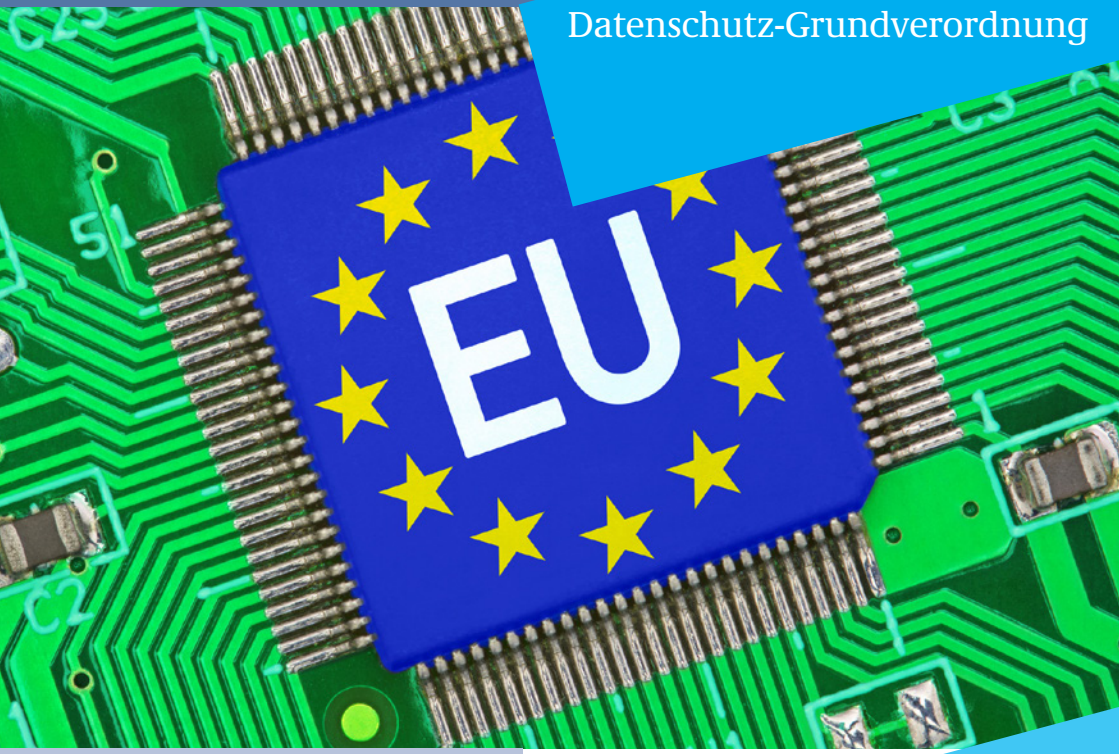
Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Datenschutz-Grundverordnung



Info 6

Jetzt mit dem neuen BDSG

Impressum

Herausgeber:
Die Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

Postfach 14 68, 53004 Bonn
Hausanschrift: Husarenstraße 30, 53117 Bonn
Tel. +49 (0) 228 997799-0
Fax +49 (0) 228 997799-550
E-Mail: referat11@bfdi.bund.de
Internet: http://www.datenschutz.bund.de

Auflage: 5. Auflage, September 2017

Diese Broschüre ist Teil der Öffentlichkeitsarbeit der BfDI.
Sie wird kostenlos abgegeben und ist nicht für den Verkauf bestimmt.

Realisation: Appel & Klinger Druck und Medien GmbH
Bildnachweis: fotolia

Datenschutz-Grundverordnung

BfDI – Info 6

1 Inhaltsverzeichnis

Vorwort

Nach etwa vierjährigen Verhandlungen haben der Europäische Rat und das Europäische Parlament im Frühjahr 2016 die EU-Datenschutz-Grundverordnung verabschiedet.

Die Datenschutz-Grundverordnung ist ein Meilenstein des Datenschutzes in Europa, denn sie verknüpft bewährte Prinzipien des grundrechtsorientierten Datenschutzrechts mit einer stärkeren Harmonisierung und einer maßvollen Modernisierung. Grundlage des Datenschutzrechts ist und bleibt das informationelle Selbstbestimmungsrecht des Einzelnen. Positiv ist die Beibehaltung des während der Verhandlungen immer wieder in Frage gestellten Verbotsprinzips, nach dem jede Datenverarbeitung, die nicht durch eine Einwilligung legitimiert ist, einer gesetzlichen Erlaubnis bedarf. Damit verbleibt auch künftig die Darlegungslast für die Notwendigkeit eines Eingriffs in das Recht auf informationelle Selbstbestimmung bei demjenigen, der diesen Eingriff vornehmen will.

Schließlich ist es erfreulich, dass die Prinzipien der Datensparsamkeit, der Angemessenheit und Erforderlichkeit, der Transparenz und Zweckbindung, der Gewährleistung der Datensicherheit sowie der unabhängigen Aufsicht und wirksamen Sanktionierung beibehalten oder gestärkt werden.

Vordringlichstes Ziel war, das Datenschutzrecht innerhalb Europas stärker zu vereinheitlichen. Trotz aller Harmonisierungsbemühungen in den vergangenen Jahren führten die nationalen Umsetzungen der Datenschutzrichtlinie aus dem Jahr 1995 und deren Durchsetzung nur bedingt zu einem einheitlichen Datenschutzniveau in der Europäischen Union. Vielmehr entstand ein Flickenteppich von datenschutzrechtlichen Regelungen und eine heterogene Aufsichtspraxis der Datenschutzbehörden.

Mit der Datenschutz-Grundverordnung gelten zukünftig in allen Staaten der Europäischen Union grundsätzlich die gleichen Standards.

Ein weiteres Ziel der europäischen Datenschutzreform war es, das Datenschutzrecht zu modernisieren, insbesondere bessere Antworten auf die Globalisierung und datenschutzrechtlichen Herausforderungen, die die zunehmende Digitalisierung und das Internetzeitalter mit sich bringen, zu geben.

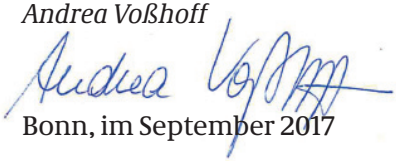
Auch dies ist weitgehend erreicht worden. Insbesondere im Bereich der Wirtschaft führen die Regelungen der Datenschutz-Grundverordnung zu einem höheren Grad an Harmonisierung als dies derzeit der Fall ist. Sie sorgen für gleiche Wettbewerbsbedingungen für alle Unternehmen, die Waren und Dienstleistungen auf dem europäischen Markt anbieten. Insbesondere werden auch ausländische Unternehmen nur dann Zugang zum europäischen Binnenmarkt erhalten, wenn sie sich an die hier geltenden Datenschutz-Regelungen halten.

Die Datenschutz-Grundverordnung bietet zudem einen wirksamen Regelungsmechanismus, um auch im Zeitalter der Digitalisierung und von Big-Data das Grundrecht jedes Einzelnen auf informationelle Selbstbestimmung im Verhältnis zu den staatlichen und kommerziellen Interessen zu sichern. Dabei lässt sie der deutschen und europäischen Digitalwirtschaft ausreichend Spielraum, innovative und intelligente Geschäftsmodelle zu entwickeln, die das in den vorhandenen enormen Datenmengen liegende Potential ökonomisch verwertbar machen und dabei zugleich die datenschutzrechtlichen Vorgaben beachten. Guter Datenschutz ist ein Qualitätsmerkmal der europäischen Wirtschaft.

Am 25. Mai 2018 wird die neue Verordnung Geltung erlangen und dann die EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) ersetzen. Bis dahin sind die nationalen Gesetzgeber aufgerufen, die Regelungsspielräume der Datenschutz-Grundverordnung mit Leben zu erfüllen. Der Bundesgesetzgeber hat hierfür einen ersten wichtigen Schritt getan und ein neues Bundesdatenschutzgesetz verabschiedet, dessen Regelungen ganz überwiegend am 25. Mai 2018 in Kraft treten werden.

Diese Broschüre will dazu beitragen, einen ersten Überblick über die neue EU-Datenschutz-Grundverordnung, insbesondere über deren Grundprinzipien und die wesentlichen Neuerungen zu vermitteln. Sie enthält neben dem Verordnungstext eine kurze Einführung in die nicht einfache Materie und das neue Bundesdatenschutzgesetz.

Andrea Voßhoff



Bonn, im September 2017

Datenschutz-Grundverordnung

1 Datenschutz-Grundverordnung – Regelungscharakter

Die EU-Datenschutz-Grundverordnung (DSGVO) löst die Datenschutzrichtlinie 95/46/EG von 1995 (im Folgenden: Datenschutzrichtlinie) ab. Im Unterschied zur Datenschutzrichtlinie gilt die DSGVO unmittelbar in der gesamten Europäischen Union (Art. 288 Abs. 2 AEUV).

2 Grundprinzipien des Datenschutzrechts – bisher bekannte Grundsätze bleiben erhalten

Die Datenschutz-Grundverordnung schreibt im Wesentlichen die bisherigen datenschutzrechtlichen Grundprinzipien fort und entwickelt sie weiter.

Die Grundsätze des „Verbots mit Erlaubnisvorbehalt“, der „Datenvermeidung und Datensparsamkeit“, der „Zweckbindung“ und der „Transparenz“ prägen auch die Datenschutz-Grundverordnung. Auch zur Datenübermittlung ins Ausland finden sich aufgrund der besonderen Bedeutung für die Rechte des Einzelnen an seinen personenbezogenen Daten detaillierte Regelungen.

2.1 Rechtmäßigkeit der Datenverarbeitung

Für die Verarbeitung personenbezogener Daten normiert Art. 6 DSGVO als allgemeinen Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt.

Die Verarbeitung von Daten ist demnach nur zulässig, wenn eine Einwilligung oder eine andere in dieser Vorschrift normierte Ausnahme vorliegt. Dies ist der Fall, wenn

- die Verarbeitung für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Antrag der betroffenen Person erfolgen;
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt;
- die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- wenn sie im öffentlichen Interesse oder zur Erfüllung hoheitlicher Aufgaben erforderlich ist oder
- sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Dieser Rechtfertigungsgrund gilt nicht für Behörden.

2.2 Datensparsamkeit

Das bereits im Bundesdatenschutzgesetz (BDSG) verankerte Prinzip der Datensparsamkeit findet sich nunmehr als eines der zentralen Prinzipien des Datenschutzes in der Datenschutz-Grundverordnung wieder.

Nach Art. 5 Abs. 1 lit. c DSGVO muss die Verarbeitung personenbezogener Daten dem Zweck angemessen und sachlich relevant sowie auf das für den Zweck der Datenverarbeitung notwendige Maß beschränkt sein.

2.3 Zweckbindung

Die Datenschutz-Grundverordnung sieht in Art. 5 Abs. 1 lit. b DSGVO eine enge Zweck-

bindung vor. Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden.

Zudem sind grundsätzlich nur solche Änderungen des Verarbeitungszwecks erlaubt, die mit dem ursprünglichen Erhebungszweck vereinbar sind (Art. 5 Abs. 1 lit. b sowie Art. 6 Abs. 4 DSGVO). Dabei stellt die Datenschutz-Grundverordnung in Art. 6 Abs. 4 Kriterien auf, die bei der Beurteilung der Vereinbarkeit einer Zweckänderung zu berücksichtigen sind. Hierzu zählen u. a. die Verbindung zwischen den Zwecken, der Gesamtkontext, in dem die Daten erhoben wurden, die Art der personenbezogenen Daten, mögliche Konsequenzen der zweckändernden Verarbeitung für den Betroffenen oder das Vorhandensein von angemessenen Sicherheitsmaßnahmen wie eine Pseudonymisierung oder Verschlüsselung. Letzteres führt zu einer vorsichtigen Privilegierung der Weiterverarbeitung pseudonymisierter bzw. verschlüsselter Daten, was für datenschutzgerechte Big-Data-Anwendungen von Bedeutung ist.

2.4 Datensicherheit

Als zentrales Prinzip des Datenschutzes wurde auch die Gewährleistung von Datensicherheit gesetzlich verankert (Art. 5 Abs. 1 lit. f und Art. 32 DSGVO).

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, der Umstände und Zweck der Datenverarbeitung, aber auch der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten haben der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen umzusetzen. Dabei muss das Sicherheitslevel im Verhältnis zum Risiko angemessen sein.

Geboten sein kann danach unter anderem eine Pseudonymisierung oder Verschlüsselung, sowie die Fähigkeit, Vertraulichkeit, Integrität und Verfügbarkeit und Belastbarkeit der Systeme zu gewährleisten (vgl. Nr. 4).

2.5 Übermittlung in Drittstaaten

Die Regelungen zur Drittstaatenübermittlung (Art. 44-50 DSGVO) übernehmen mit einigen neuen Akzenten die grundsätzliche Systematik der Regelungen in der Datenschutzrichtlinie.

Eine Übermittlung von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die im Kapitel V zur Datenübermittlung in Drittländer und zu internationalen Organisationen niedergelegten Bedingungen erfüllen und auch die sonstigen Bestimmungen der Datenschutz-Grundverordnung beachtet werden (Art. 44 DSGVO).

Eine Übermittlung ist danach zulässig, wenn die Europäische Kommission entschieden hat, dass ein angemessenes Schutzniveau besteht (Art. 45 DSGVO). Hat die Kommission keine solche Entscheidung getroffen, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten in ein Drittland oder an eine internationale Organisation nur übermitteln, sofern er geeignete Garantien vorgesehen hat und durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen (Art. 46 DSGVO), u. a. rechtlich bindende und durchsetzbare Instrumente zwischen Behörden oder öffentlichen Stellen (Art. 46 Abs. 2 lit. a DSGVO), unternehmensinterne Datenschutzvorschriften, sog. „Binding Corporate Rules“ (Art. 46 Abs. 2 lit. b i.V.m. Art. 47 DSGVO) oder Standarddatenschutzklauseln, die von der Kommission oder der Aufsichtsbehörde in einem bestimmten Verfahren angenommen werden, (Art. 46 Abs. 2 lit. c und d DSGVO).

Die Datenschutz-Grundverordnung erlaubt darüber hinaus ausnahmsweise eine Datenübermittlung in bestimmten Sonderfällen (Art. 49 DSGVO), z. B. bei Vorliegen einer ausdrücklichen Einwilligung, bei der die betroffene Person zuvor über die Risiken einer Datenübermittlung informiert worden sein muss (Art. 49 Abs. 1 lit. a DSGVO). Gerichtsurteile und behördliche Anordnungen von Drittstaaten werden unbeschadet anderer Regelungen in Kapitel V gemäß Art. 48 DSGVO nur anerkannt und durchgesetzt, wenn sie auf einer internationalen Übereinkunft – zum Beispiel einem Rechtshilfeabkommen – beruhen.

2.6 Betroffenenrechte

Kapitel III der Datenschutz-Grundverordnung regelt die Rechte der betroffenen Person. Auch sie wurden modernisiert.

Dabei normiert zunächst Art. 12 DSGVO Anforderungen an die **Transparenz** der Informationen, an die Kommunikation und die Modalitäten für die Ausübung der Rechte der betroffenen Person.

Art. 13f. DSGVO sehen einen umfangreichen Katalog proaktiver **Benachrichtigungen** vor, wobei danach differenziert wird, ob die Daten bei der betroffenen Person erhoben werden (Art. 13 DSGVO) oder nicht (Art. 14 DSGVO). Dies betrifft unter anderem Kontaktdaten des Verantwortlichen, die Verarbeitungszwecke sowie die Rechtsgrundlage, gegebenenfalls die Empfänger oder Kategorien von Empfängern sowie die Absicht der Übermittlung in ein Drittland, aber auch die Dauer der Speicherung, beziehungsweise die Kriterien für die Festlegung dieser Dauer. Der Betroffene ist zudem über seine Rechte zu informieren.

Art. 15 DSGVO regelt das **Auskunftsrecht** der Betroffenen. Die betroffene Person hat das Recht, eine Bestätigung zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist das der Fall, hat sie ein Recht auf Auskunft über diese Daten sowie über Informationen unter anderem über die Verarbeitungszwecke, deren Herkunft, Empfänger, über die Dauer der Speicherung sowie über ihre Rechte.

Die betroffene Person hat zudem das Recht, die **Berichtigung** sowie im Hinblick auf den Zweck die Vervollständigung sie betreffender unzutreffender personenbezogener Daten zu verlangen (Art. 16 DSGVO).

Daneben haben die Betroffenen nach Art. 17 DSGVO (mit bestimmten Ausnahmen) das Recht, die **Löschung** ihrer Daten zu verlangen – zum Beispiel wenn diese zu dem Zweck, zu dem sie ursprünglich erhoben oder verarbeitet wurden, nicht mehr erforderlich sind oder die dazu erteilte Einwilligung widerrufen wurde. Eine Ausnahme besteht zum Beispiel, soweit die Verarbeitung zur Ausübung der freien Meinungsäußerung erforderlich

ist. Als besondere Ausformung des Löschungsanspruches besteht nun auch ein **„Recht auf Vergessenwerden“** (Art. 17 Abs. 2 DSGVO), wenn die verantwortliche Stelle die zu löschenden Daten öffentlich gemacht hat. Dann muss sie vertretbare Schritte unternehmen, um die Stellen, die diese Daten verarbeiten, zu informieren, dass die betroffene Person von ihnen die Löschung aller Links zu diesen Daten oder von Kopien oder Replikationen verlangt. Diese Vorschrift ist von besonderer Bedeutung für den Betrieb von Internet-Suchmaschinen.

Die betroffene Person kann in bestimmten Fällen auch die **Einschränkung der Verarbeitung** verlangen (Art. 18 DSGVO) – zum Beispiel, wenn der Verantwortliche die Daten nicht mehr länger, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt oder die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen. Die Einschränkung der Verarbeitung entspricht damit begrifflich im Wesentlichen der Sperrung im Sinne von §§ 20 Abs. 3, 35 Abs. 3 BDSG.

Der Verantwortliche muss grundsätzlich allen Empfängern der Daten jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitteilen (Art. 19 DSGVO). Anders als das Recht auf Vergessenwerden knüpft diese Verpflichtung an vorangegangenen Übermittlungen an konkrete Empfänger an.

Neu ist auch das **Recht auf Datenübertragbarkeit** (Art. 20 DSGVO). Mit seiner Einführung wird die Datensouveränität der betroffenen Person gestärkt. Das Recht auf Datenübertragung gibt betroffenen Personen daher unter bestimmten Voraussetzungen einen Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten. Der Nutzer hat damit das Recht, Daten von einem Anbieter zu einem anderen „mitzunehmen“. Die Regelung kann damit insbesondere bei Social Networks den Wechsel zu einem anderen Anbieter erleichtern. Es gilt aber letztlich bei jeder automatisierten Verarbeitung personenbezogener Daten auf der Basis einer Einwilligung oder einer Vertragsbeziehung mit dem Betroffenen, also auch für Verträge mit Energieversorgern, Banken oder Versicherungen. Die betroffene Person kann sich dabei aussuchen, ob sie die Daten selbst erhalten (und an einen neuen Verarbeiter weitergeben) will oder der bisherige Verarbeiter die

Daten unmittelbar an den neuen Verarbeiter weitergeben muss. Das Recht auf Datenübertragbarkeit ist auf die Daten beschränkt, die die betroffene Person dem Verarbeiter zur Verfügung gestellt hat. Es gilt nicht für den öffentlichen Bereich.

Nach Art. 21 Abs. 1 DSGVO hat der Betroffene grundsätzlich ein allgemeines **Widerspruchsrecht** gegen eine an sich rechtmäßige Verarbeitung von personenbezogenen Daten, die im öffentlichen Interesse liegt, in Ausübung öffentlicher Gewalt oder aufgrund des berechtigten Interesses des Verantwortlichen oder eines Dritten erfolgte (Art. 6 Abs. 1 lit. e oder f DSGVO). Der Verantwortliche darf dann die Daten nur noch verarbeiten, wenn er zwingende berechtigte Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten des Betroffenen überwiegen. Ein voraussetzungsloses und uneingeschränktes Widerspruchsrecht besteht bei der Datenverarbeitung zum Zweck des Direktmarketings. Das gilt auch für das Profiling, soweit es mit der Direktwerbung zusammenhängt (Art. 21 Abs. 2 und 3 DSGVO). Der Betroffene ist ausdrücklich, in verständlicher Form und getrennt von jeglicher anderen Information auf das Widerspruchsrecht hinzuweisen (Art. 21 Abs. 4 DSGVO).

Sämtliche Betroffenenrechte können gemäß Art. 23 DSGVO durch nationale Gesetze beschränkt werden, sofern dies zur Wahrung bestimmter öffentlicher Interessen erforderlich ist. Dabei sind der Verhältnismäßigkeitsgrundsatz und der Wesensgehalt der Grundrechte zu beachten. Einschränkungen sind beispielsweise aus Gründen des Schutzes der nationalen und der öffentlichen Sicherheit, der Landesverteidigung, aber auch der Interessen der Steuerverwaltung oder zum Schutz der Unabhängigkeit der Gerichte möglich. Der Bundesgesetzgeber hat hiervon Gebrauch gemacht und in den §§ 32 bis 37 des neuen Bundesdatenschutzgesetzes (BDSG-neu) Einschränkungen der Betroffenenrechte vorgesehen. Diese sind im Lichte der DSGVO grundsätzlich eng auszulegen und am Maßstab des Art. 23 DSGVO zu messen. Ob und in welchem Umfang diese Regelungen aufgrund des Anwendungsvorrangs der DSGVO angewendet werden können, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

2.7 Unabhängige Aufsicht

Die Datenschutz-Grundverordnung bekennt sich zu einer Stärkung der Aufsicht durch unabhängige Datenschutzbehörden.

Sie normiert in Art. 51 Abs. 1, dass jeder Mitgliedstaat eine oder mehrere unabhängige Aufsichtsbehörden einzurichten hat.
Die Aufsichtsbehörden müssen sowohl vollständig unabhängig in der Wahrnehmung ihrer Aufgaben sein, als auch die Angehörigen der Aufsichtsbehörden in ihrer Aufgabenwahrnehmung frei von externem Einfluss bleiben. Dies umfasst auch ein Verbot, zugleich eine Tätigkeit wahrzunehmen, die einen Interessenkonflikt begründet (Art. 52 Abs. 1 ff. DSGVO).

Die Unabhängigkeit spiegelt sich auch darin wider, dass die Aufsichtsbehörden mit ausreichenden technischen, personellen und finanziellen Ressourcen auszustatten sind (Art. 52 Abs. 4 DSGVO).

Die Personalhoheit ist ebenfalls ausdrücklich normiert (Art. 52 Abs. 5 DSGVO). Die Auswahl der Mitglieder der Aufsichtsbehörden – d. h. in Deutschland der Bundesbeauftragten und der Landesbeauftragten bzw. der Leiter der Aufsichtsbehörden – muss in einem besonders geregelten transparenten Verfahren erfolgen (Art. 53 f. DSGVO).

Schließlich gehört zur Unabhängigkeit, dass die Mitglieder bzw. Leiter der Aufsichtsbehörden nicht ohne weiteres ihres Amtes enthoben werden können (Art. 53 Abs. 4 DSGVO). Denn auch die Sorge vor einer Amtsenthebung bei unliebsamer Amtswahrnehmung wäre geeignet, die Unabhängigkeit zu beeinträchtigen.

2.8 Effektive Durchsetzung

Effektiver Datenschutz erfordert auch die Möglichkeit einer effektiven Durchsetzung.
Die Datenschutz-Grundverordnung sieht im Vergleich zur Datenschutzrichtlinie um-

fangreichere Befugnisse für die Datenschutzaufsichtsbehörden vor. Zudem werden die Sanktionsmöglichkeiten ausgedehnt.

2.8.1 Befugnisse der Aufsichtsbehörden

Die Datenschutzbehörden werden in Zukunft auch im öffentlichen Bereich Befugnisse erhalten, die sie jedenfalls in Deutschland bislang nicht haben. So werden sie nach Art. 58 DSGVO unter anderem auch gegenüber Behörden Anordnungen erlassen können, um zum Beispiel eine rechtswidrige Datenverarbeitung zu unterbinden, die Löschung personenbezogener Daten zu erwirken oder eine Datenübermittlung in Drittstaaten zu untersagen. Diese Befugnisse sind für das deutsche Verwaltungsrecht insofern ungewöhnlich, als sie hoheitliche Maßnahmen einer Behörde gegenüber einer anderen Behörde des gleichen Verwaltungsträgers ermöglichen. Auf diese Weise werden die Datenschutzbehörden zu spezifischen Rechtsaufsichtsbehörden. Zur effektiven Durchsetzung des Datenschutzrechts sind diese Befugnisse aber unabdingbar. Sie bedingen allerdings auf nationaler Ebene die Schaffung eines gerichtlichen Rechtsschutzes auch für Behörden gegen die Maßnahmen der Datenschutzaufsichtsbehörde.

Im nicht-öffentlichen Bereich sind die Befugnisse hingegen vergleichbar mit der geltenden Rechtslage.

2.8.2 Sanktionen

Nach der Datenschutz-Grundverordnung werden die erweiterten Befugnisse durch eine Ausweitung des Bußgeldrahmens flankiert (Art. 83 DSGVO).

So sind für bestimmte Rechtsverstöße Bußgelder bis zu 4 % des Jahresumsatzes eines Unternehmens, beziehungsweise 20 Mio. Euro, zulässig, wobei der jeweils höhere Wert gilt. Dabei ist auf den gesamten weltweiten Jahresumsatz des betreffenden Unternehmens abzustellen und nicht etwa nur auf den in Europa erwirtschafteten.

Hinsichtlich der Sanktionsmöglichkeiten wird durch die Datenschutz-Grundverordnung auch eine Rechtslücke im Bereich des Telekommunikations- und Postwesens geschlossen werden, in dem die BfDI bisher keine Bußgelder verhängen kann.

Bezogen auf die öffentlichen Stellen enthält die Datenschutz-Grundverordnung in Art. 83 Abs. 7 eine Öffnungsklausel für den nationalen Gesetzgeber, wonach festgelegt werden kann, ob und in welcher Höhe auch in diesem Bereich Bußgelder verhängt werden können. § 43 Abs. 3 BDSG-neu macht davon Gebrauch und legt fest, dass gegen Behörden und sonstige öffentliche Stellen des Bundes auch in Zukunft keine Geldbußen verhängt werden können.

3 Was ist neu?

Auch wenn die Datenschutz-Grundverordnung den Datenschutz nicht neu erfindet und sich auf die seit Jahrzenten bewährten Grundprinzipien des Datenschutzes stützt, so enthält sie auch einige neue Elemente. Zum einen ist in diesem Zusammenhang das sog. Marktortprinzip zu nennen, nach dessen Maßgabe das EU-Datenschutzrecht auch für Wirtschaftsunternehmen außerhalb der Europäischen Union gilt. Zum anderen sollen komplexe Kooperations- und Kohärenzmechanismen eine möglichst einheitliche Anwendung der Regelungen des DSGVO in den EU-Mitgliedstaaten gewährleisten.

3.1 Marktortprinzip

Das Europäische Datenschutzrecht gilt nach der Datenschutz-Grundverordnung nicht nur für die in der Europäischen Union niedergelassenen Unternehmen. Voraussetzung ist nach Art. 3 Abs. 2 DSGVO lediglich, dass sich ein Angebot an einen bestimmten nationalen Markt in der EU richtet oder dass die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient. Der Anwendungsbereich erstreckt sich damit auch auf außereuropäische Unternehmen, die auf dem europäischen Markt tätig sind.

Das Marktortprinzip wird für gleiche Wettbewerbsbedingungen für alle Unternehmen sorgen, die Waren und Dienstleistungen auf dem europäischen Markt anbieten. Insbesondere werden auch ausländische Unternehmen nur dann Zugang zum europäischen Binnenmarkt erhalten, wenn sie sich an die hier geltenden Regelungen halten.

3.2 Verfahrensvereinfachung und einheitliche Rechtsanwendung

Die Datenschutz-Grundverordnung strebt eine möglichst einheitliche Rechtsanwendung in der Europäischen Union an. Dies soll im Falle grenzüberschreitender Datenverarbeitungen im nicht-öffentlichen Bereich durch einen komplexen Kooperations- und Kohärenzmechanismus umgesetzt werden, an dessen Ende eine einheitliche Entscheidung der Aufsichtsbehörden der EU-Mitgliedstaaten zur Rechtsanwendung steht. Sie kann entweder im Wege der Einigung oder zwangsweise durch einen Europäischen Datenschutzausschuss herbeigeführt werden (siehe „Kohärenzverfahren"). Die deutschen Aufsichtsbehörden werden ebenso wie diejenigen der anderen EU-Mitgliedstaaten in diesen Mechanismen nur eine Stimme haben. Die deshalb in Europäischen Angelegenheiten notwendige Abstimmung der deutschen Aufsichtsbehörden hat der Bundesgesetzgeber in § 18 BDSG-neu geregelt.

3.2.1 One-Stop-Shop

Aufgrund des durch die Datenschutz-Grundverordnung eingeführten sogenannten „One-Stop-Shop-Mechanismus" ist es für Unternehmen, die Niederlassungen in mehreren EU-Mitgliedstaaten führen und dort Datenverarbeitung betreiben, einfacher als bisher, ihre datenschutzrechtlichen Angelegenheiten zu klären: Für diese Unternehmen wird bei grenzüberschreitenden Datenverarbeitungen nur die Aufsichtsbehörde an ihrem Hauptsitz zuständig sein, sodass sie einen zentralen Ansprechpartner haben. Dies entlastet die Unternehmen gegenüber den bisherigen Regelungen ganz erheblich.

Gleichzeitig bleibt dabei aber auch gewährleistet, dass sich der von der Datenverarbeitung Betroffene mit Beschwerden immer an die Datenschutzaufsichtsbehörde an seinem Wohnsitz wenden kann.

Die grundsätzliche Architektur des One-Stop-Mechanismus ist durch die Definition einer federführenden Datenschutzbehörde am Sitz der Hauptniederlassung des Verantwortlichen gekennzeichnet, die als Hauptansprechpartner für die verantwortliche Stelle fungiert und ihr gegenüber das Datenschutzrecht durchsetzt. Sobald mehrere

Mitgliedstaaten betroffen sind, werden deren Datenschutzaufsichtsbehörden in den Abstimmungsmechanismus eingebunden (betroffene Behörden).

Einigen sich die federführende und die betroffenen Aufsichtsbehörden auf eine einheitliche Vorgehensweise, ergeht ein entsprechender Beschluss an die Hauptniederlassung des Verantwortlichen. Er hat die erforderlichen Maßnahmen zu treffen, um die Verarbeitungstätigkeiten aller Niederlassungen innerhalb der Union mit dem Beschluss in Einklang zu bringen. Die federführende Aufsichtsbehörde ist über die Maßnahmen zu unterrichten und unterrichtet wiederum ihrerseits die betroffenen Aufsichtsbehörden. Die Aufsichtsbehörde, bei der hierzu eine Beschwerde eingereicht worden ist, unterrichtet den Beschwerdeführer über den Beschluss.

Wird eine Beschwerde eines Betroffenen abgewiesen oder abgelehnt, ergeht der Beschluss gegenüber dem Petenten durch die angerufene Aufsichtsbehörde. Das Unternehmen wird lediglich darüber informiert.

Wird einer Beschwerde nur zum Teil stattgegeben, ergehen zwei Beschlüsse – einer durch die federführende Aufsichtsbehörde gegenüber dem Unternehmen und einer der angerufenen Aufsichtsbehörde gegenüber dem Betroffenen.

In den sogenannten „Marktortfällen“ (vgl. hierzu oben unter 3.1), in denen keine Niederlassung in der Europäischen Union existiert, die Datenschutz-Grundverordnung aber dennoch anwendbar ist, weil sich zum Beispiel das Angebot an Bürger in der EU richtet, gibt es diesen Kooperationsmechanismus nicht. In diesen Fällen ist jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats zuständig und kann Entscheidungen erlassen. Daher können hier auch divergierende Entscheidungen ergehen.

3.2.2 Kohärenzverfahren

Dort wo in One-Stop-Shop-Fällen kein Konsens zwischen federführender und mitbetroffenen Aufsichtsbehörden im Verfahren der Zusammenarbeit erreicht werden kann, normieren Art. 63, 65 DSGVO das sogenannte **Kohärenzverfahren** mit der Befugnis des Europäischen Datenschutzausschusses, verbindliche Beschlüsse (Art. 65 Abs. 1 DSGVO)

zu treffen, um die ordnungsgemäße und einheitliche Anwendung der Verordnung in Einzelfällen sicherzustellen.

Das Verfahren hierzu ist in den Art. 65 Abs. 6, 60 Abs. 7 bis 9 DSGVO geregelt: Die federführende Aufsichtsbehörde trifft den endgültigen Beschluss auf der Grundlage des Beschlusses des Europäischen Datenschutzausschusses gegenüber der Hauptniederlassung des Verantwortlichen, der ihr EU-weit Folge zu leisten hat. Im Falle einer erfolglosen Beschwerde erlässt die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, den Beschluss gegenüber dem Beschwerdeführer. Zeitgleich mit dem Erlass des endgültigen Beschlusses gegenüber dem Verantwortlichen oder dem Beschwerdeführer wird ein etwaiger Beschluss des Europäischen Datenschutzausschusses auf dessen Webseite veröffentlicht.

Um zur einheitlichen Anwendung der Datenschutz-Grundverordnung beizutragen werden im sogenannten Kohärenzverfahren über die Klärung von Einzelfragen (One-Stop-Shop) hinaus aber auch **gemeinsame Positionen, Stellungnahmen und Richtlinien** bestimmt.

Technischer und organisatorischer Datenschutz (vgl. Nr. 2.4)

Die Datenschutz-Grundverordnung stellt die Bedeutung des technischen und organisatorischen Datenschutzes heraus. Hierzu zählen die Regelungen zu Privacy by Design/Privacy by Default, zur Auftragsdatenverarbeitung, zu Meldungen über Datenschutzverletzungen, zur Datenschutz-Folgenabschätzung und zu den betrieblichen/behördlichen Datenschutzbeauftragten. Zudem stärkt die Datenschutz-Grundverordnung die Selbstregulierung durch die Verantwortlichen.

Privacy by Design – Privacy by Default

Schon bisher gilt das Prinzip der Datenvermeidung und Datensparsamkeit. Mit der Einführung des „Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen“ (Art. 25 DSGVO) werden nun ausdrücklich Anforderungen an die Produktentwicklung und -implementierung gestellt, um eine wirksame Umsetzung dieser Datenschutzgrundsätze zu erreichen.

Der Verantwortliche hat hierfür sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung angemessene technische und organisatorische Maßnahmen zu treffen, wie z. B. Pseudonymisierung.

Der Verantwortliche muss darüber hinaus sicherstellen, dass Standardeinstellungen darauf ausgerichtet sind, nur personenbezogene Daten zu verarbeiten, die für den konkreten Zweck auch erforderlich sind. Das betrifft den Umfang der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Diese Regelungen werden Ausstrahlungswirkungen auf sämtliche Produkte, Systeme und Prozesse in den Unternehmen haben.

Auch wenn sich die Vorschrift unmittelbar nur an die Verantwortlichen richtet, wird sie sich auch mittelbar auf die Entwicklung von IT-Produkten und -Verfahren auswirken

4.2 Auftragsverarbeitung

Die Regelungen zur Auftragsverarbeitung (Art. 28 DSGVO) orientieren sich weitgehend an der Systematik von § 11 BDSG. Neu ist, dass die Einhaltung der Verpflichtungen des Auftragsverarbeiters zu den technisch-organisatorischen Maßnahmen durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO (Code of Conduct) oder durch eine Zertifizierung nach Art. 42 DSGVO nachgewiesen werden kann. (Art. 28 Abs. 5 DSGVO).

4.3 Meldungen von Datenschutzverletzungen

Verletzungen des Schutzes personenbezogener Daten müssen unverzüglich, nach Möglichkeit innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls, an die zuständige Aufsichtsbehörde gemeldet werden. Eine Ausnahme besteht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt. (vgl. Art. 33 Abs. 1 DSGVO). Ein solches Risiko kann z. B. durch eine geeignete Verschlüsselung personenbezogener Daten ausgeschlossen werden, die etwa beim Verlust eines Datenträgers die Kenntnisnahme der Daten durch Dritte verhindert. Besteht die Wahrscheinlichkeit, dass die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten bewirkt, muss der Verantwortliche auch die betroffene Person ohne unangemessene Verzögerung benachrichtigen – es sei denn, er hat technisch-organisatorische Maßnahmen getroffen, die eine Kenntnisnahme durch Dritte verhindern oder die sicherstellen, dass aller Wahrscheinlichkeit nach kein hohes Risiko mehr für die Rechte und Freiheiten der betroffenen Person besteht (Art. 34 DSGVO).

Kommt es bei einem Auftragsverarbeiter zu einem Datenschutzverstoß, muss dieser seinen Auftraggeber informieren (Art. 33 Abs. 2. DSGVO).

4.4 Datenschutz-Folgenabschätzung

Birgt die Art der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten, muss der Verantwortliche bereits vorab eine Abschätzung der Folgen für den Schutz personenbezogener Daten durchführen. Dies ist insbesondere der Fall bei neuen Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung (Art. 35 Abs. 1 DSGVO).

Die Datenschutz-Grundverordnung nennt in Art. 35 Abs. 3 bestimmte Fallgruppen, bei denen eine Folgenabschätzung stets durchzuführen ist. Dazu zählen das Profiling, die Verarbeitung besonders sensibler Daten sowie eine umfangreiche Videoüberwachung. Bei der Folgenabschätzung ist der behördliche oder betriebliche Datenschutzbeauftragte zu beteiligen (Art. 35 Abs. 2 DSGVO). Zeigt die Datenschutz-Folgenabschätzung ein verbleibendes hohes Risiko, muss zudem die Datenschutzaufsichtsbehörde konsultiert werden (Art. 36 Abs. 1 DSGVO).

4.5 Pflicht zur Bestellung eines behördlichen oder betrieblichen Datenschutzbeauftragten

Nach Art. 37 Abs. 1 DSGVO müssen in drei Fällen interne Datenschutzbeauftragte bestellt werden.

- Öffentliche Stellen haben, sofern sie personenbezogene Daten verarbeiten, stets einen Datenschutzbeauftragten zu bestellen. Ausgenommen sind Gerichte im Rahmen der rechtsprechenden Tätigkeit.
- Nicht-öffentliche Stellen haben einen Datenschutzbeauftragten zu bestellen, wenn deren Kerntätigkeit oder desjenigen, der Daten im Auftrag verarbeitet, in einer Datenverarbeitung besteht,
  - die aufgrund ihres Zwecks oder ihres Umfangs eine umfangreiche, regelmäßige und systematische Beobachtung von betroffenen Personen erfordert oder

- eine umfangreiche Verarbeitung von Daten, die nach Art. 9 oder 10 DSGVO besonders schutzwürdig sind, umfasst.

Erwägungsgrund 97 stellt klar, dass das „Kerngeschäft" die Hauptaktivität des Unternehmens meint. Bloße Nebentätigkeiten sollen nicht darunter fallen.

Darüber hinaus enthält Art. 37 Abs. 4 DSGVO zwei Öffnungsklauseln:
Verantwortliche oder Auftragsverarbeiter können auch freiwillig einen Datenschutzbeauftragten bestellen.
Eine weitere Öffnung besteht darin, dass die Mitgliedstaaten im nationalen Recht für weitere Fälle die Bestellung eines Datenschutzbeauftragten vorschreiben können. Hiervon hat der Bundesgesetzgeber durch § 38 Abs. 1 BDSG-neu Gebrauch gemacht. Danach werden Unternehmen in Deutschland auch künftig einen Datenschutzbeauftragten zu bestellen haben, wenn mehr als 10 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Auskunfteien, Adresshändler oder Markt- und Meinungsforschungsinstitute müssen in jedem Falle einen Datenschutzbeauftragten bestellen. Damit bleibt die geltende Rechtslage erhalten.

Art. 39 DSGVO normiert die vom Datenschutzbeauftragten wahrzunehmenden Aufgaben – wie Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters sowie der Beschäftigten, Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften, Schulungen und Zusammenarbeit mit der Aufsichtsbehörde.

Der Verantwortliche oder der Auftragsverarbeiter haben sicherzustellen, dass der Datenschutzbeauftragte frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. Sie haben ihn zu unterstützen und ihm die erforderlichen Ressourcen zur Verfügung zu stellen. Der Datenschutzbeauftragte ist weisungsfrei und berichtet unmittelbar der jeweiligen Leitungsebene. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Natürlich ist er zur Geheimhaltung verpflichtet. (Vgl. Art. 38 DSGVO.)

Die Rechtstellung und die Aufgaben sind weitgehend mit der derzeitigen Rechtslage in Deutschland identisch.

4.6 Stärkung der Selbstregulierung durch Zertifizierung und Verhaltensregeln

Die Datenschutz-Grundverordnung stärkt die Selbstregulierung durch Verhaltensregeln (Art. 40, 41 DSGVO) und Zertifizierungen (Art. 42, 43 DSGVO). Diese Instrumente bieten einerseits klare Wettbewerbsvorteile. Andererseits enthält die Datenschutz-Grundverordnung an verschiedenen Stellen Anreize zur Nutzung dieser Instrumente. So können sie beispielsweise bei der Beurteilung der Datensicherheit, beim Nachweis der Einhaltung der Verpflichtungen eines Auftragsverarbeiters, bei der Durchführung einer Datenschutz-Folgenabschätzung oder bei der Prüfung geeigneter Garantien für die Übermittlung in Drittländer herangezogen werden.

Zudem ist die Schaffung branchenspezifischer Verhaltensregeln zu bestimmten Aspekten - wie das berechtigte Interesse des Verantwortlichen in bestimmten Zusammenhängen oder die Datenübermittlung in Drittstaaten (Art. 40 Abs.2 lit. b, Abs. 2 lit. j DSGVO) - möglich.

Soweit nicht die Tätigkeit in mehreren Mitgliedstaaten betroffen ist, genehmigt und veröffentlicht die Aufsichtsbehörde die Verhaltensregeln (Art. 40 Abs. 5 und 6 DSGVO). Bei einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten werden sie dem Europäischen Datenschutzausschuss vorgelegt, der dazu Stellung nimmt. Die Europäische Kommission kann dann mit Durchführungsrechtsakten die allgemeine Gültigkeit in der Union regeln (Art. 40 Abs. 7-10 DSGVO).

Der Europäische Datenschutzausschuss führt ein Register aller genehmigten Verhaltensregeln und veröffentlicht sie (Art. 40 Abs. 11 DSGVO).

Ein weiteres wichtiges Instrument der Selbstregulierung ist die Möglichkeit der Zertifizierung von Verarbeitungsvorgängen (nicht von Stellen). Sie dient dazu, nachzuweisen, dass die Datenschutz-Grundverordnung bei Verarbeitungsvorgängen eingehalten wird (Art. 42 Abs. 1 DSGVO). Eine Zertifizierung wird durch die Aufsichtsbehörde oder durch eine hierfür akkreditierte Stelle ausgesprochen (Art. 42 Abs. 5 DSGVO).

Der Europäische Datenschutzausschuss führt und veröffentlicht ein Register aller Zertifizierungsmechanismen (Art. 42 Abs. 8 DSGVO).

Die Zertifizierungskriterien werden von den Aufsichtsbehörden, gegebenenfalls im Kohärenzverfahren, festgelegt (Art. 42 Abs. 5 DSGVO).

Die Europäische Kommission kann in delegierten Rechtsakten Anforderungen und in Durchführungsrechtsakten technische Standards festlegen (Art. 43 Abs. 8f. DSGVO).

5 Einzelne weitere Aspekte

5.1 Anwendungsbereich

Die Datenschutz-Grundverordnung ist grundsätzlich sowohl im nicht-öffentlichen, als auch im öffentlichen Bereich anwendbar.

Sie gilt nicht für die Verarbeitung zu **persönlichen und familiären Zwecken** (Haushaltsausnahme, Art. 2 Abs. 2 lit. c DSGVO). Angesichts des gegenüber der Datenschutzrichtlinie unveränderten Wortlautes verbleibt es insoweit bei dem sehr weiten Anwendungsbereich des Datenschutzrechts.

Ebenso gilt die Datenschutz-Grundverordnung nicht für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie für den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit durch diese Behörden (Art. 2 Abs. 2 lit. d DSGVO). Sie ist damit zum Beispiel nicht für die Tätigkeit der Bundes- und Landespolizeien oder die Staatsanwaltschaften anwendbar.

Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit sie im Rahmen der Tätigkeiten einer **Niederlassung** in der Union erfolgt – unabhängig davon, ob die Verarbeitung in der Union stattfindet (Art. 3 Abs. 1 DSGVO). Daneben gilt das unter Nr. 3.1 dargestellte Marktortprinzip.

Die unmittelbare Geltung der Datenschutz-Grundverordnung wird im öffentlichen Bereich durch die allgemeinen Öffnungsklauseln in Art. 6 sowie in Kapitel IX für spezifisch nationale Gesetzgebung relativiert.

Art. 6 Abs. 2 DSGVO enthält eine Öffnungsklausel in Bezug auf

- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO) sowie
- die Verarbeitung im öffentlichen Interesse oder in Ausübung hoheitlicher Gewalt (Art. 6 Abs. 1 lit. e DSGVO).

Erlaubt sind im Wesentlichen aber nur Konkretisierungen und Präzisierungen und keine grundsätzlichen Änderungen der Architektur der Datenschutz-Grundverordnung. Erfasst sind hiervon auch private Stellen, die im öffentlichen Interesse tätig sind, zum Beispiel im Gesundheitswesen, Nahverkehr usw.

Art. 6 Abs. 3 lit. b DSGVO verlangt für diese Datenverarbeitungen allerdings eine Rechtsgrundlage im nationalen Recht, in der zumindest der Zweck der Verarbeitung festzulegen ist. Sie kann aber auch die Bedingungen für die Rechtmäßigkeit, den Kreis der Betroffenen, die Übermittlungsempfänger oder Speicherfristen enthalten.

Insgesamt sind damit die Spielräume für die nationalen Gesetzgeber allerdings recht weit.

5.2 Verarbeitung besonders sensibler Daten

Die Verarbeitung besonders sensibler Daten unterliegt besonderen Bedingungen. So ist die Verarbeitung von personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung, Daten über Gesundheit oder Sexualleben und sexuelle Ausrichtung grundsätzlich untersagt (Art. 9 Abs. 1 DSGVO) – es sei denn es liegen bestimmte ausdrücklich geregelte Ausnahmen vor (Art. 9 Abs. 2 DSGVO). Diese sind im Vergleich zu Art. 6 DSGVO (vgl. hierzu Nr. 2.1) strenger. Beispielsweise muss eine Einwilligung hier ausdrücklich erfolgen.

Die Mitgliedstaaten können für die Verarbeitung von genetischen, biometrischen und gesundheitlichen Daten noch zusätzliche Bedingungen und Beschränkungen einführen oder aufrechterhalten (Art. 9 Abs. 4 DSGVO). Derartige Regelungen finden sich beispielsweise in § 22 BDSG-neu.

5.3 Beschäftigtendatenschutz

Die Datenschutz-Grundverordnung verzichtet auf detaillierte Regelungen zum Beschäftigtendatenschutz. Vielmehr enthält sie für diesen Bereich eine Öffnungsklausel (Art. 88 DSGVO). Danach können die Mitgliedstaaten durch Gesetz oder Kollektivvereinbarung spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten bei der Verarbeitung von Beschäftigtendaten vorsehen. Aufgrund dieser Öffnungsklausel hat der Bundesgesetzgeber nach dem Vorbild des geltenden § 32 BDSG den § 26 BDSG-neu als nationale konkretisierende Vorschrift zum Beschäftigtendatenschutz geschaffen.

5.4 Kirchen und Religionsgemeinschaften

Die Datenschutz-Grundverordnung gilt grundsätzlich auch für Kirchen und Religionsgemeinschaften. Sie enthält aber insoweit in Art. 91 DSGVO weitreichende Öffnungsklauseln.

Danach dürfen Kirchen und Religionsgemeinschaften ihre zum Zeitpunkt des Inkrafttretens bestehenden Regeln weiter anwenden, soweit diese in Einklang mit der Datenschutz-Grundverordnung gebracht werden.

Das bedeutet, dass in Deutschland die kirchlichen Datenschutzgesetze beibehalten werden können. Änderungen des bestehenden Rechts sind demgegenüber möglich und gegebenenfalls auch notwendig (»in Einklang gebracht werden«).

Die Kirchen und religiösen Vereinigungen, die solche umfassenden Datenschutzregeln anwenden, unterliegen nach Art. 91 Abs. 2 DSGVO der Kontrolle durch eine unabhängige Aufsichtsbehörde. Diese Vorschrift erlaubt es den Kirchen, eine spezifische Art der Datenschutzaufsicht vorzusehen. Damit können die Kirchen in Deutschland mit ihren eigenen kirchlichen Datenschutzbeauftragten insoweit ihre verfassungsrechtlich und europarechtlich geschützte Autonomie weiterhin ausüben. Die kirchlichen Datenschutzbeauftragten müssen allerdings die Bedingungen des Kapitel VI der Datenschutz-Grundverordnung erfüllen. Auch sie müssen daher unabhängig sein, ihnen müssen eine angemessene Ausstattung zur Verfügung gestellt sowie bestimmte Aufgaben und Befugnisse eingeräumt werden.

5.5 Sonderregeln für wissenschaftliche Zwecke, öffentliche Archive und Statistik

Die Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke sowie für Zwecke der Statistik wird durch die Datenschutz-Grundverordnung privilegiert.

Art. 5 Abs. 1 lit. b DSGVO normiert zunächst eine weitgehende Aufhebung der Zweckbindung für Daten, die ursprünglich für andere Zwecke verarbeitet wurden. Eine Weiterverarbeitung für die vorgenannten Zwecke gilt danach nicht als unvereinbar mit den ursprünglichen Zwecken.

Die Rechtsgrundlage für die Datenverarbeitung zu den genannten Zwecken kann nach Art. 89 DSGVO weitgehend in den Mitgliedstaaten geregelt werden. Gleiches gilt gem. Art. 9 Abs. 2 lit. j DSGVO auch für die Verarbeitung besonders sensibler Daten (wie zum Beispiel über die religiöse Überzeugung oder Gesundheitsdaten) zu diesen Zwecken. Dabei müssen angemessene Garantien zum Datenschutz vorgesehen werden. Zu den danach erforderlichen technisch-organisatorische Maßnahmen können im Forschungsbereich zum Beispiel Pseudonymisierung und Anonymisierung gehören.

Von einzelnen Betroffenenrechten (vgl. Nr. 2.6) sind Ausnahmen möglich, soweit sie voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen würden. Die §§ 27 und 28 des BDSG-neu enthalten hier einige spezifische Regelungen.

5.6 Medienprivileg

Der Ausgleich zwischen dem Persönlichkeitsschutz und den Kommunikationsfreiheiten bleibt gemäß Art. 85 DSGVO den Mitgliedstaaten vorbehalten. Dabei enthält Art. 85 Abs. 1 DSGVO einerseits den allgemeinen Auftrag an die Mitgliedstaaten, in ihrem Recht einen Ausgleich zwischen dem Recht auf Datenschutz und der Meinungs- und Informationsfreiheit herzustellen. Art. 85 Abs. 2 DSGVO erlaubt es den Mitgliedstaaten darüber hinaus, bei der Verarbeitung personenbezogener Daten zu journalistischen, literarischen, künstlerischen oder wissenschaftlichen Zwecken Ausnahmen von zahlreichen Kapiteln der Datenschutz-Grundverordnung vorzusehen, sofern dies zur Wahrung der Meinungs- und Informationsfreiheit, einschließlich der Presse- und Rundfunkfreiheit erforderlich ist. An diese Vorgabe müssen die in Deutschland in erster Linie im Landesrecht geregelten besonderen Bestimmungen des Datenschutzes bei Presse und Rundfunk angepasst werden.

6 Ausblick und nationale Umsetzung

Die Datenschutz-Grundverordnung ist als europäische Verordnung unmittelbar geltendes Recht. Als „Grundverordnung“ enthält sie aber eine Vielzahl von Öffnungsklauseln, die Spielraum für nationales Recht der Mitgliedstaaten schaffen.

Auf den nationalen Gesetzgeber kommt daher ein erheblicher Umsetzungsbedarf zu. Darüber hinaus muss das gesamte Datenschutzrecht von Bund und Ländern auf seine Vereinbarkeit mit der Datenschutz-Grundverordnung geprüft und - soweit erforderlich - bereinigt werden.

Hinsichtlich des Anpassungsbedarfs im deutschen Datenschutzrecht ist zwischen dem öffentlichen und dem nicht-öffentlichen Bereich zu unterscheiden.

Im öffentlichen Bereich werden die geltenden bereichsspezifischen Vorschriften aufgrund der Öffnungsklauseln in Art. 6 Abs. 2, Art. 6 Abs. 3, Art. 9 Abs. 4, Art. 23 DSGVO und in Kapitel IX zum überwiegenden Teil erhalten bleiben. Durch den Gesetzgeber ist aber zu prüfen, in welchem Umfang eine Anpassung und Rechtsbereinigung notwendig ist. Erste Anpassungen im Bereich der Verarbeitung von Sozialdaten und im Steuerrecht hat der Bundesgesetzgeber bereits vorgenommen.

Im nicht-öffentlichen Bereich bestehen demgegenüber deutlich geringere Spielräume für nationale Regelungen.

Mit dem neuen BDSG hat der Bundesgesetzgeber bereits von einer Reihe von Regelungsspielräumen Gebrauch gemacht. Dabei hat er neben den zwingend umzusetzenden Regelungen auch zahlreiche optionale Möglichkeiten genutzt.

Zu den zwingend umzusetzenden Regelungen gehören beispielsweise die Vorschriften zur Einrichtung und näheren Ausgestaltung der Aufsichtsbehörden die für die BfDI in den §§ 8 ff. BDSG-neu geschaffen worden sind. Dazu gehören aber auch die Regelungen zur Vertretung der deutschen Datenschutzbehörden im Europäischen Datenschutzaus-

schuss und zur Zusammenarbeit der Datenschutzbehörden in Bund und Ländern, die in den §§ 17 bis 19 BDSG-neu enthalten sind.

Hinsichtlich der optionalen Öffnungsmöglichkeiten sind vor allem die Vorschriften zur Verarbeitung besonders schutzwürdiger Daten (§ 22 BDSG-neu) zur Zweckänderung (§§ 23, 24 BDSG-neu), zur Verarbeitung von Beschäftigtendaten (§ 26 BDSG-neu), zur Einschränkung der Betroffenenrechte (§§ 32 bis 37 BDSG-neu) und zur Bestellung betrieblicher Datenschutzbeauftragter (§ 38 BDSG-neu) von Bedeutung.