräume für nationale Spezialregelungen eröffnen, z.B. in Bezug auf den Beschäftigtendatenschutz. In anderen Fällen wird den Mitgliedstaaten zumindest ermöglicht, die Regelungen der DSGVO zu spezifizieren, z.B. in Bezug auf die Rechtfertigungen der Datenverarbeitung.

Der deutsche Gesetzgeber hat auf Bundeseben das BDSG-neu erlassen (Datenschutz Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), mit dem die Öffnungsklauseln der DSGVO ausgefüllt und insbesondere für Verantwortliche in Deutschland von der DSGVO abweichende Spezialregelungen getroffen werden. Das BDSG-neu gilt für nicht-öffentliche Stel-

len und die öffentliche Stellen des Bundes. Wie bisher, können die Länder eigene Landesdatenschutzgesetze erlassen und darin insbesondere die Datenverarbeitung durch öffentliche Stellen der Länder regeln.

Trotz der erstrebten Rechtsvereinheitlichung durch eine direkt anwendbare DSGVO bleibt das Datenschutzrecht der Mitgliedsstaaten und im Fall von Deutschland das Landesrecht eine wichtige datenschutzrechtliche Rechtsquelle, die neben der DSGVO für den Aufbau einer Datenschutz-Organisation zu beachten ist.

3. Grundsätze und Rechenschaftspflicht

Neu und wichtig	Das ist zu tun
• Grundsätze der Datenverarbeitung werden ausdrücklich, ausführlich und „vor die Klammer gezogen" geregelt. • Mit der DSGVO wird eine allgemeine und umfassende Rechenschaftspflicht eigeführt.	• Grundsätze der Datenverarbeitung für Gestaltung der Datenschutz-Organisation beachten. • Für Maßnahmen der Datenschutz-Organisation und Datenverarbeitungen eine angemessene Dokumentation schaffen, mit der die Einhaltung datenschutzrechtlicher Anforderungen nachgewiesen werden kann.

3.1. Grundsätze der Verarbeitung personenbezogener Daten

„Vor die Klammer gezogen" finden sich in Art. 5 DSGVO Grundsätze, die Verantwortliche bei der Verarbeitung personenbezogener Daten zu beachten haben. Die sind

- Rechtmäßigkeit der Datenverarbeitung,
- Verarbeitung nach Treu und Glauben,
- Transparenz der Datenverarbeitung,
- Zweckbindung,
- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung,
- Integrität und Vertraulichkeit und
- Rechenschaftspflicht des Verantwortlichen.

Diese Grundsätze knüpfen an die Vorgängerregelung in Art. 6 Datenschutzrichtlinie 1995 an und sind insbesondere bei der Auslegung von Erlaubnistatbeständen der DSGVO relevant. Unternehmen sollten die Grundsätze in Art. 5 DSGVO bei der Konzeption ihrer Datenschutz-

Compliance-Organisation als Orientierungshilfe verstehen und beherzigen. Konkrete Anforderungen an die Gestaltung von Verfahren zur Verarbeitung personenbezogener Daten ergeben sich jedoch in erster Linie aus den Erlaubnistatbeständen.

3.2. Rechenschaftspflicht

Durch Art. 5 Abs. 2 DSGVO wird eine neue Pflicht für Verantwortliche eingeführt, die künftig verpflichtet sind, jeder Zeit nachweisen zu können, dass sie datenschutzrechtliche Anforderungen einhalten (**Rechenschaftspflicht**). Der Grundsatz der Rechenschaftspflicht legt es nahe, umfangreichere Dokumentation der Datenschutz-Organisation zu schaffen, die es dem Verantwortlichen ermöglicht, eine Datenschutz-Organisation nachzuweisen, die den datenschutzrechtlichen Anforderungen entspricht.

4. Rechtmäßigkeit der Verarbeitung personenbezogener Daten

Neu und wichtig	Das ist zu tun
• Die allgemeinen Rechtfertigungstatbestände der DSGVO entsprechen im Wesentlichen denen des BDSG-alt. • Für besondere personenbezogene Daten ergeben sich strenge Anforderung an die Rechtmäßigkeit der Verarbeitung. • Die Verarbeitung personenbezogener Daten von Kindern auf der Basis einer Einwilligung wird eingeschränkt. • Es gibt erweiterte Hinweispflichten bei der Einholung von Einwilligungserklärungen.	• Sicherstellen, dass die Verarbeitung personenbezogener Daten auf eine Rechtfertigung nach der DSGVO gestützt werden kann. • Prüfen, ob einwilligungsbasierte Verarbeitungen auch nach Inkrafttreten der DSGVO noch gerechtfertigt sind.

4.1. Erlaubnistatbestände zur Verarbeitung personenbezogener Daten

Die DSGVO schreibt den Grundsatz des Verbots der Datenverarbeitung mit Erlaubnisvorbehalt fort. Jeder Umgang mit personenbezogenen Daten ist daher im Grundsatz unzulässig, es sei denn, der Verantwortliche kann diesen Datenumgang auf einen Rechtfertigungstatbestand stützen. Für den Umgang mit „normalen" personenbezogenen Daten folgen Rechtfertigungstatbestände aus Art. 6 DSGVO. Anforderungen an einwilligungsbasierte Rechtfertigungen ergeben sich aus Art. 7 und 8 DSGVO. Anforderungen an die Rechtfertigung der Verarbeitung besonderer Kategorien personenbezogener Daten sind in Art. 9 DSGVO geregelt. Für den Beschäftigtendatenschutz gibt es eine Öffnungsklausel in Art. 88 DSGVO und nationale Regelungen, wie § 26 BDSG-neu.

4.2. Einwilligung

Gemäß Art. 6 Abs. 1 lit. a DSGVO ist eine Datenverarbeitung zulässig, wenn sie auf die Einwilligung des Betroffenen gestützt werden kann. Inhaltliche Anforderungen an die Einwilligungserklärung ergeben sich aus Art. 7 DSGVO und für die Einwilligung von Kindern aus Art. 8 DSGVO. Der Grundsatz der Schriftlichkeit von Einwilligungserklärungen wird mit der DSGVO

abweichend von der Regelung in § 4a Abs. 1 BDSG-alt nicht fortgeschrieben. Künftig stehen andere Formen der Erklärung (elektronisch, mündlich, konkludent) der Schriftform damit gleich. Relativiert wird diese Formerleichterung allerdings durch die Nachweispflicht des Verantwortlichen, die faktisch eine schriftliche oder eine in der Praxis leichter umzusetzende elektronische Dokumentation von Einwilligungserklärungen erfordert.

Bei der Einholung von Einwilligungserklärungen gelten künftig strengere Informationspflichten. So sind Betroffene vor der Erklärung auf die Freiwilligkeit und freie Widerruflichkeit der Erklärung hinzuweisen. Weitere Informationserfordernisse ergeben sich aus den allgemeinen Informationspflichten bei der Erhebung von Daten beim Betroffenen gemäß Art. 13 DSGVO. Für bestehende Einwilligungserklärungen gilt entsprechend eines Beschlusses des Düsseldorfer Kreises vom 13./14. September 2016, dass diese im Grundsatz fortgelten, auch wenn die Informationsanforderungen der DSGVO nicht erfüllt sind.

Für diesen Grundsatz gibt es aber auch relevante Einschränkungen. So sind insbesondere die Maßstäbe für die Bewertung der Freiwilligkeit der Erklärung und die Altersgrenzen nach der DSGVO zu bewerten. Verantwortliche sollten daher einwilligungsbasierte Rechtfertigungskonzepte auf DSGVO-Konformität prüfen.

Für einwilligungsbasierte Rechtfertigungen bei Diensten der Informationsgesellschaft gegenüber Kindern folgt aus Art. 8 DSGVO, dass Kinder das sechzehnte Lebensjahr vollendet haben müssen, um eine wirksame Einwilligung zu erklären. Von der Möglichkeit zur Absenkung dieser Altersgrenze hat der deutsche Gesetzgeber keinen Gebrauch gemacht.

4.3. Allgemeine Rechtfertigungstatbestände

Aus Art. 6 Abs. 1 lit. b-f DSGVO ergeben sich allgemeine Rechtfertigungstatbestände, die für den deutschen Rechtsanwender die Rechtfertigungstatbestände gemäß § 28 Abs. 1 BDSG-alt in wesentlichen Teilen fortschreiben.

- Gemäß Art. 6 Abs. 1 lit. b DSGVO ist die Datenverarbeitung zur Erfüllung eines Vertrages mit dem Betroffenen zulässig,
- gemäß Art. 6 Abs. 1 lit. c DSGVO soweit eine rechtliche Verpflichtung dazu besteht und
- gemäß Art. 6 Abs. 1 lit. f. DSGVO bei einem berechtigten Interesse, wenn keine überwiegenden Interessen der Betroffenen entgegenstehen.

4.4. Verarbeitung besonderer Kategorien personenbezogener Daten

Aus Art. 9 DSGVO folgt ein verschärftes Rechtfertigungsgebot für die Verarbeitung besonderer Kategorien personenbezogener Daten. Diese „ist untersagt", wenn kein Rechtfertigungsgrund gemäß Art. 9 Abs. 2 DSGVO besteht.

Besondere Kategorien personenbezogener Daten sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben und zur sexuellen Orientierung. Neu in dieser Aufzählung sind biometrische Daten zur eindeutigen Identifizierung. Hierauf ist bei der Prüfung DSGVO-konformer Rechtfertigungsansätze besonders zu achten.

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist insbesondere zulässig, wenn

- der Betroffene ausdrücklich eingewilligt hat (Art. 9 Abs. 2 lit. a DSGVO),
- eine arbeits- oder sozialrechtliche Verpflichtung dazu besteht (Art. 9 Abs. 2 lit. b DSGVO),
- die Verarbeitung zur Ausübung oder Verteidigung von Rechtsansprüchen dient (Art. 9 Abs. 2 lit. f DSGVO) oder
- zur Gesundheitsvorsorge, Diagnostik, und Behandlung erforderlich ist (Art. 9 Abs. 2 lit. h DSGVO).

4.5. Beschäftigtendatenschutz

Die lange bestehende Forderung nach detaillierten Regelungen zur Datenverarbeitung in Beschäftigungsverhältnissen wird auch mit der DSGVO nicht erfüllt. Im Gegenteil. Gemäß Art. 88 DSGVO wurde für den Beschäftigtendatenschutz eine Öffnungsklausel geschaffen, und der Beschäftigtendatenschutz weitgehend aus der DSGVO ausgelagert. Der deutsche Gesetzgeber hat von der Möglichkeit zur Regelung des Beschäftigtendatenschutzes mit § 26 BDSG-neu Gebrauch gemacht und die aktuelle Regelung in § 32 BDSG-alt im Wesentlichen wortgleich übernommen. Es bleibt also (fast) alles beim Alten.

Gemäß § 26 Abs. 1 S. 1 BDSG-neu dürfen Beschäftigtendaten verarbeitet werden, soweit dies für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erfor-

derlich ist. Arbeitgeber werden damit auch künftig vor der Herausforderung stehen, diese wenig konkreten Anforderungen in ihrem Unternehmen umzusetzen. Damit verbundene erhebliche Probleme sind für die aktuelle Rechtslage bekannt und bleiben auch mit Inkrafttreten der DSGVO bestehen.

Die Datenverarbeitung zur Aufdeckung von Straftaten ist auch künftig zulässig, wenn zu dokumentierende tatsächliche Anhaltspunkte einen Verdacht begründen. Auch für die investigative Datenverarbeitung im Unternehmen bleibt damit alles beim Alten (§ 26 Abs. 1 S. 2 BDSG-neu).

5. Rechte der Betroffenen

Neu und wichtig	Das ist zu tun
• Informationspflichten gegenüber den Betroffenen werden erheblich ausgeweitet. • Auskunftsansprüche von Betroffenen werden inhaltlich konkretisiert. • Es wird ein „Recht auf Vergessen" eingeführt. • Statt einem Recht auf Datensperrung gibt es ein Recht auf Einschränkung der Verarbeitung. • Betroffene haben ein Recht auf Datenübertragung, wenn die Verarbeitung auf einer Einwilligung oder einem Vertrag mit dem Betroffenen beruht.	• Verfahren, bei denen Daten erhoben werden, überprüfen und sicherstellen, dass Informationspflichten erfüllt werden. • Prozesse zur Beauskunftung von Betroffenen überprüfen und das Format der Beauskunftung anpassen. • Überprüfen, wann personenbezogene Daten öffentlich gemacht oder Dritten offengelegt werden und einen Prozess implementieren, der es ermöglicht, Dritte über eine Korrektur oder Löschung zu informieren. • Datenverarbeitungsprozesse so strukturieren, dass eine eingeschränkte Verarbeitung möglich ist. • Prüfen, für welche Verarbeitungen ein Recht auf Datenübertragbarkeit besteht und entsprechende Exportfunktionen in IT-Systemen implementieren.

5.1. Information

Art. 13 und 14 DSGVO beinhalten Informationspflichten des Verantwortlichen gegenüber den betroffenen Personen, wenn die Daten bei den betroffenen Personen erhoben werden (Art. 13 DSGVO) oder bei Dritten erhoben werden (Art. 14 DSGVO). Diese Informationspflichten sind erheblich umfangreicher und detaillierter, verglichen mit den bisherigen Vorgaben aus Art. 10 und 11 der Datenschutzrichtlinie 1995 und deren Umsetzung etwa in § 4 Abs. 3 und § 33 Abs.

1 BDSG-alt. Dies schafft konkreten Anpassungsbedarf für datenschutzrechtliche Informationsroutinen etwa im Zusammenhang mit Bestell- und Registrierungssystemen.

Neue Informationen, die der Verantwortliche den betroffenen Personen zur Verfügung stellen muss, wenn personenbezogene Daten beim Betroffenen oder bei Dritten erhoben werden sind:

- die Kontaktdaten des Datenschutzbeauftragten,
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung,
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten in ein Drittland oder an eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission,
- die Dauer der Speicherung der personenbezogenen Daten,
- wenn die Verarbeitung auf der Grundlage eines berechtigten Interesses von dem Verantwortlichen oder einem Dritten erfolgt, die berechtigten Interessen,
- das Recht auf Auskunft und Widerspruch sowie der Hinweis, dass die Einwilligung jederzeit widerrufen werden kann,
- das Recht auf Datenübertragbarkeit,
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde,
- Quelle aus der die personenbezogenen Daten stammen,
- die Möglichkeit einer automatischen Entscheidungsfindung einschließlich Profiling,
- die Dauer der Verarbeitung.

Die in Art. 13 und 14 DSGVO aufgelisteten Informationen müssen den betroffenen Personen zur Verfügung gestellt werden,

- wenn die personenbezogenen Daten bei den betroffenen Personen direkt erhoben werden oder
- innerhalb einer angemessenen Zeit nach der Erhebung der Daten von Dritten, spätestens aber einen Monat nach der Erhebung, wenn diese veröffentlicht oder zur Kommunikation mit der betroffenen Person verwendet werden.

5.2. Auskunft

Art. 15 DSGVO legt das Recht der betroffenen Person fest, nach dem diese

- von dem Verantwortlichen eine Bestätigung darüber verlangen kann, ob sie betreffende personenbezogene Daten verarbeitet werden und
- wenn dies der Fall ist, dass sie Auskunft über die personenbezogenen Daten verlangen kann.

Art. 15 DSGVO enthält eine Liste mit Informationen, die der betroffenen Person zu Verfügung gestellt werden müssen, die den Informationspflichten des Verantwortlichen in Art. 13 und 14 DSGVO sehr ähnlich sind. Konkret müssen Verantwortliche bei Auskunftsbegehren folgende Informationen zur Verfügung stellen:

- die Verarbeitungszwecke,
- Kategorien personenbezogener Daten, die verarbeitet werden,
- Empfänger oder Kategorien von Empfängern,
- geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder Kriterien für die Festlegung der Dauer,
- Bestehen eines Rechts auf Berichtigung, Löschung und Einschränkung der Verarbeitung,
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde,
- Informationen über die Herkunft der Daten,
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling,
- bei Übermittlungen in Drittländer: Bestehen geeigneter Garantien gemäß Art. 46 DSGVO.

Im Gegensatz zu den aktuellen rechtlichen Rahmenbedingungen in Art. 12 Datenschutzrichtlinie 1995 verpflichtet Art. 15 DSGVO den Verantwortlichen, die Informationen ggf. elektronisch in einem gängigen Format zur Verfügung zu stellen.

5.3. Berichtigung, Löschung und Recht auf Vergessenwerden

Das Recht der betroffenen Personen auf Berichtigung und Löschung von Daten durch den Verantwortlichen ist den Vorgaben der Datenschutzrichtlinie 1995 sehr ähnlich. Grundlegend neu ist aber, dass das Löschungsrecht in der DSGVO ausdrücklich das "Recht auf Vergessenwerden" beinhaltet. Niederschlag findet dieses Recht in Art. 17 Abs. 2 DSGVO. Danach muss ein Verantwortlicher, der personenbezogene Daten öffentlich gemacht hat und zur Löschung verpflichtet ist, angemessene Maßnahmen treffen, um Datenempfänger von der Löschung zu informieren. Ergänzt wird diese Verpflichtung in Art. 19 DSGVO, indem Verantwortlichen Mitteilungspflichten an alle Empfänger personenbezogener Daten auferlegt werden, denen sie personenbezogene Daten offengelegt haben.

5.4. Einschränkung der Verarbeitung

Aus Art. 18 DSGVO folgt, dass Betroffene das Recht haben, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

- die Richtigkeit der personenbezogenen Daten wird von dem Betroffenen bestritten und der Verantwortliche muss die Richtigkeit überprüfen,
- die Verarbeitung unrechtmäßig ist und der Betroffene die Löschung der Daten ablehnt und die Einschränkung der Nutzung verlangt,
- der Verantwortliche benötigt die Daten nicht länger für den Verarbeitungszweck, der Betroffene benötigt die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen,
- der Betroffene hat Widerspruch gegen die Verarbeitung eingelegt und es besteht Unsicherheit, ob berechtigte Gründe des Verantwortlichen an der fortgesetzten Speicherung und Verarbeitung die Interessen des Betroffenen überwiegen.

5.5. Datenübertragbarkeit

Wenn die Verarbeitung der personenbezogenen Daten auf der Einwilligung der betroffenen Person beruht oder auf einem Vertrag, hat die betroffenen Person gemäß Art. 20 DSGVO das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die Daten bereitgestellt wurden, zu übermitteln.

6. Datenschutzdokumentation

Neu und wichtig	Das ist zu tun
• Die Pflicht zur Meldung von Datenverarbeitungen an Aufsichtsbehörden entfällt weitgehend. • Verantwortliche und Auftragsverarbeiter müssen Verzeichnisse der Verarbeitungstätigkeiten führen. • Der Rechenschaftsgrundsatz verpflichtet zur Dokumentation einer DSGVO-konformen Datenschutz Organisation.	• Verzeichnisse von Verarbeitungstätigkeiten erstellen und aktuell halten. • Eine Dokumentation schaffen mit der eine DSGVO-konforme Datenschutz-Organisation nachgewiesen werden kann.

6.1. Verzeichnis der Verarbeitungstätigkeiten

Die DSGVO übernimmt das deutsche Konzept der internen Führung von Übersichten der Prozesse zur Verarbeitung personenbezogener Daten statt umfangreicher Meldepflichten gegenüber den Aufsichtsbehörden und der Führung von Datenverarbeitungsregistern durch die Aufsichtsbehörden. Gemäß Art. 30 Abs. 1 DSGVO hat jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten zu führen, welches der „Verarbeitungsübersicht" gemäß § 4g Abs. 2 BDSG-alt vergleichbar, inhaltlich aber nur teilweise identisch ist. Neben Verantwortlichen sind Auftragsverarbeiter verpflichtet, inhaltlich reduzierte Verzeichnisse über sämtliche Verarbeitungstätigkeiten zu führen, die im Auftrag eines Verantwortlichen durchgeführten werden.

Art. 30 Abs. 5 DSGVO enthält eine Ausnahme von dieser Verpflichtung. Beschäftigt ein Unternehmen oder eine Einrichtung weniger als 250 Mitarbeiter, ist es von der Verpflichtung zur Führung des Verzeichnisses der Verarbeitungstätigkeiten ausgenommen, es sei denn die vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO.

Selbst wenn die Ausnahme in Art. 30 Abs. 5 DSGVO einschlägig ist, sollten der Verantwortliche und der Auftragsverarbeiter sorgfältig prüfen, ob auch ohne eine gesetzliche Pflicht Verzeichnisse der Verarbeitungstätigkeiten geführt werden. Zum einen besteht nämlich ggf. ein Risiko,

ob der Verantwortliche von der Pflicht tatsächlich befreit ist. Zum anderen besteht die allgemeine Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO und die Verzeichnisse von Verarbeitungstätigkeiten sind ein optimales Dokument, in denen entsprechende Dokumentation geführt werden kann.

6.2. Datenschutzdokumentation

Stärker als bisher gilt im Datenschutzrecht der Grundsatz „Wer schreibt, der bleibt". Neben der datenschutzkonformen Organisation von Geschäftsprozessen wird der Fokus der Datenschutz-Organisation damit stark auf deren Dokumentation gelenkt. Nur wer Datenschutzrecht erstens Einhält und dies zweitens jederzeit nachweisbar dokumentiert, hat eine DSGVO-konforme Datenschutz-Organisation geschaffen, die der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO gerecht wird.

Faktisch bedeutet dies, über die datenschutzkonforme Prozessgestaltung interne Dokumentation für jeden Baustein der Datenschutz-Organisation zu führen. Neben den Verzeichnissen von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO als „Pflichtdokumentation" sollten Verantwortliche daher weitere Dokumentation schaffen. Vor dem Hintergrund der Rechenschaftspflicht empfehlen sich unter anderem

- Löschkonzepte,
- Richtlinien zum technischen und organisatorischen Datenschutz,
- Konzepte zum technischen und organisatorischen Datenschutz,
- Anweisungen zur Meldung von Datenschutzvorfällen,
- Einwilligungskonzepte,
- Berichte zu Datenschutz-Audits.

7. Datenschutz-Folgenabschätzung

Neu und wichtig	Das ist zu tun
• Verantwortliche müssen für sämtliche Prozesse zur Verarbeitung personenbezogener Daten eine Risikoabschätzung und für risikohafte Verarbeitungen eine Datenschutz-Folgenabschätzung durchführen.	• Einen Prozess implementieren, der die Verarbeitungen personenbezogener Daten identifiziert, für die eine Datenschutz-Folgenabschätzung notwendig ist. • Datenschutz-Folgenabschätzungen für identifizierte Verarbeitungen durchführen.

Art. 35 Abs. 1 DSGVO implementiert die Pflicht des Verantwortlichen, eine Datenschutz-Folgenabschätzung für jede Verarbeitung personenbezogener Daten durchzuführen, für die "voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen" besteht. Art. 35 Abs. 3 DSGVO enthält Beispiele der Verarbeitung personenbezogener Daten, für die eine Datenschutz-Folgenabschätzung erforderlich ist, nämlich

- bei systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen,
- umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten (z.B. Gesundheitsdaten) und
- systematischer und umfangreicher Überwachung öffentlich zugänglicher Bereiche (z.B. durch Videoüberwachung).

Zusätzlich sollen die Aufsichtsbehörden eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist (vgl. Art. 35 Abs. 4 DSGVO). Die Aufsichtsbehörden in Deutschland haben diese Liste aktuell noch nicht erstellt.

Art. 35 Abs. 1 DSGVO verlangt von dem Verantwortlichen,

- eine Abschätzung für jeden Prozess der Verarbeitung personenbezogener Daten zu erstellen, unabhängig davon, ob eine Datenschutz-Folgenabschätzung nach den o.g. Kriterien erforderlich ist oder nicht und
- wenn erforderlich, eine Datenschutz-Folgenabschätzung durchzuführen.

Art. 35 Abs. 7 DSGVO enthält eine Beschreibung des Gegenstands einer Datenschutz-Folgenabschätzung, nämlich

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge,
- eine Bewertung ihrer Notwendigkeit und Verhältnismäßigkeit,
- eine Bewertung der Risiken für Rechte und Freiheiten der betroffenen Personen sowie
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen.

Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt, dem nicht durch Maßnahmen zur Risikoeindämmung entgegengewirkt werden kann, muss der Verantwortliche die Aufsichtsbehörde gemäß Art. 36 DSGVO konsultieren. Die Aufsichtsbehörde trifft dann die Entscheidung, ob die Verarbeitung erfolgen darf und ggf. mit welchen Auflagen.

8. Datenschutzbeauftragter

Neu und wichtig	Das ist zu tun
• Die DSGVO führt in allen Mitgliedsstaaten die Pflicht zur Bestellung von Datenschutzbeauftragten ein. • Öffentliche Stellen in Deutschland müssen einen Datenschutzbeauftragten bestellen. • Nicht-öffentliche Stellen müssen einen Datenschutzbeauftragten bestellen, wenn sie zehn oder mehr Personen bei der Verarbeitung personenbezogener Daten einsetzen.	• Sicherstellen, dass ein Datenschutzbeauftragter bestellt ist.

Mit Art. 37 Abs. 1 DSGVO wird erstmals in allen Mitgliedsstaaten die Pflicht zur Bestellung eines Datenschutzbeauftragten eingeführt. Inhaltlich bleibt diese hinter den Anforderungen des deutschen Rechts zurück und führt für die Mehrheit der Verantwortlichen letztlich nicht zu einer Bestellpflicht. Nach Art. 37 Abs. 1 DSGVO ist ein Datenschutzbeauftragter einzusetzen, wenn

- die Kerntätigkeit des Verantwortlichen (oder des Auftragsverarbeiters) in der Durchführung von Verarbeitungsvorgängen besteht, welche eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder
- besondere Arten personenbezogener Daten oder Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet werden.

Die Mitgliedstaaten können weitere Gründe für die zwingende Bestellung eines Datenschutzbeauftragten festlegen. Dies hat der deutsche Gesetzgeber mit der Regelung in §§ 5-7 BDSG-neu für öffentliche Stellen und § 38 BDSG-neu für nicht-öffentliche Stellen getan.

Für Verantwortliche in Deutschland bleibt damit alles beim Alten. Öffentliche Stellen müssten stets einen Datenschutzbeauftragten bestellen; nicht-öffentliche, wenn sie zehn oder mehr

Personen bei der Verarbeitung personenbezogener Daten einsetzen. Die Anforderungen daran sind gering. Faktisch reicht dafür schon die Nutzung eines Computers bei der Arbeit.

9. Meldepflicht bei Datenschutzverstößen

Neu und wichtig	Das ist zu tun
• Verantwortliche müssen schwere Datenschutzverstöße innerhalb von 72 Stunden an die Datenschutzaufsichtsbehörde melden. • Bei schweren Datenschutzverstößen müssen die Betroffenen unverzüglich informiert werden.	• Sicherstellen, dass Datenschutzverstöße intern schnell gemeldet und geprüft werden. • Bei schweren Datenschutzverstößen eine Meldung an die Datenschutzaufsichtsbehörde und Information der Betroffenen sicherstellen.

In Art. 33 und 34 DSGVO finden sich die Verpflichtungen der Verantwortlichen zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde (Art. 33 DSGVO) oder betroffene Personen (Art. 34 DSGVO). Diese Verpflichtungen sind in der Datenschutzrichtlinie 1995 nicht enthalten, jedoch in der aktuellen Fassung des BDSG-alt (vgl. § 42a BDSG-alt). Verglichen mit § 42a BDSG-alt sind die Melde- und Informationspflichten in der DSGVO allerdings detaillierter und weitreichender.

Verantwortliche müssen der zuständigen Aufsichtsbehörde eine Verletzung des Schutzes personenbezogener Daten unverzüglich melden, in der Regel innerhalb von 72 Stunden. Ausnahmen von dieser Meldepflicht bestehen nur, wenn die Verletzung des Schutzes personenbezogener Daten nicht zu einem Risiko für die Rechte und Freiheiten der natürlichen Personen führt. Art. 33 Abs. 2 DSGVO enthält die Informationen, die eine Meldung mindestens umfassen muss. Auftragsverarbeiter müssen einen Vorfall unverzüglich dem Verantwortlichen melden.

Ist die Verletzung des Schutzes personenbezogener Daten voraussichtlich mit einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen verbunden, so müssen die betroffenen Personen nach Art. 34 Abs. 1 DSGVO ebenfalls benachrichtigt werden. Auch diese Benachrichtigung muss unverzüglich erfolgen. Die Benachrichtigung gegenüber den betroffenen Personen muss in klarer und einfacher Sprache erfolgen. Sie muss den Personen verdeutlichen, welches Risiko aufgrund welcher Verletzung eintritt. Die Meldung kann beim

Vorliegen der in Art. 34 Abs. 3 DSGVO enthaltenen Ausnahmetatbestände unterbleiben, insbesondere, wenn der Verantwortliche Maßnahmen eingeleitet hat, die den Schaden für die betroffenen Personen mildern.

Hierbei muss allerdings die Regelung in Art. 34 Abs. 3 lit. c DSGVO beachtet werden. Dort wird festgelegt, dass die Benachrichtigung betroffener Personen nicht erforderlich ist, wenn dies mit einem unverhältnismäßig hohen Aufwand verbunden ist. In diesem Fall muss stattdessen eine öffentliche Bekanntmachung oder eine ähnlich wirksame Maßnahme ergriffen werden, durch die die betroffenen Personen vergleichbar wirksam informiert werden. In jedem Fall fordern die Art. 33 und 34 DSGVO einen schnellen internen Prozess, um diese Entscheidung sowohl auf personeller als auch auf der Ebene der Geschäftsführung zu treffen.

10. Verhaltensregeln und Zertifizierung

Neu und wichtig	Das ist zu tun
• Die DSGVO fördert die Selbstregulation und Zertifikation. Diese Instrumente werden zur Dokumentation der Einhaltung von zahlreichen Anforderungen der DSGVO künftig anerkannt.	• beobachten, ob relevante Vereinigungen Verhaltensregeln entwickeln und diese ggf. übernehmen, um die Einhaltung der DSGVO nachzuweisen. • Zertifizierungen in Erwägung ziehen, um die Einhaltung von Anforderungen der DSGVO nachzuweisen.

10.1. Genehmigte Verhaltensregeln

Art. 40 Abs. 2 DSGVO schafft die Möglichkeit, genehmigte Verhaltensregeln zu schaffen und richtet sich an Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten. Diesen soll Gelegenheit gegeben werden, Verhaltensregelungen auszuarbeiten und zu erweitern, an die sich die von ihnen vertretenen Verantwortlichen oder Auftragsverarbeiter halten müssen. Dies beinhaltet insbesondere die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen (Art. 40 Abs. 2 lit. b DSGVO) beziehungsweise unter welchen Umständen der Transfer an Drittländer rechtmäßig ist (Art. 40 Abs. 2 lit. j DSGVO). Diese Verhaltensregeln benötigen allerdings die Genehmigung der EU-Kommission.

10.2. Zertifizierung, Datenschutzsiegel und -prüfzeichen

Die DSGVO unterstützt die Vergabe von Zertifizierungen, Datenschutzsiegeln und -prüfzeichen (Art. 42 DSGVO). Die Vergabe soll nach Art. 42 Abs. 1 DSGVO von den Mitgliedstaaten, den Aufsichtsbehörden oder von dem zu gründenden Europäischen Datenschutzausschuss sowie von der Kommission gefördert werden. Zusätzlich können auch Verantwortliche und Auftragsverarbeiter, die nicht unter diese Verordnung fallen, offizielle Zertifizierungsverfahren, Siegel oder Prüfzeichen erhalten, um nachzuweisen, dass sie im Rahmen der Übermittlung von personenbezogenen Daten an Drittländer oder internationale Organisationen geeignete Garantien bilden. Es ist zu erwarten, dass die Zertifizierung eine größere Rolle spielen werden, als derzeit.

11. Datensicherheit und Datenschutz durch Technikgestaltung

Neu und wichtig	Das ist zu tun
• Mit der DSGVO wird ein neuer Referenzrahmen zur Bewertung technisch-organisatorischer Maßnahmen geschaffen. • Aus der DSGVO ergibt sich die Pflicht zur datenschutzkonformen Technikgestaltung (Privacy by Design und Privacy by Default).	• Das Konzept zum technisch-organisatorischen Datenschutz anpassen und die Änderungen umsetzen. • Belastbarkeit, rasche Widerherstellbarkeit und Verfahren zur regelmäßigen Überprüfung technisch-organisatorisch umsetzen und dokumentieren. • Grundsätze der Datenminimierung und Vertraulichkeit bei der Prozessplanung berücksichtigen und datenschutzfreundliche Voreinstellungen von Systemen umsetzen.

11.1. Technische und organisatorische Maßnahmen

Verantwortliche und Auftragsverarbeiter müssen nach Art. 32 DSGVO angemessene technisch-organisatorische Sicherheitsmaßnahmen gegen unbefugte Zugriffe und Datenverlust treffen. Die DSGVO verfolgt dabei die drei klassischen Schutzziele der IT-Sicherheit, nämlich die Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Anders als das BDSG-alt bricht die DSGVO diese abstrakten Vorgaben aber nicht auf konkrete Kontrollziele herunter, sondern bleibt bei der Datensicherheit mehr im Allgemeinen.

Wie bisher ist der erste Schritt zur Erstellung eines Datensicherheitskonzepts die Analyse der Risiken, welche die Datenverarbeitung für die Betroffenen mit sich bringt (Art. 32 Abs. 2 DSGVO). Es ist zu empfehlen, im Rahmen einer kombinierten und zu dokumentierenden Schutzbedarfs- und Risikoanalyse zunächst den Schutzbedarf der Daten zu bestimmen (z.B. Einteilung in drei Schutzbedarfsklassen unter Berücksichtigung der Stärke des Personenbezugs und der Sensibilität der Daten) und dann zu analysieren, welche physischen, materiellen und immateriellen Schäden den Betroffenen durch einen möglichen Missbrauch der Daten drohen.

Bei der Auswahl angemessener Maßnahmen dürfen Wirtschaftlichkeitserwägungen berücksichtigt werden. Außerdem müssen sich die Maßnahmen am Stand der Technik orientieren. Hierzu empfiehlt es sich jedenfalls für größere Organisationen, anerkannte Standards wie IT-Grundschutz (bzw. ISO 2700x) umzusetzen oder zumindest als Orientierungspunkt zu nehmen.

Neu sind die Schutzziele der Belastbarkeit der Systeme und der raschen Wiederherstellbarkeit personenbezogener Daten nach Zwischenfällen (Art. 32 Abs. 1 lit. b und lit. c DSGVO). Außerdem verlangt die DSGVO die Einführung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Sicherheitsmaßnahmen (Art. 32 Abs. 1 lit. d DSGVO).

11.2. Privacy by Design

Durch Art. 25 Abs. 1 DSGVO werden Verantwortliche verpflichtet, sowohl bei der Planung von IT-Anwendungen als auch bei der anschließenden Nutzung technische und organisatorische Maßnahmen (z.B. Pseudonymisierung) einzusetzen, um die Rechte der betroffenen Personen zu schützen und den Anforderungen der DSGVO zu genügen. Verantwortliche sollten daher sicherstellen, dass jeder Prozess der Datenverarbeitung so geplant und implementiert wird, dass er den Grundsätzen der Datenminimierung und Vertraulichkeit gerecht wird.

11.3. Privacy by Default

Art. 25 Abs. 2 DSGVO beinhaltete das Konzept der "datenschutzfreundlichen Voreinstellung". Durch entsprechende Voreinstellungen von Systemen ist sicherzustellen, dass nur erforderliche personenbezogene Daten verarbeitet werden. Die Voreinstellungen von Systemen sind so zu gestalten, dass personenbezogene Daten nicht ohne Eingreifen des Verantwortlichen einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden können. Verantwortliche sollten das Konzept der "datenschutzfreundlichen Voreinstellung" umsetzen, insbesondere dann, wenn Dienstleistungen an Endverbraucher angeboten werden, (d.h. bei Auswahlmöglichkeiten, sollte die „datenschutzfreundliche" Option voreingestellt sein).

12. Auftragsverarbeitung

Neu und wichtig	Das ist zu tun
• Die Anforderungen an die Gestaltung von Vereinbarungen über die Auftragsverarbeitung ändern sich mit der DSGVO.	• Bestehende und neue Beauftragungen von Auftragsverarbeitern entsprechend den neuen Anforderungen vertraglich dokumentieren.

Die Auftragsverarbeitung ist von überragender praktischer Bedeutung sowohl für die rechtssichere Gestaltung des IT-Outsourcings als auch vieler anderer extern eingekaufter Dienstleistungen. Die DSGVO führt dieses wichtige Konzept fort. Die neuen Vorgaben ergeben sich aus Art. 28 DSGVO und sind wesentlich konkreter als in der Datenschutzrichtlinie 1995. Sie gehen zu erheblichen Teilen auf das BDSG-alt zurück, so dass die Änderungen aus Sicht deutscher Unternehmen keine grundsätzlich neuen Anforderungen schaffen.

Wie bisher sind Auftragsverarbeiter sorgfältig auszuwählen und es ist zu prüfen, ob sie insbesondere die Anforderungen an technisch-organisatorische Schutzmaßnahmen erfüllen. Sodann sind schriftliche Vereinbarungen über die Auftragsverarbeitung zu schließen. Anforderungen an den Inhalt solcher Vereinbarungen ergeben sich aus Art. 28 und 29 DSGVO und weichen von den bisherigen Vorgaben in § 11 Abs. 2 BDSG-alt ab. Dies erfordert die Anpassung der vertraglichen Dokumentation sowohl für bestehende als auch für neu abzuschließende Aufträge.

13. Übermittlungen in Drittländer

Neu und wichtig	Das ist zu tun
• Das Rechtfertigungskonzept für internationale Datenübermittlungen wird ergänzt um die Rechtfertigungsinstrumente der Genehmigte Verhaltensregelungen und Zertifizierungen.	• Sicherstellen, dass für internationale Datenübermittlungen angemessene Rechtfertigungsinstrumente implementiert sind.

Die DSGVO enthält im Wesentlichen mit den Regelungen der Datenschutzrichtlinie 1995 vergleichbare Regelungen zum internationalen Datentransfer. So soll durch Art. 44 DSGVO sichergestellt werden, dass bei einer Übermittlung in Drittländer oder an internationale Organisationen das durch die DSGVO gewährleistete Schutzniveau nicht unterlaufen wird.

Wie schon nach der Datenschutzrichtlinie 1995, kann auch nach der DSGVO eine Übermittlung in Drittländer oder an eine internationale Organisation ohne gesonderte Genehmigung erfolgen, wenn das Drittland ein von der EU-Kommission durch Beschluss anerkanntes und angemessenes Schutzniveau hat.

Die Regelungen in der DSGVO zu dieser Ausnahme sind ebenfalls mit denen der Datenschutzrichtlinie 1995 vergleichbar. Demnach kann die Datenübermittlung alternativ auch auf Grundlage von Art. 46 DSGVO erfolgen, wenn ein Verantwortlicher oder ein Auftragsverarbeiter geeignete Garantien vorsieht.

Liegt weder ein Beschluss der EU Kommission (Art. 45 DSGVO) noch die oben benannte Ausnahme (Art. 46 DSGVO) vor, können an diese Stelle geeignete Garantien für die Übermittlung in Drittstaaten treten. Auch hier folgt die DSGVO den entsprechenden Regelungen in der Datenschutzrichtlinie 1995. Diese Garantien sind Bindig Corporate Rules (BCR), Standardvertragsklauseln der EU-Kommission und "ad-hoc" Klauseln, welche der Genehmigung durch die Aufsichtsbehörde bedürfen. Die DSGVO enthält außerdem zwei neue Instrumente: genehmigte Verhaltensregeln und Zertifizierungen.

14. Haftung und Sanktionen

Neu und wichtig	Das ist zu tun
• Mit der DSGVO werden neue und stark verschärfte Sanktionen für Datenschutzverstöße geschaffen. • Das Haftungsregime wird verschärft. • Betroffene haben einen Anspruch auf Ersatz materieller und immaterieller Schäden aus Datenschutzverstößen.	• Der Datenschutz-Organisation größere Beachtung schenken. • Bußgelder als relevante Gefahr im Risikomanagementsystem berücksichtigen.

14.1. Bußgelder nach DSGVO

Die DSGVO legt neue und verschärfte Sanktionsmöglichkeiten bei Datenschutzrechtsverletzungen fest.

Die in Art. 82 DSGVO festgelegten Bußgelder für Verstöße gegen das Datenschutzrecht sind signifikant höher, als die in den aktuellen Datenschutzgesetzen. Im deutschen Datenschutzrecht ist die Höhe des Bußgeldes für einen Verstoß aktuell auf 300.000 € beschränkt (mit der Ausnahme, dass der wirtschaftliche Vorteil aus dem Verstoß darüber hinausgeht; dann kann auch heute das Bußgeld über den Betrag von 300.000 € hinausgehen). Die DSGVO sieht Bußgelder von bis zu 20.000.000 € oder 4 Prozent des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres vor, abhängig davon welcher Betrag höher ist (Art. 83 Abs. 5 DSGVO).

Bei Verstößen gegen die DSGVO ist die Höhe des Bußgeldes nach dem Umsatz des "Unternehmens" zu berechnen, welches gegen die Verordnung verstoßen hat. Der Begriff "Unternehmen" wird in der DSGVO nicht genau definiert. Gemäß Erwägungsgrund 150 DSGVO hat er die gleiche Bedeutung wie die in Art. 101 und 102 des Vertrages der Europäische Union und der Arbeitsweise der Europäischen Union (**AEUV**). Folgt man der seit langem bestehenden Interpretation des EUGH, umfasst eine Unternehmung "*jede eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung*". Weiterhin wird eine Unternehmensgruppe als eine Gruppe angesehen, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.

Für die Berechnung des Bußgeldes ist demnach der Umsatz der gesamten Unternehmensgruppe relevant, unabhängig davon, welches Unternehmen gegen die DSGVO verstoßen hat.

§ 43 BDSG-neu sieht zudem vor, dass Verstöße gegen Auskunfts- und Informationspflichten mit bis zu 50.000 € Bußgeld geahndet werden können.

14.2. Strafrechtliche Sanktionen

Aktuell spielen Verstöße gegen das Datenschutzrecht in der Praxis der Strafverfolgung keine relevante Rolle. Dass sich dies mit dem Inkrafttreten der DSGVO und dem BDSG-neu ändert, ist nicht zu erwarten. Die strafrechtliche Sanktion von Datenschutzverstößen wird aber weiter möglich sein, soweit im mitgliedsstaatlichen Recht vorgesehen.

Für deutsche Verantwortliche relevant sind die Regelungen in § 42 BDSG-neu. Danach wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft, wer nicht allgemein zugängliche personenbezogene Daten einer großen Anzahl betroffener Dritten zugänglich macht. Mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe wird bestraft, wer personenbezogenen Daten die nicht allgemein zugänglich sind ohne Berechtigung verarbeitet oder erschleicht.

14.3. Haftung

Zusätzlich zur Verhängung von Bußgeldern durch die Aufsichtsbehörden können betroffene Personen Schadensersatzansprüche gegen Verantwortliche und Auftragsverarbeiter haben, soweit diese gegen Datenschutzrecht verstoßen. Derzeit haben solche Schadensersatzforderungen kaum Relevanz. Das Recht der meisten Mitgliedstaaten schließt entsprechende Ansprüche aus, wenn die betroffene Person keinen messbaren wirtschaftlichen Schaden erlitten hat. Die DSGVO sieht jedoch vor, dass die betroffenen Personen auch bei einem immateriellen Schaden einen Anspruch auf Schadensersatz haben. Diese Ansprüche ergeben sich aus Art. 82 DSGVO. Bedeutsam ist darüber hinaus, dass durch Art. 82 Abs. 2 DSGVO sowohl Verantwortliche als auch Auftragsverarbeiter zur Haftung herangezogen werden können.

Die prozessualen Vorschriften und Details bezüglich der Schadensersatzansprüche werden durch das Recht der jeweiligen Mitgliedstaaten geregelt. Art. 80 Abs. 1 DSGVO sieht explizit vor, dass betroffene Personen das Recht haben, eine Organisation (z.B. die Verbraucherzentrale) zu beauftragen, in ihrem Namen eine Beschwerde einzureichen, ihre Rechte wahrzunehmen und ggf. das Recht auf Schadensersatz geltend zu machen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist.