REVISIO GMBH
Steuerberatungsgesellschaft

Datenschutz-Grundverordnung (DS-GVO)

Das müssen Sie wissen …

Mandanten-Info

zur

Datenschutz-Grundverordnung

(DS-GVO)

REVISIO GmbH Steuerberatungsgesellschaft
Kreuzberger Ring 18a, 65205 Wiesbaden
Telefon: 0611/778860, Telefax: 0611/7788666
E-Mail: wiesbaden@re-visio.com, Internet: www.re-visio.com

Datenschutz-Grundverordnung (DS-GVO)

1 Einführung

Das Thema Datenschutz erfährt derzeit eine ungewohnte Aufmerksamkeit in Unternehmen: Seminare, Bücher, Informationen überall. Warum erscheint dies so?

Das Datenschutzrecht gibt es in Deutschland bundesweit seit 1977 für Unternehmen und Behörden. Durch die europaweite Einführung gleichlautender Regelungen verbunden mit drastischen Strafandrohungen, die man bislang nur aus wettbewerbsrechtlichen Verfahren kannte, fühlen sich weitaus mehr Unternehmen angesprochen, als bisher.

Doch warum wirkt das Datenschutzrecht so kompliziert? Entgegen dem sonstigen freiheitlich-demokratischen Grundsatz, jeder tut, was er will, es sei denn, es ist verboten, gilt bei der Verarbeitung personenbezogener Daten ein **Verbot mit Erlaubnisvorbehalt**. Allein diese Festlegung ist schon erklärungsbedürftig. Bei einer – allein abstrakten – Gefährdung eines Rechtsguts, so fordert die Rechtsordnung hier eine Umkehr: Ich brauche eine rechtliche Erlaubnis, weil ein unsachgemäßes Verhalten einen unangemessen großen Schaden anrichten kann. Jeder Bürger kennt dies aus dem normalen Leben: Zu Fuß gehen darf jeder, auch Fahrradfahren ist an keine Erlaubnis gebunden. Doch bei einem Kraftfahrzeug bzw. Motorrad fordern wir den Nachweis der Befähigung – weil ein Schadensrisiko für Leib und Leben anderer dadurch wesentlich erhöht wird, wenn jeder ohne Mindestkenntnisse und praktischen Nachweis ans Steuer dürfte.

Durch die Verarbeitung personenbezogener Daten können sich aber für die betroffene Person Nachteile ergeben, wenn diese Daten falsch sind oder zweckwidrig verwendet werden. Dies könnte zu lebenslangen Nachteilen in allen Lebensbereichen führen, ohne dass dem Betroffenen die Ursache bekannt wird. Die Anforderung an eine starke Regulierung ergibt sich auch aus Art. 8 der Europäischen Grundrechtecharta. Durch Kenntnis dieser Hintergründe wird es Ihnen leichter fallen, die Ableitungen aus dem Verbot mit Erlaubnisvorbehalt, die sich im Datenschutzrecht hinsichtlich der Rechtmäßigkeit, Transparenz und Kontrolle ergeben, zu verstehen.

Zielrichtung:

Diese Broschüre soll den Einstieg erleichtern und ersetzt nicht ausführlichere Werke zu diesem Thema, auch wird soweit noch sinnvoll auf die Zitierung der jeweiligen Artikel der DS-GVO verzichtet, um die Lesbarkeit zu erleichtern. Sie werden bei der Umsetzung der DS-GVO alle Personengruppen berücksichtigen müssen, deren Daten Sie verarbeiten: Dies umfasst die personenbezogenen Daten Ihrer Kunden, Ihrer Beschäftigten und Ihrer Lieferanten.

Begrifflichkeiten:

In der DS-GVO werden Begriffe verwendet, mit denen Sie sich vertraut machen müssen. Der **Verantwortliche** ist für die Umsetzung der datenschutzrechtlichen Anforderungen verantwortlich. Er ist derjenige, der den Zweck und die Mittel der Verarbeitung bestimmt, also die jeweilige Unternehmensleitung. Die **betroffene Person** ist derjenige, dessen Daten verarbeitet werden. **Personenbezogene Daten** sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen lassen, also auch Kundennummern, Personalnummern, Telefonnummern, KfZ-Zeichen etc. Der Begriff der **Verarbeitung** ist weit auszulegen und umfasst u. a. Vorgänge von der Erhebung über Ordnen, Ändern, Speichern, Verwenden, Offenlegung durch Übermitteln sowie Löschen und Vernichten. Ein **Auftragsverarbeiter** verarbeitet weisungsgebunden personenbezogene Daten im Auftrag eines Verantwortlichen.

1.1 Warum neues Recht?

Bisher war das europäische Datenschutzrecht über eine Richtlinie geregelt, die dann durch die 28 Mitgliedstaaten umzusetzen ist. Dabei ergaben sich bei vielen Themen 28 Varianten, eine europaweit einheitliche Umsetzung wurde nicht erreicht. Dies wurde zum Anlass genommen, durch eine Verordnung, die innerhalb der gesamten EU unmittelbar gilt, eine Vereinheitlichung anzustreben. Auch die Wirtschaft profitiert davon, die künftig in einem einheitlichen Rechtsrahmen innerhalb Europas agieren soll und kann.

Die DS-GVO gilt in ihrer jeweiligen durch die EU in deren Amtsblatt veröffentlichten Sprachfassung.[1] Die englische Fassung der DS-GVO wird jedoch gerne zu Auslegungszwecken herangezogen, weil die Verhandlungen zum Gesetz in Englisch stattfanden.

[1] http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679

1.2 Was ändert sich?

Die Verantwortlichen und Auftragsverarbeiter werden stärker in die Pflicht genommen, die Einhaltung der Datenschutzvorgaben nachweisen zu können. Hinzu kommen neue Rechte für die betroffenen Personen, aber auch die Einführung eines risikobasierten Ansatzes bei der Schutzbedarfsermittlung, der die Rechte und Freiheiten der natürlichen Person berücksichtigt.

Hinweis

Wenn Sie bislang das bisherige BDSG eingehalten haben, ist das Delta nicht ganz so groß. Aber auch dann werden Sie mit Ressourcenaufwand bei der Analyse der Umsetzungsmaßnahmen und deren Implementierung rechnen müssen.

1.3 Struktur des Gesetzes

Die DS-GVO gliedert sich in zwei Teile: In 173 Erwägungsgründe (ErwGr.) und 99 Artikel. Maßgeblich sind die Artikel, die ErwGr. sind aber als unmittelbare Auslegungshinweise ebenso heranzuziehen. Es ist nicht so, dass es zu jedem Artikel einen klar zuordenbaren ErwGr. gibt. Zu manchen Themen können mehrere ErwGr. herangezogen werden, zu manchen Artikeln findet man keinen direkt unterstützenden ErwGr.

Hinweis

Besorgen Sie sich eine Gesetzesfassung, bei welcher bei den Artikeln auf den passenden ErwGr. hingewiesen wird. Beachten Sie aber, dass dies immer nur die Einschätzung des jeweiligen Herausgebers ist und es eine offizielle Zuordnung seitens des Gesetzgebers nicht gibt.

1.4 Öffnungsklauseln

Den Mitgliedstaaten werden innerhalb der DS-GVO eigene Regelungsbereiche zugestanden, die sie ausfüllen können, manchmal sogar müssen. Dabei legt die DS-GVO die Leitplanken fest, innerhalb derer die Mitgliedstaaten eigene Regelungen treffen dürfen. In Deutschland wurde hierfür das BDSG (Bundesdatenschutzgesetz) neu formuliert, dieses gilt ab 25.05.2018 und wird hier als **BDSG (2018)**[2] bezeichnet.

Beachten Sie bitte, dass innerhalb des BDSG (2018) der Dritte Teil nicht der Umsetzung der DS-GVO dient, sondern der Umsetzung einer Richtlinie, die auch „Richtlinie Polizei und Justiz“ genannt wird. Die Regelungen im Dritten Teil gelten daher nur für Unternehmen und Behörden bei der Verarbeitung personenbezogener Daten im Rahmen von Strafverfolgungs- und Strafjustiztätigkeiten.

Aufgrund der föderalen Struktur in Deutschland werden aber auch die Bundesländer für die in ihrem Zuständigkeitsbereich zu regelnden Verarbeitungen Landesdatenschutzgesetze erlassen, um den Spielraum der DS-GVO umzusetzen.

Betrifft es eine öffentlich-rechtliche Einrichtung, können daher auch die jeweiligen landesrechtlichen Datenschutzbestimmungen der Bundesländer anzuwenden sein. Aus historischen Gründen haben die evangelische und die katholische Kirche weiterhin ein Sonderrecht zu einem eigenen Datenschutzrecht – und haben davon auch Gebrauch gemacht.[3]

Hinweis

Prüfen Sie, welches Recht für Sie anzuwenden ist: In den meisten Fällen wird die DS-GVO, ergänzt durch das BDSG (2018), für Sie gelten.

Sind Sie ein Unternehmen mit mehreren Standorten, ist diejenige Aufsichtsbehörde zuständig, in der der Sitz der Hauptniederlassung liegt, sofern dort die Entscheidungen über Zweck und Mittel der Verarbeitungen getroffen werden. Werden in einer Niederlassung solche Entscheidungen getroffen und dort auch umgesetzt, gilt diese Niederlassung dafür als Hauptniederlassung. Die Rechtsform der Niederlassung ist unerheblich.

---

[2] BGBl. I 2017, 2097

[3] https://www.ekd.de/ekd_de/ds_doc/s17-8-3-Beschluss-Datenschutzgesetz.pdf
https://www.datenschutz-kirche.de/sites/default/files/KDG%20i.d.%20Fassung%20des%20Beschlusses%20der%20VV%20vom%2020.11.2017.pdf

1.5 Sanktionsrahmen

Die Sanktionsmöglichkeiten wurden erheblich erweitert. Der Bußgeldrahmen wurde – abhängig vom Verstoß – auf Geldbußen von bis zu 10 Mio. bzw. 20 Mio. Euro oder von bis zu 2 % bzw. 4 % des weltweiten Vorjahresumsatzes erhöht, je nachdem welcher Betrag höher ist.

Art. 83	Abs. 4	Abs. 5	Abs. 6
Geldbußen	Bis 10 Mio. Euro oder bis 2 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist.	Bis 20 Mio. Euro oder bis 4 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist.	Bis 20 Mio. Euro oder bis 4 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist.
Beispiele	Verstöße z. B. gegen Regelungen zu: Verzeichnis der Verarbeitungstätigkeiten Auftragsverarbeitung Datenschutz Folgenabschätzung etc.	Verstöße z. B. gegen Regelungen zu: Grundsätze Rechtmäßigkeit Einwilligung Rechte Betroffener etc.	Verstöße gegen: Anordnungen der Aufsichtsbehörde etc.

Allein diese Änderung führt bei vielen Unternehmen zu einem geänderten Bewusstsein, sich mit diesen Themen auseinanderzusetzen. Der deutsche Gesetzgeber hat Bußgelder gegen öffentliche Stellen bislang ausgeschlossen. Ebenso hat er in § 42 BDSG (2018) Strafvorschriften aufgenommen, bei denen es keine Privilegierung öffentlicher Stellen gibt.

2 Managementaufgaben

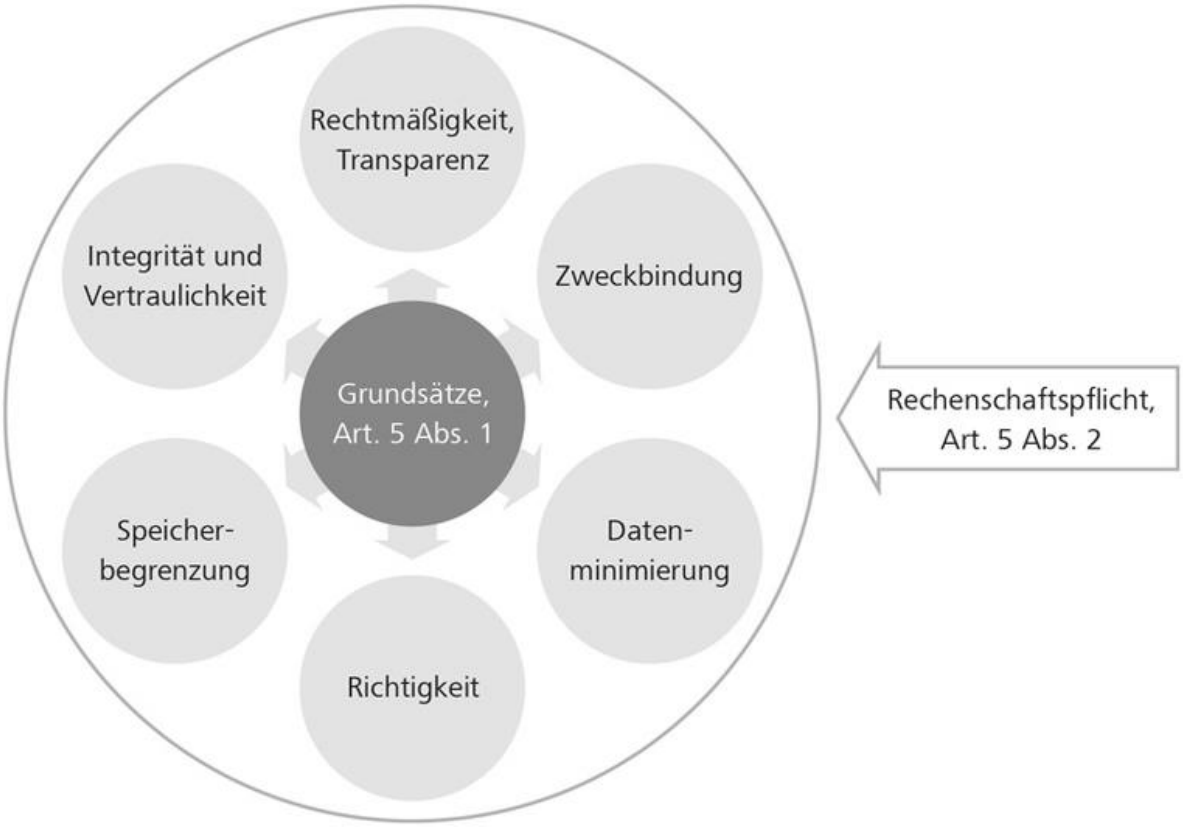
Der Verantwortliche ist Adressat der DS-GVO und muss die Einhaltung der DS-GVO nachweisen können. Das sorgt dafür, dass es eine unmittelbare Managementaufgabe ist, interne Regelungen zu schaffen, die die Einhaltung sicherstellen und durch Kontrollen zu überwachen, ob diese befolgt werden. Somit wird spätestens jetzt Datenschutz auch zum **Compliance-Thema** der Unternehmensleitung.

2.1 Grundsätze

In der DS-GVO werden in Art. 5 Grundsätze definiert, die sich alle aus Art. 8 der Europäischen Grundrechtecharta ableiten lassen. Sie müssen durch den Verantwortlichen nachweisbar eingehalten werden (Rechenschaftspflicht). Diese Grundsätze umfassen

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung (Löschpflicht)
- Integrität und Vertraulichkeit.

Als Rechtmäßigkeitsgrundlage (Art. 6) kommen neben der Einwilligung der betroffenen Person u. a. auch die Verarbeitung aufgrund eines Vertrages, einer rechtlichen Verpflichtung oder die Wahrung berechtigter Interessen in Frage. Zweckänderungen unterliegen einer Prüfung zur Vereinbarkeit des neuen Zwecks mit dem bisherigen Zweck (Art. 6 Abs. 4).



Die Grundsätze aus Art. 5 werden in der Datenschutz-Grundverordnung systematisch konkretisiert: In Kapitel II finden sich die Vorgaben zur Rechtmäßigkeit, in Kapitel III zu den Rechten der betroffenen Person und in Kapitel IV die Anforderungen an Verantwortliche und Auftragsverarbeiter die Grundsätze umzusetzen. Mit dem Sonderfall des Transfers von personenbezogenen Daten außerhalb der Europäischen Union/des Europäischen Wirtschaftsraums befasst sich Kapitel V.

Wie ernst es der Gesetzgeber damit meint, zeigt sich auch, dass er Verstöße gegen Art. 5 mit dem höheren Bußgeld bewehrt.

Hinweis

Machen Sie Ihre Mitarbeiter mit diesen Grundsätzen vertraut und dokumentieren Sie dies. Verdeutlichen Sie dabei die Grundsätze mit praktischen Beispielen, um das Verständnis dafür zu fördern.

Der Nachweis der Einhaltung der DS-GVO kann auch über **genehmigte Verhaltensregeln** erfolgen, die z. B. durch Branchenverbände definiert und durch die zuständigen Aufsichtsbehörden bestätigt werden. Je nach inhaltlicher Ausgestaltung können diese Verhaltensregeln dann auch bei der Einschaltung von Dienstleistern herangezogen werden.

Hinweis

Informieren Sie sich, ob es für Ihre Branche oder für Ihre Tätigkeiten genehmigte Verhaltensregeln gibt. Daraus können Sie Rechtssicherheit in der Umsetzung der Anforderungen der DS-GVO erhalten.

2.2 Datenschutzbeauftragter

Wer in Deutschland[4] bisher schon einen Datenschutzbeauftragten zu bestellen hatte, wird auch weiterhin einen benennen müssen. Die DS-GVO sieht in Art. 37 vor,

- dass jede öffentliche Stelle einen benennen muss.
- Ebenso müssen Unternehmen, zu deren Kerntätigkeit in der Verarbeitung personenbezogener Daten liegt, die eine regelmäßige Überwachung von betroffenen Personen erforderlich machen,
- aber auch jedes Unternehmen zu deren Kerntätigkeit die Verarbeitung personenbezogene Daten besonderer Kategorien gehört, einen Datenschutzbeauftragten benennen. Daten besonderer Kategorien (Art. 9) umfassen Gesundheitsdaten, biometrische oder genetische Daten, religiöse oder weltanschauliche Überzeugungen, rassische und ethnische Herkunft, politische Meinungen und Daten zu Sexualleben oder der sexuellen Orientierung und Gewerkschaftszugehörigkeit.

Im BDSG (2018) werden weitere Voraussetzungen definiert, nach denen ein Datenschutzbeauftragter zu benennen ist:

- mindestens zehn Personen sind mit der automatisierten Verarbeitung personenbezogener Daten befasst;
- das Unternehmen muss eine Datenschutz-Folgenabschätzung (siehe unten)

[4] Durch die Öffnungsklausel in Art. 37 Abs. 4 differenzieren die nationalen Vorgaben. Österreich z. B. hat von dieser Regelung, weitere Benennungsvoraussetzungen vorgeben zu können, bislang keinen Gebrauch gemacht.

Der Datenschutzbeauftragte kann weiterhin ein externer Dienstleister sein; er kann als Konzerndatenschutzbeauftragter benannt oder auch bei Verbänden angesiedelt werden.

Die Benennung eines Datenschutzbeauftragten befreit das Management nicht von der eigenen Verantwortung: Die meisten Aufgaben aus der DS-GVO richten sich direkt an das Management. Der Datenschutzbeauftragte hat nur eine beratende, unterstützende Funktion und dient als Ansprechpartner für betroffene Personen und Aufsichtsbehörden. Für benannte Datenschutzbeauftragte ist das Arbeitsverhältnis bezogen auf ihre datenschutzberatende Tätigkeit weisungsfrei auszugestalten, sie unterliegen einem Benachteiligungsverbot, sind mit angemessenen Mitteln auszustatten, wozu auch Fortbildungsmöglichkeiten gehören. Aus dem BDSG (2018) ergibt sich zudem ein besonderer Kündigungsschutz – wie bisher auch.

Hinweis

Überlegen Sie frühzeitig, ob Sie einen internen Mitarbeiter mit dieser Aufgabe betrauen oder einen externen Spezialisten beauftragen. Viele der externen Datenschutzbeauftragten haben sich auf Branchen spezialisiert und kennen die branchenüblichen Besonderheiten. Klären Sie klar das übertragene Aufgabengebiet ab. Der Datenschutzbeauftragte kann auch weitere Aufgaben übernehmen, so lange diese nicht zu einem Interessenskonflikt führen (z. B. beim Leiter Personal oder IT-Beauftragten).

2.3 Verzeichnis der Verarbeitungstätigkeit

Jeder Verantwortliche muss ein Verzeichnis seiner Verarbeitungstätigkeiten führen, in dem er entsprechend den Vorgaben aus Art. 30 Abs. 1 Informationen auflistet. Zwar sieht die DS-GVO nur vor, dass dieses Verzeichnis der Aufsichtsbehörde auf Anforderung vorzulegen ist, doch kann es auch gleichzeitig als Managementinformationsgrundlage für Entscheidungen dienen. Aus ihm ist ersichtlich, welche Kategorien von Daten für welchen Zweck verarbeitet werden und welche Schutzmaßnahmen dafür vorgesehen sind. Ebenso wird hier dokumentiert, an welche Empfänger die Daten weitergegeben werden. Auch wenn die DS-GVO die Möglichkeit bietet, dass in bestimmten Fällen (Art. 30 Abs. 5) auf dieses Verzeichnis verzichtet werden kann, empfiehlt es sich, eines zu führen, um zentral entscheidungserhebliche Informationen zu bündeln und Dokumentationsanforderungen gerecht zu werden. Hinweis

Ergänzen Sie Ihr Verzeichnis der Verarbeitungstätigkeiten um weitere Informationen wie

Rechtsgrundlage (insb. berechtigtes Interesse),

die Erforderlichkeit der Daten bei konkreter Verarbeitungstätigkeit,

die Klassifikation des Schutzbedarfs der Daten,

eine Aussage zur Datenschutz-Folgenabschätzung,

Löschmaßnahmen gemäß eines Löschkonzepts

und die Dokumentation, dass Sie bei der Verarbeitung einen Prozess der Betroffenenrechte wie Information, Beauskunftung und Berichtigung haben.

So haben Sie eine zentrale Stelle, aus der Sie der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO nachkommen können.

2.4 Sicherheit

Entgegen den bisherigen Regelungen im BDSG werden Anforderungen an die Sicherheit eine zentrale Anforderung an den Verantwortlichen und den Auftragsverarbeiter. Neben der Berücksichtigung der Anforderungen an eine **datenschutzfreundliche Technikgestaltung** und **datenschutzfreundliche Voreinstellung**, sind die Schutzmaßnahmen in Abhängigkeit des jeweiligen Risikos für die Rechte und Freiheiten der natürlichen Person umzusetzen.

Die Schutzziele der Informationssicherheit der **Vertraulichkeit, Integrität** und **Verfügbarkeit** werden durch den Begriff der **Belastbarkeit** erweitert. Verantwortliche und Auftragsverarbeiter müssen somit auch die Belastbarkeit ihrer Dienste und Systeme sicherstellen. Um geeignete technische und organisatorische Maßnahmen treffen zu können, muss zunächst der Schutzbedarf der zu verarbeitenden personenbezogenen Daten festgelegt werden. Die daraus abzuleitenden Schutzmaßnahmen sind auch im Hinblick auf die Risiken auszuwählen, die sich durch die Verarbeitung für natürliche Personen ergeben können.

Die Ermittlung des angemessenen Schutzniveaus erfolgt unter Berücksichtigung der Risiken, d. h. es muss eine **Risikoanalyse** durchgeführt werden.

Höhe des Risikos für die Rechte und Freiheiten natürlicher Personen	=	Eintrittswahrscheinlichkeit einer Bedrohung	x	Schwere der Auswirkungen (= Schadenspotenzial)

Unter Berücksichtigung bestimmter Punkte (z. B. Stand der Technik, den Implementierungskosten, der Art, des Umfangs und der Zwecke der Datenverarbeitung, der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen etc.), sind technische und organisatorische Schutzmaßnahmen festzulegen. Diese müssen geeignet sein, die Datenschutzgrundsätze (z. B. Datenminimierung etc.) wirksam umzusetzen, die Anforderungen der DS-GVO zu erfüllen und die Rechte der betroffenen Personen zu schützen.

Durch geeignete Voreinstellungen ist außerdem sicherzustellen, dass personenbezogene Daten nur zweckbezogen verarbeitet und nur berechtigten Personen zugänglich gemacht werden.

Art. 32 bezieht sich auf die **Sicherheit der Verarbeitung**, um ein dem o. g. Risiko angemessenes Schutzniveau zu gewährleisten. Hierfür hat der Verantwortliche ebenfalls wieder unter Berücksichtigung der o. g. Punkte (Stand der Technik etc.) geeignete technische und organisatorische Schutzmaßnahmen zu treffen, um Daten vor Vernichtung, Verlust, unbefugter Offenlegung, unbefugtem Zugang, unbefugter Speicherung etc. zu schützen. Hierzu gehören auch die Konzeption eines Löschkonzepts und daraus abgeleitete Löschmaßnahmen. Dies beinhaltet die Zuordnung einzelner Daten oder Verarbeitungsschritte zu einem definierten internen Vorgehen, das die Löschung nach einem vorher festgelegten Zeitraum sichert. Bei Bewerberdaten könnten beispielsweise die Daten der abgelehnten Bewerber nach einem Zeitraum von 6 Monaten nach Abschluss der Besetzung gelöscht werden.

Folgende Schutzmaßnahmen legt einem der Gesetzgeber u. a. hierfür nahe:

- Pseudonymisierung und Verschlüsselung
- Sicherstellen der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit personenbezogener Daten
- Fähigkeit der raschen Wiederherstellbarkeit nach einem physischen oder technischen Zwischenfall
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit von Maßnahmen zur Gewährleistung der Sicherheit
- Schritte, die sicherstellen, dass unterstellte Personen Daten nur auf Anweisung verarbeiten

Hinweis

Beziehen Sie Ihren Verantwortlichen für die Informationssicherheit mit ein. Die meisten dieser Schutzmaßnahmen sollten Sie bereits in eigenem Interesse umgesetzt haben, um die Risiken für Ihr Unternehmen durch eingeschränkte Verfügbarkeit oder unberechtigte Änderung/Kenntnisnahme zu minimieren.

Durch eine regelmäßige Überprüfung, Bewertung und Anpassung der Schutzmaßnahmen muss der Verantwortliche im Rahmen seiner Rechenschaftspflicht nachweisen können, dass die Verarbeitungstätigkeiten konform sind mit den Anforderungen der DS-GVO. Bereits bestehende Prozesse der Informationssicherheit nach dem **PDCA-Zyklus** (**P**lan-**D**o-**C**heck-**A**ct) können dabei zu Synergieeffekten führen. Genehmigte Verhaltensregeln und Zertifizierungen werden somit an Bedeutung gewinnen. Diese können herangezogen werden, um die Erfüllung der Schutzmaßnahmen nachzuweisen.

Eingesetzte Systeme sollten den Grundsatz „Datenschutz durch Technikgestaltung“ bzw. „datenschutzfreundliche Voreinstellungen“ berücksichtigen (data protection by design und by default), z. B. keine Datenerhebung nicht benötigter Daten oder die Zugriffsrechtevergabe nach dem Freigabeprinzip.

Hinweis

Diese Anforderungen werden sich mittelbar auf die Konzeption von Produkten zur Datenverarbeitung auswirken. Sie können diese Anforderungen bei der Auswahl von Produkten künftig stärker berücksichtigen.

2.5 Datenschutz-Folgenabschätzung

Entsteht voraussichtlich durch die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten einer natürlichen Person, muss der Verantwortliche eine Datenschutz-Folgenabschätzung gemäß Art. 35 durchführen.

Diese kann sehr umfangreich ausfallen und die Aufsichtsbehörden haben hierbei konkrete Vorstellungen, unter welchen Voraussetzungen und wie diese umzusetzen ist. Sofern ein Datenschutzbeauftragter benannt wurde, ist dieser hinzuzuziehen.

Hinweis

Unterschätzen Sie den Aufwand hierbei nicht. Eine frühzeitige Planung und eine evtl. zeitliche Verzögerung bei größeren Projekten sollten Sie berücksichtigen.

Besteht auch trotz Schutzmaßnahmen weiterhin ein hohes Risiko, muss der Verantwortliche vor Beginn der Verarbeitung seine Datenschutzaufsichtsbehörde gemäß Art. 36 konsultieren. Hierbei informiert der Verantwortliche über das geplante Vorgehen und übergibt auch die Dokumentation der Datenschutz-Folgenabschätzung. Weitere Informationen können durch die Aufsichtsbehörde angefordert werden, die innerhalb von acht Wochen eine Empfehlung abgibt. Diese Frist kann bei komplexen Sachverhalten um weitere sechs Wochen verlängert werden. In manchen Kommentaren wird die Ansicht vertreten, dass eine Verarbeitung vor der Reaktion der Aufsichtsbehörde nicht erfolgen dürfe.

Hinweis

Beobachten Sie die Meinungsbildung. Selbst wenn eine Verarbeitung nicht von einer Genehmigung der Aufsichtsbehörde abhängt, berücksichtigen Sie das Risiko, dass die Aufsichtsbehörde noch Empfehlungen gibt, die sich auf die prozessuale Gestaltung der Verarbeitung oder die Formulierung von Texten auswirken können.

2.6 Betroffenenrechte

Die betroffenen Personen haben umfassende Rechte, die das **Transparenzgebot**, dem der Verantwortliche unterliegt, ausgestalten. Diese beinhalten das Informationsrecht, Auskunftsrecht, Recht auf Widerspruch bei bestimmten Verarbeitungskonstellationen, das Recht auf Datenportabilität, das Recht auf Berichtigung und Löschung („Recht auf Vergessenwerden“) gegenüber dem Verantwortlichen. Die Details können zu komplexen internen Verfahren führen, denn auch diese unterliegen der Rechenschaftspflicht. Teilweise werden die Betroffenenrechte unter bestimmten gesetzlichen Voraussetzungen eingeschränkt, eine fachkundige Beratung hierzu wird unerlässlich sein. Auch wenn die Betroffenenrechte im Prinzip schon unter dem bisherigen BDSG bekannt waren: Neue Rechte wie Datenportabilität, die Anforderungen an eine klare sprachliche Formulierung oder die Einführung von Erledigungsfristen bei Auskunftsansprüchen macht eine Befassung damit unumgänglich.

Hinweis

Binden Sie insbesondere bei den Betroffenenrechten von Beschäftigen auch eine evtl. vorhandene Mitarbeitervertretung ein. Über Betriebsvereinbarungen lassen sich Prozesse definieren, wie Sie den Betroffenenrechten bei Beschäftigten nachkommen und somit für Rechtssicherheit sorgen können.

2.7 Meldepflichten nach DS-GVO

Alle **Verletzungen des Schutzes personenbezogener Daten** (Art. 4 Nr. 9) müssen Sie dokumentieren (Art. 33 Abs. 5) und gemäß Art. 33 Abs. 1 ohne unangemessene Verzögerung und möglichst binnen 72 Stunden nach Bekanntwerden der zuständigen Aufsichtsbehörde melden. Die Meldepflicht entfällt, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt. Wenn die Wahrscheinlichkeit besteht, dass die Verletzung ein hohes Risiko für die persönlichen Rechte und Freiheiten der natürlichen Person bewirkt, so haben Sie die Betroffenen ohne unangemessene Verzögerung in klarer und einfacher Sprache zu informieren (Art. 34). Allerdings darf gemäß § 43 Abs. 4 BDSG (2018) eine erfolgte Meldung nur mit Zustimmung des Meldepflichtigen in Bußgeldverfahren verwendet werden.

Hinweis

Richten Sie einen internen Prozess ein, dass Ihre Mitarbeiter wissen, wen Sie bei Verdacht einer Schutzverletzung intern informieren müssen, sodass diese Stelle innerhalb der Frist eine Entscheidung treffen kann. Ihre Auftragsverarbeiter sind in diese Informationskette entsprechend einzubinden.

2.8 Auftragsverarbeitung

Die Einschaltung eines Dienstleisters bei der Verarbeitung personenbezogener Daten wird im Regelfall über eine Auftragsverarbeitung abgebildet: Der Dienstleister ist streng **weisungsgebunden**, der Auftraggeber bleibt im datenschutzrechtlichen Sinne weiterhin verantwortlich für die Rechtmäßigkeit der Verarbeitung und die Einhaltung der Betroffenenrechte, auch wenn der Auftragsverarbeiter zusätzlich durch die DS-GVO stärker direkt adressiert wird. Aufgrund der weiterhin bestehenden Hauptverantwortlichkeit des Auftraggebers für die ordnungsgemäße Datenverarbeitung brauchen Sie keine weitere Rechtmäßigkeitsgrundlage für die Einschaltung eines Dienstleisters, wenn Sie die Vorgaben des Art. 28 beachten. Der Auftraggeber muss mit dem Auftragsverarbeiter eine Vereinbarung abschließen, deren Mindestregelungsgehalt durch die DS-GVO in Art. 28 vorgegeben wird. Vieles davon ist bereits aus der bisherigen Gestaltung aus § 11 BDSG bekannt. Dennoch kann sich aus neuen Begrifflichkeiten, die Interpretationsspielraum bieten, Handlungsbedarf ergeben. So darf als Auftragsverarbeiter nur ausgewählt werden, wer hinreichende Garantien bieten kann, dass die Verarbeitung im Einklang mit der Verordnung durchgeführt wird und der Einsatz weiterer Auftragsverarbeiter muss durch den Auftragsverarbeiter mit dem Verantwortlichen abgestimmt werden.

Hinweis

Prüfen Sie, ob es Anpassungsbedarf für Ihre aktuellen Auslagerungen von Tätigkeiten gibt. Passen Sie die Verträge baldmöglichst an.

Für die vertragliche Ausgestaltung gibt es bereits von Verbänden Musterformulierungen, an denen man sich orientieren kann. Auch bei Musterformulierungen der Aufsichtsbehörden empfiehlt es sich, fachlichen Rat für die Umsetzung einzuholen, insbesondere, wenn es sich um Formulierungen handelt, deren Regelungsbedarf sich nicht aus der DS-GVO ableiten lässt.

Hinweis

Auch die EU-Kommission und Aufsichtsbehörden dürfen Standardvertragsklauseln festlegen, an denen Sie sich orientieren können. Beobachten Sie diese Entwicklung!

Noch nicht abschließend geklärt ist der Sachverhalt, wenn ein Dienstleister bei Erbringung seiner Tätigkeit personenbezogene Daten zur Kenntnis nehmen kann, auch wenn er keinen direkten Auftrag hat, diese irgendwie zu verarbeiten (Bsp. **Fernwartung**). Bislang waren über § 11 Abs. 5 BDSG die Vorgaben zur Auftragsverarbeitung entsprechend anzuwenden. Eine solche Regelung gibt es in der DS-GVO aber nicht. Die deutschen Aufsichtsbehörden gehen hier nun von einer Auftragsverarbeitung aus, verweisen aber dabei darauf, dass diese Ansicht unter dem Vorbehalt einer Meinungsbildung der Europäischen Aufsichtsbehörde steht.

Hinweis

Bei der datenschutzrechtlichen Gestaltung der Vereinbarung zur Auftragsverarbeitung sollten Sie sich fachkundig beraten lassen. Die Meinungsentwicklung bei den Detailfragen sind dabei im Auge zu behalten.

Befindet sich der Dienstleister außerhalb der EU/bzw. des EWR (sogenannte „Drittstaaten“), sind darüber hinaus die Vorgaben der DS-GVO zu beachten, um sicherzustellen, dass auch beim empfangenden Unternehmen ein angemessenes Datenschutzniveau vorliegt. Das kann durch einen **Angemessenheitsbeschluss** der EU-Kommission geschehen, der pauschal für das ganze Land gilt, wie bei der Schweiz. Oder das empfangende Unternehmen hat sich unternehmensweiten Verhaltensregeln (**C**orporate **B**inding **R**ules – **BCR**) unterworfen, die durch eine europäische Aufsichtsbehörde bestätigt wurden, eine entsprechende Zertifizierung liegt vor, oder die betroffene Person hat eingewilligt. Auch hat die EU-Kommission **Standardvertragsklauseln** veröffentlicht, deren unveränderter Abschluss zwischen datenexportierenden und datenimportierenden Unternehmen dafür sorgt, dass beim Empfänger ein angemessenes Datenschutzniveau angenommen wird.

Eine Sonderregelung gibt es für die USA: Hier ist das **EU-USA Privacy Shield** eine Sonderform des Angemessenheitsbeschlusses, der nur gilt, wenn sich Unternehmen in den USA den Regelungen unterwerfen und diese anwenden. Hinsichtlich der USA stehen EU-USA Privacy Shield und Standardvertragsklauseln in der Kritik, weil umstritten ist, ob diese aufgrund der rechtlichen Rahmenbedingungen in den USA für ein ausreichendes Datenschutzniveau sorgen können.

Hinweis

Es ist nicht auszuschließen, dass sich mit dieser Frage bald der Europäische Gerichtshof (EuGH) zu befassen hat. Eine Entscheidung des EuGH kann daher direkten Einfluss auf die Rechtmäßigkeit Ihrer Datenweitergabe haben. Beobachten Sie daher die Meinungsbildung auch auf europäischer Ebene.

Unternehmen, die als Auftragsverarbeiter am Markt auftreten, werden viel stärker in die Pflicht genommen als bisher. Schutzmaßnahmen, Dokumentationspflichten und auch die direkte Adressierung von Bußgeldern machen es erforderlich, sich hier intensiv mit der DS-GVO zu befassen.

Hinweis

Beobachten Sie als Auftragsverarbeiter den Markt der Zertifizierungen und anderweitiger Nachweismöglichkeiten. Sie sollten als Dienstleister in der Lage sein, Ihren Kunden einen Nachweis der Einhaltung geeigneter Garantien anzubieten, der eine aufwändige Prüfung von Unterlagen oder eine vor-Ort-Inspektion nicht erforderlich macht.

Des Weiteren gibt es Auslagerungen von Tätigkeiten, die **keine Auftragsverarbeitung** darstellen z. B. die Mandatierung von Rechtsanwälten, Steuerberatern oder Wirtschaftsprüfern. Agieren diese im Rahmen ihres berufsrechtlich geregelten Aufgabenbereiches, so nehmen sie diese Tätigkeiten weisungsfrei wahr und werden zu einem neuen Verantwortlichen. Bei Steuerberatern umfasst dies z. B. auch die Beratung und Durchführung der Lohn- und Gehaltsabrechnung. Die Rechte der betroffenen Personen können dann aufgrund der vorrangigen berufsrechtlichen Verschwiegenheit eingeschränkt sein.

Einigen sich zwei Verantwortliche auf eine **gemeinsame Verarbeitung** zu einem gemeinsamen Zweck, kann nach Art. 26 DS-GVO eine gemeinschaftliche Verantwortlichkeit vorliegen. Dabei ist gegenüber den betroffenen Personen transparent zu machen, durch wen die Betroffenenrechte wahrzunehmen sind. Diese Gestaltungsform war im bisherigen BDSG nicht abgebildet. Sie bietet sich an bei einem konzernweiten Zusammenschluss der Kundendatenbank oder einer zentralen Personalverwaltung. Aber auch hier wird eine Rechtmäßigkeitsgrundlage erforderlich, die im Regelfall in der Wahrung berechtigter Interessen (Art. 6 (1) lit. f DS-GVO) zu finden sein wird.

2.9 Beschäftigtendatenschutz

Der Beschäftigtendatenschutz ist künftig in § 26 Abs. 1 ff. BDSG (2018) geregelt. Die Mitgliedstaaten haben hierzu die Befugnis über die Öffnungsklausel in Art. 88. Inhaltlich ergeben sich keine gravierenden Änderungen gegenüber den bisherigen Regelungen.

Mitarbeiterdaten dürfen für Zwecke des Beschäftigtenverhältnisses verarbeitet werden, wenn die Verarbeitung für die Entscheidung über das Beschäftigtenverhältnis oder für die Durchführung und Beendigung des Beschäftigtenverhältnisses erforderlich ist. Zur Aufdeckung von Straftaten dürfen Mitarbeiterdaten nur nach einem zu dokumentierenden Anfangsverdacht und einer Interessenabwägung verarbeitet werden.

Eine Einwilligung im Beschäftigtenverhältnis ist möglich, muss jedoch freiwillig erteilt worden sein. Freiwilligkeit kann insbesondere vorliegen, wenn für den Mitarbeiter ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und Mitarbeiter gleichgelagerte Interessen verfolgen. Damit bleibt z. B. die Veröffentlichung von Mitarbeiterfotos auf Webseiten weiterhin problematisch.

Hinweis

Ein Arbeitgeber unterliegt bei der Einwilligung durch Beschäftigte der Rechenschaftspflicht, sodass sich auch hier mindestens eine Textform empfiehlt, wenn Sie eine Verarbeitung auf Basis einer Einwilligung durchführen möchten.

3 Rahmenbedingungen und weiteres Vorgehen

3.1 Aufsichtsbehörde

Ihre bisherige Datenschutzaufsichtsbehörde bleibt unverändert. Den Aufsichtsbehörden kommen nun neben der Beratung und Überwachung auch vielfältige Aufgaben im Rahmen der europaweiten Abstimmung mit den anderen Aufsichtsbehörden zu. Im Rahmen ihrer Aufgabenerfüllung können Aufsichtsbehörden Anordnungen treffen, die Verarbeitungen untersagen können. Auch erweitert sich nun der Anwendungsbereich durch das festgelegte Marktortprinzip auf alle Unternehmen, die im europäischen Raum Daten verarbeiten. Damit werden auch Unternehmen erfasst, die ihren Sitz außerhalb der Europäischen Union haben. Allein entscheidend ist, dass hier Verarbeitungen von personenbezogenen Daten angeboten werden. Diese Unternehmen müssen dann für die datenschutzrechtlichen Themen einen Vertreter benennen. Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten hängt dann eindeutig nicht mehr vom Sitz des verarbeitenden Unternehmens ab.

Hinweis

Prüfen Sie, welche Aufsichtsbehörde für Sie zuständig ist und machen sich mit deren Webseite vertraut. Oft lassen sich daraus Ansprechpartner für konkrete Fragestellungen und viele Informationen zu Themenkomplexen entnehmen. In den regelmäßig erscheinenden Tätigkeitsberichten der Aufsichtsbehörden finden sich zudem auch Orientierungshilfen in Einzelfragen.

Bei internationalen Fragestellungen, also Verarbeitungen, die gegenüber Personen in mehreren Mitgliedstaaten der Europäischen Union erfolgen, wurde ein „One-Shop-Stop“ eingeführt. Dies bezeichnet die Möglichkeit, alle notwendigen bürokratischen Schritte, die zur Erreichung eines Zieles führen, an einer einzigen Stelle durchzuführen. Die beteiligten Aufsichtsbehörden koordinieren sich dann in der Meinungsbildung untereinander.

3.2 Internetaktivitäten

Bislang werden die datenschutzrechtlichen Anforderungen beispielsweise bei der Betreibung einer Webseite über das Telemediengesetz in Deutschland geregelt. Auf europäischer Ebene wird aktuell über eine Verordnung namens ePrivacy verhandelt, die dann europaweit die Verarbeitung von personenbezogenen Daten im Rahmen von Online-Anwendungen regelt. Dies betrifft u. a. den Einsatz von Cookies, Reichweitenmessung etc.

Derzeit ist nicht abzusehen, mit welchen konkreten Vorgaben hier zu rechnen sein wird, die konkrete Hinweise rechtfertigen würden.

Hinweis

Beobachten Sie die weitere Entwicklung im Gesetzgebungsprozess. Es ist davon auszugehen, dass eine Umsetzungsfrist sehr knapp ausfallen wird. Wenn Sie Ihre Webseite von einem externen Dienstleister erstellen lassen, vereinbaren Sie vertraglich, ob und wenn ja, welche personenbezogenen Daten bei der Nutzung Ihrer Webseite erhoben werden sollen und dokumentieren Sie für sich, für welchen Zweck Sie diese verwenden möchten. Ihre Webseite muss dann bereits jetzt eine leicht zugängliche Datenschutzerklärung enthalten, in der Sie u. a. über die Verarbeitung dieser Daten informieren.

3.3 Erste Schritte

Für erste Schritte ist es nie zu spät!

- Definieren Sie interne Zuständigkeiten für die einzelnen Aufgaben der DS-GVO. Berücksichtigen Sie dabei, dass der Datenschutzbeauftragte nur eine beratende und überwachende Funktion hat, um das Management bei seiner Aufgabe zu unterstützen, regelkonform zu agieren.

- Ausgehend von Ihrem bisherigen Verfahrensverzeichnis nach § 4d BDSG, sollten Sie sich einen Überblick über die bereits bestehenden Verarbeitungen verschaffen. Ergänzen Sie diese Angaben um die neuen Anforderungen aus dem Verzeichnis für Verarbeitungstätigkeiten aus Art. 30 Abs. 1. Sind Sie als Auftragsverarbeiter tätig, berücksichtigen Sie zusätzlich die Anforderungen aus Art. 30 Abs. 2.

- Legen Sie den jeweiligen Dokumentationsumfang zur Erfüllung der Rechenschaftspflicht fest.

- Prüfen Sie mit Ihren intern zuständigen Mitarbeitern für die jeweilige Verarbeitung, ob die Rechte der betroffenen Personen auf Information, Auskunft, Berichtigung und Löschung etc. umgesetzt werden könnten. Setzen Sie Projekte auf, um dies ggf. zu ermöglichen und den Nachweis über eine Dokumentation zu führen.

- Analysieren Sie bei bestehenden Verarbeitungsprozessen, ob die Konzeption, Umsetzung und Dokumentation der Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten die Vorgaben aus Art. 32 erfüllt werden.

- Implementieren Sie Informations- und Meldeprozesse, um bei Schutzverletzungen zeitnah reagieren zu können.

- Informieren Sie Ihren Einkauf, dass Verträge mit Ihren Dienstleistern, die in Ihrem Auftrag Daten verarbeiten, überprüft und angepasst werden, um den Anforderungen der DS-GVO (insb. Art. 28 und 29) zu entsprechen.

- Prüfen Sie sich selbst durch einen der bereits veröffentlichten Fragebögen zur DS-GVO, den einige Aufsichtsbehörden schon auf ihrer Webseite veröffentlicht haben.

- Beenden Sie Ihre Aktivitäten zur DS-GVO nicht mit dem Lesen dieser Information! Diese gibt Ihnen nur einen überblickartigen Einstieg, um das Verständnis für die Komplexität zu erleichtern. Es gibt zahlreiche Angebote von Verbänden wie auch den Aufsichtsbehörden, branchenorientiert selbst bei Detailfragen zu unterstützen.

Bleiben Sie optimistisch: Abhängig von Ihrer Kerntätigkeit kann sich der Aufwand in Grenzen halten. Auch wenn Sie merken, dass Sie bis Ende Mai 2018 nicht alle Anforderungen umsetzen können, werden Aufsichtsbehörden Ihre Anstrengungen bei einer Prüfung berücksichtigen, wenn Sie diese entsprechend belegen können.

3.4 Weitere Informationen

Zahlreiche Verbände und Einrichtungen stellen derzeit Informationen bereit. Ferner informieren die Aufsichtsbehörden in Kurzpapieren über ihre Interpretation und die Arbeitsgemeinschaft der Europäischen Aufsichtsbehörden („Art. 29 Datenschutzgruppe“) veröffentlicht Guidelines und Empfehlungen aus ihrer Sicht. Die Empfehlungen und die Interpretation der Aufsichtsbehörde sind aber nur eine Art der Interpretation, letztendlich wird der Europäische Gerichtshof über unklare Formulierungen und widersprüchliche Anforderungen aus der DS-GVO zu entscheiden haben.

Verbände:

- Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.: *www.bitkom.org*
- Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.: *www.bvdnet.de*
- Gesellschaft für Datenschutz und Datensicherheit: *www.gdd.de*

Aufsichtsbehörde, statt vieler:

- Bayerisches Landesamt für Datenschutzaufsicht: *www.lda.bayern.de*

Leitfäden der Art. 29-Datenschutzgruppe:

- *http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360&tpa_id=6936*