Bundesministerium des Innern, für Bau und Heimat

Häufig nachgefragt

Datenschutz-Grundverordnung

Was sind die Ziele und wesentlichen Neuerungen der Datenschutz-Grundverordnung?

Die Verordnung (EU) 2016/679 (EU-Datenschutz-Grundverordnung) löst die Europäische Datenschutzrichtlinie aus dem Jahr 1995 (RL 95/46/EG) mit dem Ziel der Harmonisierung und Modernisierung des europäischen Datenschutzrechts ab. Sie fördert den Schutz der Betroffenen bei der Verarbeitung personenbezogener Daten und den freien Verkehr solcher Daten (Artikel 1 Absatz 1 Datenschutz-Grundverordnung).

Die bis zum 25. Mai 2018 geltende Datenschutzrichtlinie hatten die Mitgliedstaaten sehr unterschiedlich umgesetzt. Dieser Flickenteppich mitgliedstaatlicher Regelungen hinderte den grenzüberschreitenden Datenverkehr in der Europäischen Union. Die Datenschutz-Grundverordnung schafft einen einheitlichen und unmittelbar geltenden Rechtsrahmen, der den freien Verkehr personenbezogener Daten in der Europäischen Union gewährleistet. Dies ist eine wichtige Voraussetzung für die Vollendung des digitalen Binnenmarkts und für gleiche Wettbewerbsbedingungen in der Europäischen Union. Zu einer einheitlichen Rechtsanwendung trägt der Europäische Datenschutzausschuss, der Zusammenschluss der Aufsichtsbehörden aller Mitgliedstaaten auf der Ebene der Europäischen Union, bei. Dieser entscheidet künftig verbindlich über zentrale Fragen der Datenschutz-Grundverordnung. Mit der federführenden Aufsichtsbehörde am Ort der Hauptniederlassung steht Unternehmen mit grenzüberschreitenden Datenverarbeitungstätigkeiten künftig ein zentraler Ansprechpartner zur Verfügung (sog. One Stop Shop-Prinzip).

Gleichzeitig wird das europäische Datenschutzrecht modernisiert und das Grundrecht auf Schutz der personenbezogenen Daten aus Artikel 8 der Europäischen Grundrechtecharta gestärkt. Die Betroffenen erhalten mehr Kontrolle und Transparenz bei der Datenverarbeitung, auch und gerade im digitalen Zeitalter. Durch die Datenschutz-Grundverordnung werden die Anforderungen an eine rechtswirksame Einwilligung der betroffenen Personen erhöht und deren Rechte, insbesondere auf Information und Auskunft, erweitert. Die Datenschutzbehörden erhalten weit reichende Abhilfebefugnisse; bei Verstößen gegen die Datenschutz-Grundverordnung können sie Geldbußen bis zu 20 Mio. € oder 4 Prozent des weltweiten Jahresumsatzes verhängen. Auch Unternehmen außerhalb der Europäischen Union unterliegen der Datenschutz-Grundverordnung, wenn sie Waren oder Dienstleistungen in der Europäischen Union anbieten oder das Verhalten von Personen in der Europäischen Union beobachten (sog. Marktortprinzip).

Für wen gilt der neue Rechtsrahmen?

Die Datenschutz-Grundverordnung gilt grundsätzlich für jegliche Verarbeitung personenbezogener Daten. Einzelheiten regeln die Artikel 2 und 3 Datenschutz-Grundverordnung.

Sowohl öffentliche (Behörden, Gerichte und andere öffentliche Stellen ungeachtet ihrer Rechtsform) als auch nicht-öffentliche (natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des Privatrechts) Stellen haben die Anforderungen der Datenschutz-Grundverordnung zu beachten, wenn sie Informationen über eine identifizierte oder identifizierbare natürliche Person verarbeiten.

Ausnahmen gelten insbesondere

- bei der nicht automatisierten Verarbeitung personenbezogener Daten, die nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen - beispielsweise Akten und Aktensammlungen, die nicht nach bestimmten Kriterien geordnet sind;

- für natürliche Personen, die personenbezogene Daten zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten verarbeiten - beispielsweise privater Schriftverkehr, Adressbücher oder die Nutzung sozialer Netzwerke und Online-Tätigkeiten im Rahmen persönlicher oder familiärer Zwecke;
- für Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen - insbesondere die nationale Sicherheit betreffende Tätigkeiten;
- für die Datenverarbeitung zum Zwecke der Strafverfolgung und Gefahrenabwehr durch die zuständigen Behörden - hier gilt die zeitgleich mit der Datenschutz-Grundverordnung verabschiedete Richtlinie (EU) 2016/680.

Die Datenschutz-Grundverordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeit einer Niederlassung in der Europäischen Union erfolgt oder im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen in der Europäischen Union steht (sog. Marktortprinzip). Dies gilt unabhängig davon, ob die Verarbeitung in der Europäischen Union stattfindet. Die Datenschutz-Grundverordnung gilt zudem auch dann, wenn das Verhalten betroffener Personen in der Europäischen Union beobachtet werden soll oder die Verarbeitung an einem Ort erfolgt, der aufgrund völkerrechtlicher Bestimmungen dem Recht eines Mitliedstaats der Europäischen Union unterliegt. Es spielt hierbei keine Rolle, ob die verarbeiteten Daten einen Bürger der Europäischen Union betreffen oder nicht.

Wo finde ich die wichtigsten Begriffsbestimmungen?

Artikel 4 Datenschutz-Grundverordnung enthält die zentralen Definitionen. Künftig finden sich die Begriffsbestimmungen zu personenbezogenen Daten, Verantwortlichen oder der Verarbeitung somit unmittelbar und abschließend in der Datenschutz-Grundverordnung.

Was ändert sich bei den Prinzipien des Datenschutzes und den Rechtsgrundlagen?

Die Datenschutz-Grundverordnung führt die Grundsätze für die Datenverarbeitung aus der geltenden EU-Datenschutzrichtlinie 95/46/EG, etwa die Zweckbindung, Erforderlichkeit und Datensparsamkeit, in Artikel 5 weitgehend unverändert fort.

Der Zweckbindungsgrundsatz wird ergänzt durch Artikel 6 Absatz 4, welcher Kriterien zur Prüfung kompatibler Zwecke benennt. Sind der ursprüngliche Zweck der Erhebung und der Zweck der Weiterverarbeitung durch die gleiche verantwortliche Stelle kompatibel, dürfen die Daten auf Basis der ursprünglichen Rechtsgrundlage weiterverarbeitet werden.

Mit der neuen "Rechenschaftspflicht" betont die Datenschutz-Grundverordnung die Verantwortlichkeit der Daten verarbeitenden Stellen für die Einhaltung der Prinzipien und dessen Nachweis (Artikel 5 Absatz 2 Datenschutz-Grundverordnung).

Artikel 6 Datenschutz-Grundverordnung zählt die Zulässigkeitstatbestände für die Verarbeitung personenbezogener Daten auf. Auch er entspricht weitgehend geltendem europäischen Datenschutzrecht. Wie bisher bedarf jegliche Verarbeitung personenbezogener Daten einer legitimierenden Rechtsgrundlage - unabhängig davon, ob von der Verarbeitung ein hohes oder geringes Risiko für die Rechte und Freiheiten der betroffenen Personen ausgeht. Dieses "Verbot mit Erlaubnisvorbehalt" stützt sich auf Artikel 8 der EU-Grundrechtecharta.

Eine Verarbeitung personenbezogener Daten ist nur rechtmäßig

- mit der Einwilligung der betroffenen Person

oder wenn die Verarbeitung erforderlich ist

- für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen ,
- zum Schutz lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person,
- zur Wahrung berechtigter Interessen des Verantwortlichen oder Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen,
- zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen oder
- für die Wahrnehmung einer im öffentlichen Interesse liegenden oder in Ausübung hoheitlicher Gewalt erfolgenden Aufgabe des Verantwortlichen.

Diese Zulässigkeitstatbestände bilden ein abschließendes System; die Mitgliedstaaten dürfen jedoch in einigen Bereichen die Anforderungen an die Rechtmäßigkeit der Verarbeitung durch nationales Datenschutzrecht konkretisieren und präzisieren (Artikel 6 Absatz 2 und 3 Datenschutz-Grundverordnung). Viele Rechtsgrundlagen, insbesondere für die Verarbeitung personenbezogener Daten durch öffentliche Stellen, finden sich daher nach wie vor im allgemeinen oder besonderen Datenschutzrecht auf nationaler Ebene.

Artikel 7 und 8 enthalten konkretisierende Bedingungen für die Einwilligung. Der deutsche Gesetzgeber hat vorerst nicht von der Möglichkeit Gebrauch gemacht, die Altersgrenze für die Einwilligung eines Kindes bei Nutzung der Dienste der Informationsgesellschaft abweichend von der Datenschutzgrund-Verordnung (16 Jahre) zu regeln.

Nach Artikel 9 Datenschutz-Grundverordnung ist - wie bisher - die Verarbeitung besonders sensibler Daten nur ausnahmsweise zulässig. Zu diesen „besonderen Kategorien personenbezogener Daten“ zählen beispielsweise Daten über die ethnische Herkunft, politische Meinungen, religiöse Überzeugungen oder die sexuelle Orientierung, genetische und biometrische Daten und Gesundheitsdaten. Um diese Daten verarbeiten zu können, bedarf es stets einer Rechtsgrundlage nach Artikel 6 Absatz 1 und zusätzlich eines Ausnahmetatbestandes vom Verbot der Verarbeitung sensibler Daten. Die Ausnahmetatbestände finden sich in Artikel 9 Absatz 2 Datenschutz-Grundverordnung und ergänzend im nationalen Datenschutzrecht (z.B. in § 22 BDSG 2018 oder aber auch im bereichsspezifischen Fachrecht des Bundes).

Artikel 10 Datenschutz-Grundverordnung stellt personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten unter einen besonderen Schutz. Sie dürfen nur unter behördlicher Aufsicht verarbeitet werden oder wenn dies gesetzlich vorgesehen ist.

Artikel 11 Datenschutz-Grundverordnung bestimmt, dass Daten nicht allein deshalb gespeichert werden müssen, um eine Person identifizieren zu können (z.B. um eine Auskunft geben zu können). Dies kann z.B. dazu führen, dass bei dem Foto eines Bauwerks, auf dem unbekannte Personen zu sehen sind, nicht Daten wie Namen, Adresse etc. erhoben werden müssen, um die abgebildete Person zu informieren.

Gelten Einwilligungen der Betroffenen nach altem Recht fort?

Gemäß Erwägungsgrund 171 Satz 3 Datenschutz-Grundverordnung gelten Einwilligungen dann fort und es bedarf keiner erneuten Einwilligung, wenn "die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht". Die Bedingungen für die Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung haben die Aufsichtsbehörden des Bundes und der Länder konkretisiert.

Was ändert sich bei den Betroffenenrechten?

Um größere Transparenz im Umgang mit personenbezogenen Daten zu schaffen, erweitert die Datenschutz-Grundverordnung im Kapitel III die bestehenden Betroffenenrechte und führt zugleich neue Rechte ein. Einzelheiten regeln die Artikel 12 bis 23.

Artikel 12 enthält allgemeine Verfahrensvorschriften für die Kommunikation mit den Betroffenen, Bearbeitungsfristen und Fragen der Entgeltlichkeit. Anträge der betroffenen Personen sind grundsätzlich unentgeltlich innerhalb eines Monats in klarer und einfacher Sprache zu beantworten.

Artikel 13 und 14 Datenschutz-Grundverordnung regeln die Informationspflichten des Verantwortlichen gegenüber den betroffenen Personen. Im Vergleich zur bisherigen Rechtslage weitet sich nicht nur der Umfang, sondern auch der Anlass der Information aus. Die betroffenen Personen sind nicht nur bei der erstmaligen Erhebung, sondern grundsätzlich bei jeder beabsichtigten Weiterverarbeitung für andere Zwecke über die aufgeführten Aspekte zu unterrichten. Die Informationen hat der Verantwortliche eigeninitiativ, d.h. ohne einen Antrag der betroffenen Person, zur Verfügung zu stellen. Die Abgrenzung, wann Daten bei der betroffenen Person erhoben werden oder nicht, ist im Einzelfall nicht leicht. Die Sichtweise, wonach Artikel 13 Datenschutz-Grundverordnung voraussetzt, dass sich die betroffene Person der Datenerhebung bewusst sein muss, erscheint vorzugswürdig. Dies führt im Fall von Videoaufzeichnungen oder Fotoaufnahmen zu praxisgerechten Ergebnissen.

Neben den Informationspflichten steht der betroffenen Person nach Artikel 15 Datenschutz-Grundverordnung ein umfangreiches Auskunftsrecht über die sie betreffenden personenbezogenen Daten zu. Das Auskunftsrecht umfasst auch den Anspruch, eine unentgeltliche Kopie der verarbeiteten Daten zu erhalten.

Unter den Voraussetzungen der Artikel 16 bis 18 Datenschutz-Grundverordnung können die betroffenen Personen die Berichtigung, Löschung und Einschränkung der Verarbeitung verlangen. Das Recht auf Löschung umfasst zugleich das sog. "Recht auf Vergessen werden": Hat der Verantwortliche die personenbezogenen Daten öffentlich und damit anderen Verantwortlichen zugänglich gemacht, hat er im Falle einer Löschverpflichtung angemessene Maßnahmen zu treffen, um die anderen Verantwortlichen darüber zu informieren, dass eine betroffene Person die Löschung aller Links zu bzw. Vervielfältigungen dieser personenbezogenen Daten verlangt.

Artikel 20 räumt den betroffenen Personen erstmals das Recht auf Datenübertragbarkeit ein. Betroffene haben demnach in bestimmten Fällen das Recht, ihre Daten in einem strukturierten, gängigen und maschinenlesbaren Format ausgehändigt zu erhalten, um sie von einem Verantwortlichen ohne Behinderung auf einen anderen (privaten) Anbieter übertragen zu lassen. Ausweislich der Norm geht es um die Daten, die der Betroffene "aktiv" bereitgestellt hat und nicht auch um solche, die der Verantwortliche erst erzeugt hat, wie z.B. Standortdaten. Bei dem Anspruch ist zu beachten, dass bei der Übertagung der Daten von einem auf einen anderen Verantwortlichen die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden dürfen. Dies kann z.B. der Fall sein, wenn auf einem Foto nicht nur die betroffene Person, sondern auch Dritte abgebildet sind.

Artikel 21 verleiht den betroffenen Personen das Recht, gegen eine (rechtmäßige) Datenverarbeitung aus Gründen, die sich aus ihrer besonderen Situation ergeben, Widerspruch einzulegen. Zudem besteht ein jederzeitiges Widerspruchsrecht gegen die Verarbeitung personenbezogener Daten zum Zweck der Direktwerbung. Auf das Widerspruchsrecht sind die betroffenen Personen spätestens zum Zeitpunkt der ersten Kommunikation ausdrücklich hinzuweisen.

Die Betroffenenrechte gelten nicht, wenn die Datenschutz-Grundverordnung unmittelbare Ausnahmen vorsieht oder die Mitgliedstaaten über Artikel 23 Datenschutz-Grundverordnung Beschränkungen der Betroffenenrechte vorgesehen haben. Das ab dem 25. Mai 2018 geltende Bundesdatenschutzgesetz (BDSG 2018) enthält in den §§ 32-37 für den öffentlichen wie auch den nicht-öffentlichen Bereich weitere punktuelle Beschränkungen der Betroffenenrechte.

Welche Pflichten treffen Daten verarbeitende Stellen?

Neben der Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (Kapitel II) und der Gewährleistung der Betroffenenrechte (Kapitel III) enthält Kapitel IV der Datenschutz-Grundverordnung zentrale Vorschriften für die Pflichten der Daten verarbeitenden Stellen. Diese ergeben sich künftig unmittelbar aus der Datenschutz-Grundverordnung. Im Gegensatz zur alten Rechtslage enthält das ab dem 25. Mai 2018 geltende Bundesdatenschutzgesetz daher nur sehr wenige Ausführungen zu den Verarbeiterpflichten.

Viele Verarbeiterpflichten sind konzeptionell mit der bisherigen Rechtslage in Deutschland vergleichbar, erfordern aber dennoch Anpassungen in der behördlichen und betrieblichen Praxis.

Als wesentliche Pflichten bei der Datenverarbeitung sind zu nennen:

- Gewährleistung geeigneter technischer und organisatorischer Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit, Artikel 24, 25 und 32
- Anforderungen an die Auftragsverarbeitung, Artikel 28
- Führen eines Verzeichnisses der Verarbeitungstätigkeiten, Artikel 30
- Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und Benachrichtigung der betroffenen Personen, Artikel 33 und 34
- Durchführung einer Datenschutz-Folgenabschätzung und vorherige Konsultation der Aufsichtsbehörden, Artikel 35 und 36
- Benennung eines Datenschutzbeauftragten, Artikel 37 bis 39

Prägend für die von den Verantwortlichen zu erfüllenden Pflichten ist das Konzept der Risikoadäquanz: Je wahrscheinlicher oder schwerer das von der Datenverarbeitung ausgehende Risiko, desto umfangreicher und höher sind die Pflichten des Verantwortlichen. Dieser flexible Ansatz trägt insbesondere den Belangen kleinerer und mittlerer Unternehmen Rechnung, die nicht risikobehaftete Daten verarbeiten:

- So sind bei den technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit u.a. die Eintrittswahrscheinlichkeit und Schwere des von der Datenverarbeitung ausgehenden Risikos für die betroffenen Personen im Einzelfall zu berücksichtigen.

- Von der Pflicht zur Führung eines Verarbeitungsverzeichnisses sind Unternehmen mit weniger als 250 Mitarbeitern u.a. befreit, wenn die Datenverarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt.
- Bei Sicherheitsvorfällen (Verletzungen des Schutzes personenbezogener Daten) entfällt die Meldepflicht gegenüber der Aufsichtsbehörde, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der Betroffenen führt; eine Pflicht zur Benachrichtigung der betroffenen Personen über einen Vorfall besteht nur dann, wenn die Verletzung voraussichtlich ein hohes Risiko für die betroffenen Personen zur Folge hat.
- Die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung besteht ebenfalls nur, wenn die Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Wenn aber Datenschutz-Folgenabschätzung bestätigt, dass die Verarbeitung ein solches hohes Risiko zur Folge hätte, besteht eine Pflicht zur vorherigen Konsultation der zuständigen Datenschutzaufsichtsbehörde.

a) Technische und organisatorische Maßnahmen, Artikel 24, 25 und 32

Technische und organisatorische Maßnahmen dienen dem Ziel, die Einhaltung der Datenschutz-Grundverordnung sicherzustellen und dies zur Erfüllung der Rechenschaftspflicht des Artikel 5 Absatz 2 Datenschutz-Grundverordnung auch nachweisen zu können (Artikel 24 Absatz 1). Insbesondere für die Gewährleistung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25) sowie der Datensicherheit (Artikel 32) spielen technische und organisatorische Maßnahmen - wie die Pseudonymisierung und Verschlüsselung sowie Maßnahmen zur Gewährleistung der Schutzziele der IT-Sicherheit - eine wichtige Rolle.

Nicht jede Datenverarbeitung erfordert gleich hohe Schutzmaßnahmen. Die Maßnahmen müssen im Einzelfall geeignet sein, ein dem jeweiligen Risiko angemessenes Schutzniveau zu gewährleisten (Artikel 32 Absatz 1). Hierbei sind der Stand der Technik, die Implementierungskosten und die Art, Umfang, Umstände und Zwecke der Verarbeitung, die Eintrittswahrscheinlichkeit und Schwere des Risikos zu berücksichtigen.

b) Auftragsverarbeitung, Artikel 28

Mit Artikel 28 schafft die Datenschutz-Grundverordnung erstmals europaweit einheitliche Anforderungen an die Auftragsverarbeitung. Eine Auftragsverarbeitung darf nur erfolgen, wenn der Auftragsverarbeiter hinreichende Garantien dafür bietet, dass die Verarbeitung im Einklang mit den Anforderungen der Datenschutz-Grundverordnung erfolgt. Zudem sind die in Absatz 3 genannten Festlegungen zwischen dem Verantwortlichen und dem Auftragsverarbeiter zu treffen. Dies betrifft insb. die Weisungsgebundenheit des Auftragverarbeiters, die Gewährleistung der Vertraulichkeit, die Einhaltung geeigneter technischer und organisatorischer Maßnahmen und die Unterstützung des Verantwortlichen bei der Erfüllung der Betroffenenrechte.

§ 11 BDSG a.F., der bisher die Anforderungen an die Auftragsdatenverarbeitung im deutschen Recht bestimmte, wurde aufgrund der unmittelbaren Geltung des Artikels 28 Datenschutz-Grundverordnung aufgehoben und findet sich im BDSG 2018 nicht mehr.

c) Verzeichnis von Verarbeitungstätigkeiten, Artikel 30

An die Stelle der bisherigen Meldepflicht tritt nach Artikel 30 die Pflicht des Verantwortlichen und des Auftragverarbeiters, ein Verzeichnis der Verarbeitungstätigkeiten mit den in Absatz 1 und Absatz 2 genannten Angaben zu führen. Eine Ausnahme gilt für Unternehmen mit weniger als 250 Mitarbeitern unter den in Artikel 30 Absatz 3 genannten Voraussetzungen. Das Verzeichnis dient als wichtiger Baustein zum Nachweis der Einhaltung der Datenschutz-Grundverordnung und ist der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Das Verarbeitungsverzeichnis ersetzt das bislang nach § 4g Absatz 2 BDSG a.F. zu führende Verfahrensverzeichnis.

d) Meldung von Sicherheitsvorfällen, Artikel 33 und 34

Sicherheitsvorfälle können bei den Betroffenen zu schwerwiegenden wirtschaftlichen und gesellschaftlichen Nachteilen wie finanziellen Schäden, Identitätsdiebstahl, Rufschädigung oder der Offenbarung von Berufsgeheimnissen führen. Unter einer solchen „Verletzung des Schutzes personenbezogener Daten“ versteht die Datenschutz-Grundverordnung jede Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung oder zum unbefugten Zugang zu personenbezogenen Daten führt (Artikel 4 Nummer 12 Datenschutz-Grundverordnung).

Sicherheitsvorfälle hat der Verantwortliche nach Artikel 33 und 34 Datenschutz-Grundverordnung zu dokumentieren und einschließlich der wahrscheinlichen Folgen des Vorfalls und der ergriffenen oder vorgeschlagenen Abhilfemaßnahmen der zuständigen Aufsichtsbehörde und den betroffenen Personen grundsätzlich unverzüglich zu melden. Falls die Benachrichtigung der Aufsichtsbehörde nicht binnen 72 Stunden erfolgen kann, müssen die Gründe für die Verzögerung angegeben werden. Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.

Die Meldepflicht besteht nicht, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Eine Benachrichtigung der betroffenen Personen muss zudem nur erfolgen, wenn der Vorfall voraussichtlich ein hohes Risiko für die betroffenen Personen zur Folge hat. Die Aufsichtsbehörde kann gegenüber dem Verantwortlichen die Benachrichtigung der betroffenen Personen anordnen.

Das System der Meldung der Verletzungen des Schutzes personenbezogener Daten löst die bislang in § 42a BDSG a.F. und einigen Fachgesetzen vorgesehene Informationspflicht bei unrechtmäßiger Kenntniserlangung personenbezogener Daten ab. Auch öffentliche Stellen unterliegen nach der Datenschutz-Grundverordnung nunmehr den Meldepflichten bei Sicherheitsvorfällen. Wie bisher darf eine Benachrichtigung über Sicherheitsvorfälle jedoch nicht in einem Strafverfahren gegen den Verantwortlichen verwendet werden (§ 42 Absatz 4 BDSG 2018).

e) Datenschutz-Folgenabschätzung und Konsultationspflicht, Artikel 35 und 36

Verarbeitungsvorgänge, die aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, müssen von dem Verantwortlichen nach Artikel 35 Datenschutz-Grundverordnung vorab einer Folgenabschätzung unterzogen werden. Bestätigt sich in der Datenschutz-Folgenabschätzung, dass die Verarbeitung ein hohes Risiko zur Folge hätte, hat der Verantwortliche nach Artikel 36 die zuständige Aufsichtsbehörde vor Beginn der Verarbeitung zu konsultieren.

Die Datenschutz-Folgenabschätzung umfasst eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und Verarbeitungszwecke sowie eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungszwecke und der Risiken für die von der Verarbeitung betroffenen Personen. Sie zeigt schließlich die zur Bewältigung der Risiken vorgesehenen Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren auf, durch die die datenschutzrechtlichen Belange sichergestellt werden. Der betriebliche oder behördliche Datenschutzbeauftragte ist hierbei einzubinden. Gegebenenfalls ist der Standpunkt der betroffenen Personen oder ihrer Interessenvertreter einzuholen.

Die Notwendigkeit einer Datenschutz-Folgenabschätzung ist insbesondere bei der Verwendung neuer Technologien zu prüfen und bei umfangreichen Verarbeitungsvorgängen, bei denen große Mengen personenbezogener Daten verarbeitet werden oder eine große Zahl von Personen betroffen sind. Die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen auf der Basis eines Profilings, die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikel 9 Absatz 1 oder Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 sowie die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche - insbesondere mittels Videoüberwachung - unterliegen unter den Voraussetzungen des Absatzes 3 zudem stets einer Folgenabschätzung. Die Aufsichtsbehörden können weitere Verarbeitungsvorgänge bestimmen, bei denen eine Datenschutz-Folgenabschätzung durchzuführen ist oder bei denen keine Pflicht zur Folgenabschätzung besteht.

Die Datenschutz-Folgenabschätzung ersetzt künftig die bislang in § 4d Absatz 5 BDSG a.F. vorgeschriebene Vorabkontrolle automatisierter Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Sie verfolgt eine ähnliche Zielrichtung wie die Vorabkontrolle, ist jedoch strukturierter aufgebaut und zudem nicht mehr Aufgabe des betrieblichen oder behördlichen Datenschutzbeauftragten.

Gleichfalls ersetzt die Datenschutz-Folgenabschätzung die durch die Datenschutz-Richtlinie 95/46/EG vorgesehene Meldepflicht jeglicher Verarbeitungen personenbezogener Daten bei der zuständigen Aufsichtsbehörde (ehemals § 4d und § 4e BDSG a.F.). Durch das Entfallen der Meldepflicht wird bürokratischer und finanzieller Aufwand für die Verantwortlichen reduziert. Die Konzentration auf Verarbeitungsvorgänge mit einem voraussichtlich hohen Risiko für die betroffenen Personen gestaltet den Schutz personenbezogener Daten zugleich effektiver als eine unterschiedslose, formale Meldepflicht bei der zuständigen Aufsichtsbehörde.

f) Bestellung betrieblicher/behördlicher Datenschutzbeauftragter, Artikel 37 bis 39

Die Bestellung betrieblicher und behördlicher Datenschutzbeauftragter ist in Deutschland seit langem vorgesehen und hat sich bewährt. Mit den Datenschutzbeauftragten stehen öffentlichen und nicht-öffentlichen Stellen interne Ansprechpartner für den Datenschutz zur Verfügung, die mit den Datenverarbeitungsvorgängen und Abläufen der Organisation vertraut sind und den Verantwortlichen, deren Mitarbeitern, betroffenen Personen und Aufsichtsbehörden als zentrale Anlaufstelle dienen.

Mit der Datenschutz-Grundverordnung wird die Institution des Datenschutzbeauftragten nun EU-weit eingeführt. Die Voraussetzungen für die Bestellung, die Rechtsstellung und die Aufgaben der Datenschutzbeauftragten nach den Artikeln 37 bis 39 Datenschutz-Grundverordnung sind weitgehend mit der bisherigen Rechtslage in Deutschland vergleichbar.

Öffentliche Stellen haben wie bisher stets eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu bestellen. Nicht-öffentliche Stellen unterliegen nach Artikel 37 Absatz 1 Datenschutz-Grundverordnung einer Bestellpflicht, wenn ihre Kerntätigkeit

- in Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfordert, oder
- in der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht.

Ergänzend bestimmt § 38 BDSG 2018, dass nicht-öffentliche Stellen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten auch dann zu bestellen haben, wenn sie

- in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen,
- Verarbeitungsvorgänge ausführen, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen oder
- personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten.

Die bestehende Rechtslage zur Bestellung betrieblicher Datenschutzbeauftragter wird hierdurch fortgeführt.

Datenschutzbeauftragte müssen über das für die Erfüllung ihrer Aufgaben erforderliche Fachwissen verfügen. Sowohl die Bestellung eigener Mitarbeiter als auch die Ernennung einer externen Person ist zulässig. Auch ist die Bestellung gemeinsamer Datenschutzbeauftragter für eine Unternehmensgruppe oder mehrere Behörden möglich.

Die Aufgaben der Datenschutzbeauftragten sind in Artikel 39 Datenschutz-Grundverordnung festgelegt: Die Datenschutzbeauftragten unterrichten und beraten die Verantwortlichen und ihre Beschäftigten in datenschutzrechtlichen Fragen, insbesondere bei der Durchführung der Datenschutz-Folgenabschätzung nach Artikel 35. Sie überwachen die Einhaltung des Datenschutzrechts und die Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter. Sie arbeiten mit den zuständigen Aufsichtsbehörden zusammen und fungieren für diese als Anlaufstelle in mit der Datenverarbeitung zusammenhängenden Fragen.

Der Verantwortliche hat die Datenschutzbeauftragte oder den Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Tätigkeiten umfassend zu unterstützen. Er hat nach Artikel 38 insbesondere sicherzustellen, dass die Datenschutzbeauftragten

- ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden,
- über die für die Erfüllung ihrer Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen verfügen und
- bei der Erfüllung ihrer Aufgaben keinen Weisungen unterliegen.

§ 6 Absatz 3 bis 6 i.V.m. § 38 BDSG 2018 sichert die Stellung des Datenschutzbeauftragten in Fortführung der bisherigen Rechtslage weiter ab. Zur Gewährleistung ihrer Unabhängigkeit dürfen Datenschutzbeauftragte wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden. Sie unterliegen wie bislang einem besonderen Kündigungs- und Abberufungsschutz, einer umfassenden Verschwiegenheitspflicht und einem Zeugnisverweigerungsrecht.

Welche Rolle spielen künftig Verhaltensregeln und Zertifizierungen?

Die Harmonisierung bietet enorme Chancen für die Wirtschaft, insbesondere für grenzüberschreitend tätige Unternehmen, da in der gesamten Europäischen Union die gleichen Regeln gelten; der hohe Abstraktionsgrad der Datenschutz-Grundverordnung stellt die Wirtschaft jedoch auch vor Rechtsunsicherheit.

Von hoher Bedeutung sind daher die Mechanismen, die die Wirtschaft befähigen, eigeninitiativ zur Konkretisierung der Datenschutz-Grundverordnung beizutragen. Die Instrumente der Verhaltensregeln, so genannte Codes of Conduct, und der Datenschutz-Zertifizierung werden durch die Datenschutz-Grundverordnung gestärkt und dienen als wichtiges Mittel zur Schaffung von Rechtssicherheit. Sie sind ein wichtiger Aspekt, um Datenschutz-Konformität nachzuweisen und hierdurch Vertrauen zu schaffen. Die Aufsichtsbehörden sind in die Ausarbeitung von Verhaltensregeln und der Zertifizierungskriterien eng einzubinden und genehmigen diese, so dass es sich um Instrumente der „regulierten“ Selbstregulierung handelt. Genehmigte Verhaltensregeln und Zertifizierungsmechanismen können Teil geeigneter Garantien für Datenübermittlung in Drittländer sein (Artikel 46 Absatz 2 Buchstabe e) und f) Datenschutz-Grundverordnung).

Über das Instrument der Verhaltensregeln (Artikel 40 Datenschutz-Grundverordnung) können Verbände und andere Vereinigungen die Anwendung der Datenschutz-Grundverordnung für spezielle Verarbeitungsbereiche oder Branchen präzisieren und hierbei insbesondere den Anforderungen kleinerer und mittlerer Unternehmen Rechnung tragen. Die Verhaltensregeln werden von der zuständigen nationalen Aufsichtsbehörde oder den Europäischen Datenschutzausschuss genehmigt und veröffentlicht. Die Europäische Kommission kann die vom Europäischen Datenschutzausschuss genehmigten Verhaltensregeln EU-weit für allgemein gültig erklären. Die Überwachung der Verhaltensregeln kann nach Artikel 41 Datenschutz-Grundverordnung einer unabhängigen Stelle übertragen werden, die von den Aufsichtsbehörden akkreditiert wird. Die Aufgaben und Befugnisse der Aufsichtsbehörden bleiben hiervon unberührt.

Mit datenschutzspezifischen Zertifizierungsverfahren (Artikel 42 Datenschutz-Grundverordnung) können Verantwortliche und Auftragsverarbeiter nachweisen, dass die Datenschutz-Grundverordnung bei den zertifizierten Verarbeitungsvorgängen eingehalten wird. Die Zertifizierung erfolgt anhand der durch die nationalen Aufsichtsbehörden oder - im Falle eines EU-weiten Europäischen Datenschutzsiegels - durch den Europäischen Datenschutzausschuss genehmigten Zertifizierungskriterien (Artikel 42 Absatz 5). Die Stellen, die die Zertifizierung vornehmen (Zertifizierungsstellen), müssen durch die Deutsche Akkreditierungsstelle (DAkkS) unter Einbindung der Aufsichtsbehörden akkreditiert werden (Artikel 43 Datenschutz-Grundverordnung i.V.m. § 39 BDSG 2018).

Für den in der Praxis sehr bedeutsamen Bereich der Auftragsverarbeitung im Rahmen von Cloud Computing steht mit dem Trusted Cloud Datenschutz Profil für Cloud-Dienste (TCDP) ein Zertifizierungsstandard auf der Basis des geltenden Bundesdatenschutzgesetzes zur Verfügung, von dem Anbieter und Nutzer von Cloud-Diensten gleichermaßen profitieren. Der Prüfstandard wurde im Rahmen des Technologieprogramms "Trusted Cloud" des Bundesministeriums für Wirtschaft und Energie entwickelt und wird durch die Stiftung Datenschutz verwaltet. Durch das vom Bundesministerium für Wirtschaft und Energie geförderte Forschungsprojekt AUDITOR wird der Standard derzeit an die Datenschutz-Grundverordnung angepasst und fortentwickelt. Ziel des Projektes ist insbesondere die Erstellung eines durch den Europäischen Datenschutzausschuss nach Artikel 42 Absatz 5 Datenschutz-Grundverordnung genehmigten Kriterienkatalogs für die Zertifizierung und die Entwicklung eines Prüf- und Zertifizierungsverfahrens.

Unter welchen Voraussetzungen dürfen Daten an Nicht-EU-Staaten übermittelt werden?

Während Datenübermittlungen in andere Mitgliedstaaten der Europäischen Union keinen Einschränkungen unterliegen und eine Behinderung des freien Datenverkehrs aus Gründen des Datenschutzes unzulässig ist (vgl. Art. 1 Absatz 3 Datenschutz-Grundverordnung), ist ein Transfer personenbezogener Daten in Staaten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (Drittländer) nur unter den Voraussetzungen des Kapitels V zulässig.

Sinn und Zweck der Regelungen für den internationalen Datentransfer ist die Gewährleistung eines umfassenden Schutzes des Grundrechts auf Datenschutz (Artikel 8 der EU-Grundrechtecharta): Der innerhalb der Europäischen Union und des Europäischen Wirtschaftsraums gewährleistete hohe Datenschutzstandard soll nicht dadurch ausgehöhlt werden, dass personenbezogene Daten ohne angemessene Schutzvorkehrungen in Drittstaaten übermittelt werden können.

Für einen Drittstaatstransfer müssen zunächst die allgemeinen Regelungen der Datenschutz-Grundverordnung eingehalten sein (Artikel 44 Datenschutz-Grundverordnung). Insbesondere muss eine Rechtsgrundlage für die Datenübermittlung in der Datenschutz-Grundverordnung oder im nationalen Datenschutzrecht bestehen.

Zusätzlich muss für eine Datenübermittlung in ein Drittland eine der nachstehenden Bedingungen erfüllt sein:

- Vorliegen eines **Angemessenheitsbeschlusses** der Europäischen Kommission nach Artikel 45 Datenschutz-Grundverordnung. Beschlüsse der Europäischen Kommission über ein angemessenes Schutzniveau liegen zum Beispiel für Argentinien, die Schweiz, Kanada, Neuseeland und Uruguay vor. Ein solcher Angemessenheitsbeschluss ist auch der EU-US-Datenschutzschild ("Privacy Shield") vom 12. Juli 2016. Danach können personenbezogene Daten aus der Europäischen Union an solche Organisationen in den USA übermittelt werden, die sich verbindlich zur Einhaltung der Datenschutzgrundsätze des Datenschutzschilds verpflichtet haben und auf der "Datenschutz-Liste" aufgeführt sind.
- Vorliegen **geeigneter Garantien** (Artikel 46 Datenschutz-Grundverordnung), insbesondere in Form von
  - verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules),
  - Standarddatenschutzklauseln oder
  - genehmigten Verhaltensregeln oder eines genehmigten Zertifizierungsmechanismus.

- Vorliegen einer **Ausnahme** nach Artikel 49 Datenschutz-Grundverordnung, insbesondere:
  - bei Vorliegen einer ausdrücklichen Einwilligung der betroffenen Person,
  - zum Schutz lebenswichtiger Interessen der betroffenen Person,
  - bei Erforderlichkeit zur Vertragserfüllung,
  - aus wichtigen Gründen eines öffentlichen Interesses,
  - zur Verfolgung von Rechtsansprüchen oder
  - zur Wahrung zwingender berechtigter Interessen des Verantwortlichen.

Wer kontrolliert die Einhaltung der Datenschutz-Grundverordnung?

Die Einhaltung der Datenschutz-Grundverordnung und der nationalen Rechtsvorschriften zum Datenschutz wird in allen Mitgliedstaaten durch unabhängige Aufsichtsbehörden überwacht und durchgesetzt.

In Deutschland sind dies die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) und die Aufsichtsbehörden der Bundesländer. Die BfDI ist zuständig für die Aufsicht über die öffentlichen Stellen des Bundes, die Gemeinsamen Einrichtungen nach dem Sozialgesetzbuch II (Jobcenter) und die Unternehmen, die Telekommunikations- oder Postdienstleistungen erbringen; im Übrigen sind die Aufsichtsbehörden der Länder zuständig.

Eine Übersicht über die Aufsichtsbehörden und deren Kontaktdaten findet sich auf der Website der BfDI.

Die Aufsichtsbehörden verfügen über die umfangreichen Untersuchungs-, Abhilfe- und Genehmigungsbefugnisse des Artikels 58 Datenschutz-Grundverordnung. Sie können gegenüber dem Verantwortlichen insbesondere Verbote oder Anordnungen aussprechen und Bußgelder verhängen. Sie beraten zudem die nationalen Parlamente und Regierungen und gehen Beschwerden betroffener Personen nach. Bei der Erfüllung ihrer Aufgaben sind die Aufsichtsbehörden völlig unabhängig; sie unterstehen insbesondere keiner Rechts- oder Fachaufsicht.

Die Aufsichtsbehörden der Mitgliedstaaten arbeiten bei der Überwachung und Durchsetzung der Datenschutz-Grundverordnung eng zusammen. Sie leisten sich gegenseitige Amtshilfe und können gemeinsame Maßnahmen durchführen. Wichtige Auslegungs- und Anwendungsfragen, insbesondere solche mit grenzüberschreitendem Bezug, werden im Europäischen Datenschutzausschuss, dem Zusammenschluss aller Aufsichtsbehörden der Mitgliedstaaten auf EU-Ebene, beraten und verbindlich entschieden. Der Europäische Datenschutzausschuss trägt mit diesem Kohärenzverfahren zu einer EU-weit einheitlichen Anwendung der Datenschutz-Grundverordnung bei.

Die Aufsichtsbehörde am Ort der Hauptniederlassung oder der einzigen Niederlassung eines Unternehmens in der Europäischen Union handelt bei den Abstimmungsprozessen mit den Aufsichtsbehörden der übrigen Mitgliedstaaten als federführende Aufsichtsbehörde. Sie ist für Fragen grenzüberschreitender Datenverarbeitung einziger Ansprechpartner des Verantwortlichen (Artikel 56 Datenschutz-Grundverordnung). Dieses "One Stop Shop-Prinzip" bewirkt für Daten verarbeitende Unternehmen eine erhebliche Vereinfachung.

Welche Konsequenzen drohen bei Rechtsverstößen?

Erlangt eine Aufsichtsbehörde durch eine Beschwerde oder eine anlasslose Kontrolle Kenntnis von einem Verstoß gegen die Datenschutz-Grundverordnung oder eine nationale Datenschutzvorschrift, kann sie den Verantwortlichen verwarnen oder Anweisungen, Anordnungen oder Verarbeitungsverbote aussprechen (Artikel 58 Absatz 2 Datenschutz-Grundverordnung). Zusätzlich oder anstelle der Abhilfebefugnisse kann sie nach Artikel 83 Datenschutz-Grundverordnung Geldbußen von bis zu 20 Millionen € oder 4 Prozent des weltweiten Jahresumsatzes verhängen. Dem Gebot der Wirksamkeit, aber auch der Verhältnismäßigkeit, ist hierbei in jedem Einzelfall Rechnung zu tragen. Gegen rechtsverbindliche Verfügungen der Aufsichtsbehörden kann der Verantwortliche einen gerichtlichen Rechtsbehelf einlegen (Artikel 78 Datenschutz-Grundverordnung).

Neben einer Beschwerde bei der zuständigen Aufsichtsbehörde können betroffene Personen zudem Klagen vor den zuständigen Gerichten erheben, wenn sie der Ansicht sind, dass ihre Rechte durch die Verarbeitung ihrer personenbezogenen Daten verletzt wurden (Artikel 79 Datenschutz-Grundverordnung). Entsteht einer Person wegen eines Verstoßes gegen die Datenschutz-Grundverordnung ein materieller oder immaterieller Schaden, hat sie zudem Anspruch auf Schadensersatz nach Artikel 82 Datenschutz-Grundverordnung.

§ 42 BDSG 2018 sieht schließlich Straftatbestände für das unbefugte Verarbeiten nicht allgemein zugänglicher Daten vor, wenn die Tat gewerbsmäßig, gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht begangen wurde.

Welche Funktion hat das BDSG? Warum ist es kein Vollrecht mehr?

Das ab dem 25. Mai 2018 geltende Bundesdatenschutzgesetz (BDSG 2018) ergänzt die Datenschutz-Grundverordnung in den Bereichen, in denen den Mitgliedstaaten Gestaltungsspielräume verbleiben. Zwar gilt eine EU-Verordnung nach Artikel 288 des Vertrags über die Arbeitsweise in der Europäischen Union (AEUV) unmittelbar in jedem Mitgliedstaat und bedarf daher keiner Umsetzung in nationales Recht. Die Datenschutz-Grundverordnung enthält jedoch zahlreiche Klauseln, die den Mitgliedstaaten Handlungsverpflichtungen oder -optionen einräumen ("hinkende Verordnung").

Dem nationalen Gesetzgeber ist es grundsätzlich verwehrt, unmittelbar geltende Regelungen einer EU-Verordnung im nationalen Recht lediglich „abzuschreiben“ (Wiederholungsverbot). Das BDSG 2018 enthält daher im Anwendungsbereich der Datenschutz-Grundverordnung keine umfassenden Regelungen des Datenschutzrechts mehr, sondern nur noch punktuelle Ergänzungen. So regelt die Datenschutz-Grundverordnung die Rechte der betroffenen Personen in Kapitel III unmittelbar und das BDSG 2018 sieht lediglich ergänzende Einschränkungen vor. Für die Anwendungspraxis bedeutet dies, dass die Datenschutz-Grundverordnung und das BDSG 2018 zusammen zu lesen sind. Ergänzend treten ggf. bereichsspezifische Normen hinzu.

Im Anwendungsbereich der Datenschutz-Grundverordnung gelten lediglich Teil 1 und 2 (§§ 1 bis 44) des BDSG 2018; die Regelungen des Teil 3 (§§ 45 bis 84) dienen hingegen der Umsetzung der Richtlinie (EU) 2016/680 und betreffen somit allein die Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung durch die zuständigen Behörden. Der abschließende Teil 4 (§ 85) enthält Regelungen für die Verarbeitung personenbezogener Daten außerhalb der Datenschutz-Grundverordnung und der Richtlinie (EU) 2016/680, etwa zu Zwecken der Landesverteidigung oder der humanitären Hilfe.

Wie ist das Verhältnis der Datenschutz-Grundverordnung zu bestehenden Datenschutzregelungen im nationalen Recht?

Das EU-Recht steht normenhierarchisch über dem nationalen Recht. Es genießt einen Anwendungsvorrang. Datenschutzrechtliche Regelungen im nationalen Recht sind aber auch nach dem 25. Mai 2018 grundsätzlich weiterhin anwendbar. Der Bundesgesetzgeber ist unter Hochdruck dabei, sein Fachrecht an das neue allgemeine Datenschutzrecht bestehend aus Datenschutz-Grundverordnung und BDSG2018 anzupassen. Im Einzelfall kann es zu Auslegungsfragen kommen, da die bestehenden Gesetze vor Abschluss der Anpassungsarbeiten keine spezifischen Bezüge auf die Datenschutz-Grundverordnung enthalten. Die nationalen Normen sind insofern EU-rechtskonform auszulegen.

Wie ist das Verhältnis zwischen gegebenenfalls divergierenden Grundrechten?

Erwägungsgrund 4 der Datenschutz-Grundverordnung stellt klar, dass das Recht auf den Schutz personenbezogener Daten kein uneingeschränktes Recht ist. Vielmehr muss es unter Wahrung des Verhältnismäßigkeitsgrundsatzes gegen andere Grundrechte abgewogen werden.

Gemäß Art. 85 der Datenschutz-Grundverordnung bringen die Mitgliedstaaten das Recht auf Schutz der personenbezogenen Daten durch Rechtsvorschriften in Einklang mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken. Unter den Begriff Rechtsvorschrift fallen auch die Artikel des Grundgesetzes, wie Artikel 5 GG, samt der einschlägigen Rechtsprechung.

Unter welchen Voraussetzungen ist das Anfertigen und Verbreiten personenbezogener Fotografien künftig zulässig?

Die Datenschutz-Grundverordnung führt zu keinen wesentlichen Veränderungen der bisherigen Rechtslage im Umgang mit Fotografien. Die Anfertigung und Veröffentlichung einer personenbezogenen Fotografie unterliegt den allgemeinen Regelungen des Datenschutzrechts. Wie bisher auch dürfen Fotos nur verarbeitet werden, wenn die betroffene Person eingewilligt hat oder eine Rechtsgrundlage dies erlaubt.

Erfolgt die Anfertigung auf der Grundlage einer Einwilligung der betroffenen Person(en), ist diese bereits nach geltendem Recht jederzeit widerrufbar. Aufgrund der jederzeitigen Widerruflichkeit und der fehlenden Praktikabilität bei Aufnahmen größerer Menschenmengen ist die datenschutzrechtliche Einwilligung bereits nach geltender Rechtslage vielfach keine praktikable Rechtsgrundlage. Neben der Einwilligung kommen als weitere Rechtsgrundlagen für die Anfertigung und Veröffentlichung zur Durchführung eines Vertrags (Artikel 6 Absatz 1 Buchstabe b) Datenschutz-Grundverordnung) oder zur Wahrnehmung berechtigter Interessen des Fotografen (Artikel 6 Absatz 1 Buchstabe f) Datenschutz-Grundverordnung) in Betracht.

Die grundrechtlich geschützte und garantierte Meinungs- und Informationsfreiheit stellen berechtigte Interessen nach Artikel 6 Absatz 1 Buchstabe f) der Datenschutz-Grundverordnung dar. Sie fließen somit unmittelbar in die Auslegung und Anwendung der Datenschutz-Grundverordnung ein. Die Datenschutz-Grundverordnung betont, dass der Schutz personenbezogener Daten kein uneingeschränktes Recht ist, sondern im Hinblick auf seine gesellschaftliche Funktion und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden muss (Erwägungsgrund 4).

Für die Veröffentlichung von Fotografien enthält das Kunsturhebergesetz (KunstUrhG) ergänzende Regelungen, die auch unter der ab dem 25. Mai 2018 anwendbaren Datenschutz-Grundverordnung fortbestehen. Das Kunsturhebergesetz stützt sich auf Artikel 85 Absatz 1 der Datenschutz-Grundverordnung, der den Mitgliedstaaten nationale Gestaltungsspielräume bei dem Ausgleich zwischen Datenschutz und der Meinungs- und Informationsfreiheit eröffnet. Es steht nicht im Widerspruch zur Datenschutz-Grundverordnung, sondern fügt sich als Teil der deutschen Anpassungsgesetzgebung in das System der Datenschutz-Grundverordnung ein.

Was ändert sich für kleine Vereine und ehrenamtliche Organisationen?

Bei den Verhandlungen zur Datenschutz-Grundverordnung hat die Bundesregierung Wert auf eine angemessene, die besonderen Belange kleinerer Institutionen berücksichtigende Ausgestaltung gelegt.

Ob und in welchem Umfang die Pflichten der Datenschutz-Grundverordnung zu erfüllen sind, bemisst sich daher vor allem nach dem Umfang, den Zwecken und der Schwere des von der Datenverarbeitung ausgehenden Risikos (sog. risikobasierter Ansatz). Lediglich Institutionen, deren Geschäftszweck (Kerntätigkeit) in der Verarbeitung personenbezogener Daten liegt oder die außergewöhnliche, hochriskante Datenverarbeitungsvorgänge vornehmen, unterliegen dem vollen Pflichtenkatalog der Datenschutz-Grundverordnung.

Geht die Datenverarbeitung hingegen nicht über eine übliche, unterstützende Tätigkeit (z.B. Lohnabrechnung, Mitglieder- und Beitragsverwaltung, Betrieb einer Vereinswebsite) hinaus, führt die Datenschutz-Grundverordnung im Vergleich zur geltenden Rechtslage zu keinen wesentlichen Neuerungen.

Die Verarbeiterpflichten des Kapitels IV der Datenschutz-Grundverordnung sind nach geltendem Datenschutzrecht bereits bekannt, etwa die Pflicht zu geeigneten technischen und organisatorischen Maßnahmen, die Bestellung betrieblicher Datenschutzbeauftragter oder die Erstellung eines Verarbeitungsverzeichnisses.

- Für die technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit gilt: Nicht jede Datenverarbeitung erfordert gleich hohe Sicherheitsstandards. Es ist ein dem Risiko angemessenes Schutzniveau unter Berücksichtigung der Implementierungskosten erforderlich. Im Rahmen der üblichen Vereins- oder ehrenamtlichen Tätigkeit genügen daher im Regelfall bereits Standardmaßnahmen, wie die Lagerung personenbezogener Daten in abschließbaren Vorrichtungen, aktuelle Betriebssysteme mit Passwortschutz, Zugriffsrechten und aktuellem Virenschutz den Anforderungen.
- Ein betrieblicher Datenschutzbeauftragter ist - wie bislang auch schon - bei Vereinen und ehrenamtlichen Institutionen in der Regel nur dann zu bestellen, wenn „mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten“ beschäftigt sind (§ 38 Absatz 1 Satz 1 BDSG 2018). Eine Datenschutz-Folgeabschätzung bei hochriskanten Datenverarbeitungen, die unabhängig von diesem Schwellenwert zur Bestellung betrieblicher Datenschutzbeauftragter führt, ist nur in deutlich von den üblichen Verarbeitungstätigkeiten in Vereinen und ehrenamtlichen Institutionen abweichenden Einzelfällen angezeigt. Die Pflicht gilt daher nicht schon ab zehn Beschäftigten oder Mitgliedern, sondern regelmäßig erst bei mehr als neun in der Verwaltung (d. h. insbesondere in der Mitglieder- und Beitragsverwaltung sowie der Lohnabrechnung) tätigen Mitarbeitern. Nur diese sind „ständig“ - und nicht nur regelmäßig oder bei Gelegenheit - mit der automatisierten Verarbeitung personenbezogener Daten betraut.
  Betriebliche Datenschutzbeauftragte können Beschäftigte oder externe Dienstleister sein. Die Datenschutzbeauftragten müssen über die zur Erfüllung ihrer Beratungs- und Überwachungsfunktionen erforderlichen zeitlichen Ressourcen verfügen, was jedoch keinesfalls eine vollständige Freistellung erfordert.
  Die Bestellung betrieblicher Datenschutzbeauftragter auf freiwilliger Grundlage bleibt zulässig. Denn auch hier gilt: Die Befreiung von der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragen befreit im Übrigen nicht von der Einhaltung des Datenschutzrechts!

- Das schon bislang zu führende Verfahrensverzeichnis wird durch das Verzeichnis der Verarbeitungstätigkeiten ersetzt. Das Verfahrensverzeichnis umschreibt stichpunktartig die wesentlichen Angaben jeder Verarbeitungstätigkeit, wie z. B. die Zwecke der Verarbeitung und eine Beschreibung der Kategorien der personenbezogenen Daten, der betroffenen Personen und der Empfänger.

Die Rechte der betroffenen Personen auf Information und Auskunft werden durch die Datenschutz-Grundverordnung zwar ausgeweitet, sind mit Ausnahme des Rechts auf Datenübertragbarkeit (Artikel 20 Datenschutz-Grundverordnung) aber ebenfalls nicht neu. Das zum 25. Mai 2018 in Kraft getretene, novellierte Bundesdatenschutzgesetz 2018 enthält ergänzende Ausnahmen von den Betroffenenrechten, die an die bisherige Rechtslage in Deutschland nach dem alten Bundesdatenschutzgesetz anknüpfen.

Die Aufsichtsbehörden haben mittlerweile eine Vielzahl abgestimmter Kurzpapiere zur Umsetzung der Datenschutz-Grundverordnung veröffentlicht, die auch den Bedürfnissen kleinerer und mittlerer Institutionen Rechnung tragen. Zu verweisen ist insbesondere auf die Handreichung des Bayerischen Landesamtes für Datenschutzaufsicht für kleine Unternehmen und Vereine, welche die Anforderungen der Datenschutz-Grundverordnung für typische Vereinstätigkeiten in der praktischen Umsetzung (für den Freistaat Bayern) erläutert.

Drohen demnächst existenzgefährdende Geldbußen?

Um dem Grundrecht auf Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten besondere Wirksamkeit zu verleihen, drohen bei Verstößen gegen die wichtigsten Regelungen der Datenschutz-Grundverordnung Geldbußen von bis zu 20 Mio. € oder bis zu 4 Prozent des gesamten weltweit erzieltes Jahresumsatzes des vorangegangenen Geschäftsjahrs (Artikel 83 Datenschutz-Grundverordnung).

Die Verhängung von Geldbußen bei Datenschutzverstößen steht im pflichtgemäßen Ermessen der Aufsichtsbehörden. Zusätzlich zu oder anstelle von einer Geldbuße kommen die übrigen Abhilfebefugnisse der Aufsichtsbehörden nach Artikel 58 Absatz 2 Datenschutz-Grundverordnung in Betracht. Die Höhe der Geldbuße muss zudem verhältnismäßig sein. Sinn und Zweck der von der Datenschutz-Grundverordnung festgelegten Obergrenze ist die Abschöpfung des durch den Rechtsverstoß erlangten Gewinns, nicht jedoch die Insolvenz eines Unternehmens. Es soll verhindert werden, dass Unternehmen, die mit der Verarbeitung personenbezogener Daten hohe Gewinne erzielen, Datenschutzverstöße „aus der Portokasse“ bezahlen. Eine Mindesthöhe schreibt die Datenschutz-Grundverordnung indes nicht vor.

Bei der Entscheidung über die Verhängung einer Geldbuße und deren Betrag sind die in Artikel 83 Absatz 2 genannten Aspekte, u. a. die Art, Schwere und Dauer des Verstoßes, die Vorsätzlichkeit oder Fahrlässigkeit, die getroffenen Maßnahmen zur Schadensminderung und -prävention, der Umfang der Zusammenarbeit mit den Aufsichtsbehörden sowie alle erschwerenden und mildernden Umstände des jeweiligen Einzelfalles gebührend zu berücksichtigen. Insbesondere bei geringfügigen Verstößen oder unverhältnismäßigen Belastungen sieht die Datenschutz-Grundverordnung anstelle einer Geldbuße die Möglichkeit einer Verwarnung vor (Erwägungsgrund 148).

Gegen den Bußgeldbescheid einer Aufsichtsbehörde stehen das Verfahren und die Rechtsbehelfe des Gesetzes über Ordnungswidrigkeiten (OWiG) zur Verfügung.

Wo finde ich weiterführende Informationen?

Auf europäischer Ebene hat die Artikel 29-Gruppe, der Zusammenschluss der Aufsichtsbehörden aller Mitgliedstaaten in der Europäischen Union, zu zentralen Fragen der Datenschutz-Grundverordnung gemeinsame Leitlinien veröffentlicht . Die Artikel 29-Gruppe wird unter Geltung der Datenschutz-Grundverordnung durch den Europäischen Datenschutzausschuss abgelöst.

Auf nationaler Ebene hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu vielen wichtigen Themenbereichen der Datenschutz-Grundverordnung gemeinsame Kurzpapiere veröffentlicht, die Auslegungshilfen bei der praktischen Anwendung der Datenschutz-Grundverordnung geben.

Einige Aufsichtsbehörden haben darüber hinaus weitergehende Auslegungshilfen und Formulare veröffentlicht, wie etwa das Musterformular für ein Verzeichnis zu den Verarbeitungstätigkeiten nach Artikel 30 Datenschutz-Grundverordnung.

Weitere Praxishilfen werden von zahlreichen Datenschutz- und Wirtschaftsverbänden veröffentlicht.

Einen Überblick über aktuelle Themen und wichtige Entwicklungen im Datenschutz gibt schließlich die Stiftung Datenschutz.
