INFO
06

Die DSGVO in der Bundesverwaltung

BfDI
Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Impressum

Herausgegeben von:

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Postfach 14 68, 53004 Bonn
Tel. +49 (0) 228 997799-0
Fax +49 (0) 228 997799-5550
E-Mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de

Stand: Dezember 2020

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

Realisation: Appel & Klinger Druck und Medien GmbH

Bildnachweis: Adobe Stock

Hinweis:
Die Verwendung des generischen Maskulinums erfolgt aufgrund
des Gesetzeswortlauts der DSGVO.

Die DSGVO in der Bundesverwaltung

BfDI – Info 6

Inhalt

Vorwort 8

1 Verfahren – Anforderungen und Anpassung 10

1.1 Nachweis- und Rechenschaftspflichten der DSGVO und weiterer Rechtsvorschriften insbesondere nach Art. 5, 24 und 25 DSGVO 10

1.2 Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO 12

1.2.1 Adressat der Erstellungs- und Führungspflicht 13

1.2.2 Inhalt des Verzeichnisses für Verantwortliche 14

1.3 Anforderungen an die Datensicherheit nach Art. 25 und 32 DSGVO 15

1.3.1 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen nach Art. 25 DSGVO 15

1.3.2 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO 15

1.3.3 Stand der Technik und Geeignetheit der Maßnahmen 16

1.3.4 Zertifizierung und genehmigte Verfahrensregeln nach Art. 42 und 43 DSGVO 17

1.4 Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO 17

1.4.1 Verpflichtung des Verantwortlichen zur Durchführung einer DSFA 17

1.4.2 Welche Verarbeitungen erfordern eine DSFA 18

1.4.3 Behandlung von Bestandsverfahren 18

1.4.4 Hinweise zur Vorabkonsultation des BfDI nach Art. 36 DSGVO 19

1.5 Meldung von Datenschutzverletzungen nach Art. 33 und 34 DSGVO 19

1.5.1 Voraussetzungen der Verpflichtung zur Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO 19

1.5.2 Voraussetzungen der Verpflichtung zur Benachrichtigung der von der Verletzung betroffenen Person nach Art. 34 DSGVO ... 21

1.5.3 Dokumentationspflichten im Zusammenhang mit Art. 33 und 34 DSGVO ... 22

1.5.4 Empfehlung der zur Sicherstellung der Meldepflichten erforderlichen organisatorischen Maßnahmen des Verantwortlichen nach Art. 33 und 34 DSGVO ... 22

1.6 Auftragsverarbeitung nach Art. 28 DSGVO ... 23

1.6.1 Einführung ... 23

1.6.2 Bestandsaufnahme, Prüfung bestehender Verträge hinsichtlich Konformität mit DSGVO ... 25

1.6.3 Neuabschluss von Verträgen zur Auftragsverarbeitung nach Art. 28 DSGVO ... 27

2 Datenschutzbeauftragte (DSB) nach Art. 37, 38 und 39 DSGVO ... 28

2.1 Regelungen der DSGVO für den DSB ... 28

2.1.1 Benennung/Rechtsstellung des DSB nach Art. 37 und 38 DSGVO ... 28

2.1.2 Aufgaben des DSB nach Art. 39 DSGVO ... 32

2.2 Zusammenarbeit des DSB mit dem BfDI/ Anlaufstelle für den BfDI nach Art. 39 Abs. 1 lit. d) DSGVO ... 33

2.3 Verantwortlichkeitsverteilung DSB – Verantwortlicher nach Art. 5 Abs. 2, Art. 24 und Art. 39 Abs. 1 lit. a) DSGVO ... 34

3 Rechtsgrundlagen ... 35

3.1 Systematik des Datenschutzrechts ... 35

3.1.1 Vorrang der DSGVO ... 35

3.1.2 Anwendungsbereich der JI-Richtlinie ... 36

3.1.3 Öffentliche Stellen außerhalb des Anwendungsbereichs des EU-Rechts nach § 1 Abs. 8 BDSG ... 37

3.2 Zulässigkeit der Datenverarbeitung nach der DSGVO ... 37

3.2.1 Allgemeines ... 37

3.2.2 Die einzelnen Zulässigkeitstatbestände der DSGVO nach Art. 6 DSGVO ... 37

3.3 Beschäftigtendatenschutz 40

3.3.1 Beschäftigtendatenschutz gemäß Art. 88 DSGVO und § 26 BDSG 40

3.3.2 Übersicht über den Regelungsinhalt von § 26 BDSG 41

3.3.3 Spezifische Regelungen für Beamte nach §§ 106 ff. BBG 41

4 Umsetzung der Betroffenenrechte 42

4.1 Informationspflichten nach Art. 13 und 14 DSGVO 42

4.1.1 Informationspflicht bei Direkterhebung nach Art. 13 DSGVO 43

4.1.2 Datenerhebung bei Dritten im Hinblick auf Art. 14 DSGVO 45

4.1.3 Informationen bei Zweckänderung nach Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO 45

4.1.4 Ausnahmen nach Art. 13 Abs. 4 und 14 Abs. 5 DSGVO sowie §§ 32 und 33 BDSG 45

4.1.5 Implementierung der Informationspflichten nach Art. 12 DSGVO 46

4.2 Auskunftsrecht nach Art. 15 DSGVO 46

4.2.1 Ausnahmen nach § 34 BDSG 47

4.2.2 Form und Frist der Auskunftserteilung nach Art. 15 Abs. 3 DSGVO 48

4.2.3 Implementierung eines Auskunftsprozesses nach Art. 12 DSGVO 48

4.3 Recht auf Berichtigung nach Art. 16 DSGVO 48

4.4 Recht auf Löschung („Recht auf Vergessenwerden“) nach Art. 17 DSGVO 49

4.5 Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO 50

4.6 Mitteilungspflicht über Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung nach Art. 19 DSGVO 51

4.7 Widerspruchsrecht nach Art. 21 DSGVO 52
4.8 Automatisierte Einzelfallentscheidung nach Art. 22 DSGVO 52
4.9 Implementierung von Prozessen zur Gewährleistung der Betroffenenrechte entsprechend Art. 12 DSGVO 53

Vorwort

Seit dem 25. Mai 2018 besteht mit der Datenschutz-Grundverordnung (DSGVO) und der Richtlinie für den Datenschutz bei der polizeilichen und justiziellen Datenverarbeitung ein umfassender, europaweit einheitlicher Rechtsrahmen für die Verarbeitung personenbezogener Daten und zum Schutz der Rechte und Freiheiten der Menschen in der digitalen Welt. Mittlerweile wurden auch das Bundesdatenschutzgesetz (BDSG) und zahlreiche weitere Gesetze an die DSGVO angepasst.

Die europaweite Vereinheitlichung des Datenschutzrechts hat neue Schwerpunkte gesetzt, auch mit Blick auf andere Rechtsgebiete. Der Schutz personenbezogener Daten hat in der täglichen Arbeit der öffentlichen Stellen des Bundes und nicht zuletzt auch ihrer Datenschutzbeauftragten (DSB) einen noch höheren Stellenwert erhalten. Die DSGVO und das BDSG legen einen besonderen Fokus auf die Dokumentation der Verarbeitung personenbezogener Daten und auf den entsprechenden Nachweis der Einhaltung der datenschutzrechtlichen Bestimmungen.

Die DSGVO enthält – erstmals auch europaweit – einheitliche Regelungen zur Benennung, Rechtsstellung und zu den Aufgaben der Datenschutzbeauftragten. Damit hat der Europäische Gesetzgeber das in Deutschland bereits seit langem bestehende und bewährte Rechtsinstrument der Datenschutzbeauftragten bestätigt und verfestigt; auch wenn in Deutschland diese Regelungen zwischenzeitlich leider aufgeweicht wurden.

Schließlich sind die Befugnisse des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zur Durchsetzung des Datenschutzrechts in der Bundesverwaltung durch die DSGVO deutlich erweitert worden. Der BfDI kann rechtsverbindliche Anordnungen zur Durchsetzung der datenschutzrechtlichen Bestimmungen auch gegenüber öffentlichen Stellen des Bundes treffen. Mehr denn je unterstützt der BfDI die öffentlichen Stellen des Bundes bei der Umsetzung der oft abstrakt gehaltenen rechtlichen Anforderungen auch beratend.

In die hiermit vorliegende 2. Auflage dieser Broschüre sind die Erfahrungen aus mehr als zweieinhalb Jahren der Anwendung des neuen Rechtsrahmens eingeflossen. Die Broschüre soll damit weiterhin dazu beitragen, aktuell über die Schwerpunkte des einheitlichen europäischen Datenschutzrechts zu informieren. Sie richtet sich in erster Linie an diejenigen Organisationseinheiten aller öffentlichen Stellen des Bundes, die für die Einhaltung des Datenschutzes Verantwortung tragen und darüber hinaus auch an die Datenschutzbeauftragten aller öffentlichen Stellen des Bundes.

Bonn, im Dezember 2020

Prof. Ulrich Kelber
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

1 Verfahren – Anforderungen und Anpassung

1.1 Nachweis- und Rechenschaftspflichten der DSGVO und weiterer Rechtsvorschriften insbesondere nach Art. 5, 24 und 25 DSGVO

Nach dem Grundsatz der Rechenschaftspflicht in Art. 5 Abs. 2 DSGVO hat der Verantwortliche die Grundsätze in Art. 5 Abs. 1 DSGVO einzuhalten und deren Einhaltung auch nachzuweisen. Die Rechenschaftspflicht wird konkretisiert durch Art. 24 und 25 DSGVO. Nach Art. 24 DSGVO hat der Verantwortliche durch geeignete technische und organisatorische Maßnahmen sicherzustellen und nachzuweisen, dass die Verarbeitung gemäß der DSGVO erfolgt. Art. 25 DSGVO fordert dazu Maßnahmen der Technikgestaltung und datenschutzfreundliche Voreinstellungen (Data Protection by Design und Data Protection by Default).

Der Verantwortliche hat eine Dokumentation zu erstellen, mit der er nachweist, dass er rechtmäßig handelt. Durch diese Dokumentationspflicht wird er angehalten, die Einhaltung der genannten Vorschriften zu prüfen. Den Aufsichtsbehörden und den DSB wird durch die Prüfung, ob der Verantwortliche personenbezogene Daten rechtmäßig verarbeitet, die Arbeit erleichtert. Die DSGVO hat die Rechenschaftspflicht in dieser Form neu eingeführt.

Im Einzelnen ist insbesondere die Einhaltung der folgenden Vorschriften der DSGVO nachzuweisen:

- Rechtmäßigkeit der Datenverarbeitung, Rechtsgrundlagen,
- Verarbeitung nach Treu und Glauben und Transparenz, Information und Auskunft,
- Zweckbindung, Weiterverarbeitung,
- Datenminimierung,
- Richtigkeit, Berichtigung und Einschränkung der Verarbeitung,
- Speicherbegrenzung, Löschung,
- Integrität und Vertraulichkeit, Sicherheit der Verarbeitung.

Die DSGVO macht keine Angaben über die Art und Weise der Dokumentation. Die Aufsichtsbehörden erwarten jedoch in einem möglichst frühen Stadium der Entwicklung des Verfahrens die Vorlage eines aussagekräftigen Datenschutzkonzepts. Darin ist insbesondere darzustellen:

- die Verarbeitung der personenbezogenen Daten im Geschäftsprozess,
- die Begründung der Rechtmäßigkeit auf der Grundlage der konkreten Rechtsgrundlage,
- die Beachtung der Grundsätze der Zweckbindung und Datenminimierung,
- die Umsetzung der Anforderungen, die sich aus dem Grundsatz der Speicherbegrenzung und den Betroffenenrechten ergeben,
- die Gewährleistung der Sicherheit der Verarbeitung im Hinblick auf die Grundsätze der Vertraulichkeit, Integrität und Verfügbarkeit.

Zur Festlegung der erforderlichen technischen und organisatorischen Maßnahmen kann das Standard-Datenschutzmodell (SDM) der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) herangezogen werden.

Bei der Anwendung des Art. 24 Abs. 1 S. 1 DSGVO und des Erwägungsgrunds (EG) 76 ist der sogenannte risikobasierte Ansatz zu beachten.

Danach sollen die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person bestimmt werden.

In einigen der dem Art. 24 DSGVO nachfolgenden Vorschriften über den Verantwortlichen wird dieser risikobasierte Ansatz herangezogen (z. B. Art. 32 DSGVO – Sicherheit der Verarbeitung). Außerdem enthalten diese Vorschriften auch weitere Konkretisierungen der Rechenschaftspflicht, z. B. Art. 30 DSGVO – Verzeichnis der Verarbeitungstätigkeiten – und Art. 35 DSGVO – Datenschutz-Folgenabschätzung (DSFA).

1.2 Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO

Alle öffentlichen Stellen des Bundes haben – ebenso wie andere Verantwortliche – gemäß Art. 30 DSGVO ein Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten zu führen. Es betrifft sämtliche auch teilweise automatisierte sowie nichtautomatisierte Verarbeitungen, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Als Verarbeitungstätigkeit ist bei öffentlichen Stellen die Erfüllung einer bestimmten Aufgabe auf geeignetem Abstraktionsniveau zu verstehen. Beispiele sind die Erteilung von strom- und schifffahrtspolizeilichen Genehmigungen, die Zulassung von Arzneimitteln, die Bewilligung von Beihilfe oder die Bearbeitung von Bürgerbeschwerden. Die Verarbeitungstätigkeit ist dabei grundsätzlich an die Zweckbestimmung einer zu erfüllenden Aufgabe gebunden.

Die Verpflichtung zur Führung des Verzeichnisses von Verarbeitungstätigkeiten soll dem Nachweis der Einhaltung der Verordnung dienen (vgl. EG 82 DSGVO) und konkretisiert damit die allgemeine Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO. Siehe hier Kurzpapier Nr. 1 des DSK unter www.bfdi.bund.de/kurzpapiere.

Einerseits dokumentiert das Verzeichnis die Umsetzung von materiellen Anforderungen der DSGVO und schafft damit Transparenz der Verarbeitung. Andererseits verpflichtet es die Verantwortlichen auch, sich mit den datenschutzrechtlichen Vorgaben auseinanderzusetzen. Dies trägt so dazu bei, dass die Vorgaben in den Verarbeitungsprozessen und deren Gestaltung Berücksichtigung finden.

Das Verzeichnis ist nach Art. 30 Abs. 4 DSGVO dem BfDI als zuständiger Aufsichtsbehörde für die öffentlichen Stellen des Bundes auf Anfrage zur Verfügung zu stellen.

Der Aufsichtsbehörde und dem behördlichen DSB dient es als Ausgangspunkt ihrer Kontrollmaßnahmen. Es kann aber in der Regel nur eine vorläufige Rechtmäßigkeitsprüfung ermöglichen.

Das Verzeichnis dient internen Zwecken und ist nicht öffentlich zugänglich. Das Verzeichnis ist schriftlich oder elektronisch zu führen (Art. 30 Abs. 3 DSGVO). Auch Auftragsverarbeiter (AV) müssen ein eigenständiges Verzeichnis der Verarbeitungstätigkeiten führen (Art. 30 Abs. 2 DSGVO). Dieses enthält einen etwas geringeren Umfang an Informationen.

Die DSK hat Hinweise zum Verzeichnis von Verarbeitungstätigkeiten sowie entsprechende Muster für Verantwortliche und Auftragsverarbeiter herausgegeben und veröffentlicht. (www.bfdi.bund.de/muster-verarbeitungsverzeichnis)

1.2.1 Adressat der Erstellungs- und Führungspflicht

Adressat der in Art. 30 DSGVO normierten Verpflichtung zur Erstellung und Führung des Verzeichnisses von Verarbeitungstätigkeiten sind die Verantwortlichen und ggf. deren Vertreter. Die Erstellung der einzelnen Beiträge über die Verarbeitungsprozesse sollte von den Fachreferaten und/oder Organisationseinheiten geleistet werden können, die mit den Verarbeitungsprozessen befasst sind. Die Verpflichtung zur Erstellung und Aktualisierung des Verfahrensverzeichnisses ist keine Aufgabe des DSB. Der Europäische Datenschutzausschuss (EDSA) erachtet es jedoch als zulässig, eine Übertragung von Tätigkeiten im Zusammenhang mit der Erstellung und Führung des Verarbeitungsverzeichnisses auf DSB vorzunehmen (EDSA – Artikel 29 Gruppe, WP 243, Leitlinien in Bezug auf DSB, zu 4.5, Seite 22 f., https://ec.europa.eu/newsroom/article29/news-overview.cfm).

Die Rechenschaftspflicht kann nicht vom Verantwortlichen auf den DSB übertragen werden. Die Führung des Verzeichnisses von Verarbeitungstätigkeiten ist keine originäre Aufgabe des DSB.

Davon unbenommen bleibt selbstverständlich die Beratungsfunktion des DSB im Sinne des Art. 39 Abs. 1 DSGVO. Auf Grund seiner

Fachkompetenz dürfte es vorteilhaft sein, den DSB in den Prozess der Erstellung und Aktualisierung des Verzeichnisses einzubinden. Zudem gehört die Überwachung der Vollständigkeit und Rechtmäßigkeit der Verzeichnisse zu den Aufgaben des DSB.

1.2.2 Inhalt des Verzeichnisses für Verantwortliche

Das Verzeichnis der Verarbeitungstätigkeiten enthält eine schriftliche Dokumentation der wesentlichen Informationen einer Datenverarbeitung. Die Pflichtangaben ergeben sich aus Art. 30 Abs. 1 S. 2 und Art. 49 Abs. 6 DSGVO:

- Namen und Kontaktdaten des/der gemeinsam Verantwortlichen sowie deren Vertreter;
- Angaben und Kontaktdaten der behördlichen DSB;
- Angaben über die Zwecke und Rechtsgrundlagen der Verarbeitung;
- Beschreibungen der Kategorien der betroffenen Personen und der betroffenen Datenkategorien personenbezogener Daten. Dabei sollte erkennbar werden, ob es sich um besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO handelt;
- Empfänger bzw. Beschreibung der Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt werden;
- Aussage dazu, ob Datentransfers in Drittländer oder an internationale Organisationen erfolgen. Ist dies der Fall, dann ist das Verarbeitungsverzeichnis um Angaben zur Angemessenheitsentscheidung der EU-Kommission bzw. um die Abwägungsergebnisse des Verantwortlichen für die vorgesehenen und angemessenen Garantien zu ergänzen;
- wenn möglich, Löschfristen;
- wenn möglich, eine Darstellung der wesentlichen technischen und organisatorischen Maßnahmen.

Darüber hinaus ist ausdrücklich zu empfehlen, auch Angaben zum Vorliegen einer Auftragsverarbeitung mit in das Verzeichnis für Verantwortliche aufzunehmen. Damit wird für den DSB, aber auch für den BfDI leichter erkennbar, ob eine Beauftragung vorliegt und ob hierbei die gesetzlichen Anforderungen eingehalten worden sind.

1.3 Anforderungen an die Datensicherheit nach Art. 25 und 32 DSGVO

1.3.1 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen nach Art. 25 DSGVO

Die beiden Prinzipien Datenschutz durch Technikgestaltung (Data Protection by Design) sowie durch datenschutzfreundliche Voreinstellungen (Data Protection by Default) regeln die Anforderung an die Gestaltung und den Betrieb von Verfahren, die personenbezogene Daten verarbeiten. Auf diese Weise soll der Verantwortliche für die Datenverarbeitung dazu verpflichtet werden, möglichst frühzeitig, also bereits in der Phase des Entwurfs bzw. der Umsetzung eines Verfahrens die Voraussetzungen dafür zu schaffen, dass die Anforderungen der Verordnung eingehalten werden.

Art. 25 DSGVO verpflichtet den Verantwortlichen außerdem, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass nur solche personenbezogenen Daten verarbeitet werden, die für den jeweils bestimmten Verarbeitungszweck notwendig sind, und dass diese Daten auch nicht einer unbestimmten Zahl von Personen zugänglich gemacht werden.

Art. 25 DSGVO konkretisiert damit das Prinzip der Datensparsamkeit (vgl. auch Art. 5 DSGVO „Datenminimierung“).

1.3.2 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Sowohl der Verantwortliche als auch ein möglicher Auftragsverarbeiter sind dazu verpflichtet, geeignete technische und organisatorische Maßnahmen umzusetzen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, das durch die Verarbeitung der Daten entsteht. Art. 32 DSGVO nennt ausdrücklich die drei Grundwerte der Informationssicherheit: Vertraulichkeit, Integrität und Verfügbarkeit als Schutzziele. Darüber hinaus werden weitere Anforderungen an die Verarbeitung gestellt, nämlich die Belastbarkeit der Systeme und Dienste sowie die Fähigkeit, die Verfügbarkeit bei Zwischenfällen rasch wiederherzustellen.

Auf diese Weise stellt Art. 32 DSGVO eine enge Verbindung zwischen Datenschutz und IT-Sicherheit bzw. IT-Sicherheitsmanagement her.

Als konkrete Beispiele für mögliche Maßnahmen nennen Art. 25 und 32 DSGVO die Pseudonymisierung sowie Art. 32 DSGVO zusätzlich die Verschlüsselung personenbezogener Daten.

1.3.3 Stand der Technik und Geeignetheit der Maßnahmen

Wichtig sowohl bei Art. 25 als auch bei Art. 32 DSGVO ist, dass die Maßnahmen, die Verantwortliche und/oder Auftragsverarbeiter ergreifen, dem Stand der Technik entsprechen müssen. Die Beurteilung der Angemessenheit der Maßnahmen soll insbesondere auch unter Berücksichtigung des Implementierungsaufwands und der bestehenden Risiken erfolgen. Auf diese Weise wird der risikobasierte Ansatz bei der Beurteilung von Verfahren zur Verarbeitung personenbezogener Daten zum Regelfall erklärt. Eine Herausforderung bei der Umsetzung wird sicherlich oft die Frage sein, was zu einem bestimmten Zeitpunkt als Stand der Technik betrachtet werden kann bzw. muss. Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden. Gemeint sind bewährte Techniken und Vorgehensweisen, die auf gesicherten Erkenntnissen beruhen und ausreichend zur Verfügung stehen, um angemessen umgesetzt zu werden. Die Verpflichtung schließt also die Möglichkeit eines neuen bzw. anderen Vorgehens nicht aus, wenn hierbei ein ebenso effektiver Schutz gewährleistet wird.

Für den Bereich der Bundesverwaltung sind die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten Mindeststandards (https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards_Bund/Mindeststandards_Bund_node.html) verbindlich umzusetzen, und es muss ein Sicherheitsmanagement nach dem BSI-Grundschutz aufgebaut werden. Die Umsetzung der Mindeststandards und des IT-Grundschutzes stellt für den Bereich der technisch-organisatorischen Maßnahmen des Datenschutzes eine gute Basis dar. In Abhängigkeit von der konkreten Verarbeitungstätigkeit kann es trotzdem erforderlich sein, zusätzliche Maßnahmen umzusetzen.

1.3.4 Zertifizierung und genehmigte Verfahrensregeln nach Art. 42 und 43 DSGVO

Die DSGVO sieht in Art. 42 ein datenschutzspezifisches Zertifizierungsverfahren vor, das die Einhaltung der europarechtlichen Datenschutzbestimmungen gewährleisten soll. Diesem Zertifizierungsverfahren können sich zukünftig private und öffentliche Institutionen stellen. Um für die zukünftig geplanten Zertifizierungsverfahren einen möglichst hohen Qualitätsstandard sicherzustellen, sieht die DSGVO in Art. 43 vor, dass nur solche Stellen Zertifizierungen nach Art. 42 erteilen dürfen, die im Vorhinein auf ihre Eignung zur Durchführung von Zertifizierungsverfahren überprüft und anschließend förmlich akkreditiert worden sind. Für die Bundesrepublik Deutschland sieht § 39 BDSG eine Konstruktion vor, bei der die Entscheidung, ob jemand als Zertifizierungsstelle agieren darf, durch die jeweils zuständige Datenschutzaufsichtsbehörde (BfDI oder eine Datenschutzaufsichtsbehörde eines Landes) auf Grundlage einer Akkreditierung durch die Deutsche Akkreditierungsstelle (DAkkS) erfolgen soll. Bisher gibt es in Deutschland noch keine nach Art. 43 DSGVO akkreditierten Zertifizierungsstellen und demnach auch noch keine Zertifizierungen nach Art. 42 DSGVO. Die Ausarbeitung der dafür erforderlichen Grundlagen ist aber weit fortgeschritten.

1.4 Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO

1.4.1 Verpflichtung des Verantwortlichen zur Durchführung einer DSFA

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, vermutlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche nach Art. 35 DSGVO vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Eine DSFA ist folglich eine für bestimmte Verarbeitungsvorgänge vorgeschriebene strukturierte Risikoanalyse. Sie dient einer Vorabbewertung derjenigen Verarbeitungsvorgänge, die ein Verantwortlicher vornehmen möchte.

1.4.2 Welche Verarbeitungen erfordern eine DSFA

Eine DSFA ist gemäß Art. 35 Abs. 1 DSGVO immer dann erforderlich, wenn eine geplante Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Art. 35 Abs. 3 DSGVO nennt explizit drei Klassen von Verarbeitungen, für die regelmäßig eine DSFA durchgeführt werden muss.

Diese sind:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Öffentliche Stellen des Bundes sind bei bestimmten Verarbeitungen personenbezogener Daten außerdem verpflichtet, eine DSFA zu erstellen, wenn die Verarbeitung bestimmte Voraussetzungen erfüllt. Maßgeblich dafür ist die vom BfDI erstellte und veröffentlichte Liste nach Art. 35 Abs. 4 DSGVO. Diese kann unter www.bfdi.bund.de/liste-verarbeitungsvorgaenge abgerufen werden.

1.4.3 Behandlung von Bestandsverfahren

Die Regelungen zur DSFA sind auf Datenverarbeitungen, deren datenschutzrechtliche Prüfung vor dem 25. Mai 2018 abgeschlossen wurde, nur dann anzuwenden, wenn sich bei diesen Verfahren Änderungen ab dem Zeitpunkt der Geltung der DSGVO nach Art. 99 Abs. 2 DSGVO ergeben haben. Voraussetzung dafür ist, dass vor dem 25. Mai 2018 bereits eine Vorabkontrolle stattgefunden hatte. Unabhängig davon wird mit Blick auf einen einheitlichen Datenschutzstandard der Behörde emp-

fohlen, alle Bestandsverfahren sukzessive einer Überprüfung unter Zugrundelegung der Regelungen zur DSFA zu unterziehen.

1.4.4 Hinweise zur Vorabkonsultation des BfDI nach Art. 36 DSGVO

Der Verantwortliche ist nach Art. 36 Abs. 1 DSGVO verpflichtet, die Aufsichtsbehörde vor der Verarbeitung zu konsultieren, wenn aus der DSFA hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, und sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft. Eine Konsultation der Aufsichtsbehörde ist mithin nur dann erforderlich, wenn nach den Gegenmaßnahmen ein Restrisiko verbleibt und dieses als zu hoch eingestuft wird. Dabei sind der Aufsichtsbehörde Informationen nach Art. 36 Abs. 3 DSGVO vorzulegen.

Soweit die Aufsichtsbehörde dabei zu dem Ergebnis kommt, dass die geplante Verarbeitung nicht datenschutzkonform wäre, unterbreitet sie dem Verantwortlichen ggf. Empfehlungen zur Eindämmung des Risikos und kann die ihr durch Art. 58 DSGVO übertragenen Befugnisse ausüben. Dies betrifft insbesondere die Befugnis nach Art. 58 Abs. 2 lit. f) DSGVO, eine vorübergehende oder endgültige Beschränkung der Verarbeitung – einschließlich deren Verbots – anzuordnen.

1.5 Meldung von Datenschutzverletzungen nach Art. 33 und 34 DSGVO

Nach der DSGVO hat – wenn der Schutz personenbezogener Daten verletzt ist und bestimmte Voraussetzungen erfüllt sind – eine Meldung des Verantwortlichen an den BfDI und ggf. zusätzlich eine Benachrichtigung an die von der Verletzung betroffene Person zu erfolgen.

1.5.1 Voraussetzungen der Verpflichtung zur Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO

Der für die Datenverarbeitung Verantwortliche – nicht jedoch der Auftragsverarbeiter – hat dem BfDI die Datenschutzverletzung zu melden.

Der Auftragsverarbeiter ist jedoch verpflichtet, eine Verletzung, soweit sie im Rahmen seiner Tätigkeit eingetreten ist, dem Verantwortlichen zu melden, damit dieser ggf. seiner Verpflichtung gegenüber dem BfDI nachkommen kann.

Grundsätzlich löst die Verletzung des Schutzes jedes personenbezogenen Datums die Meldepflicht aus. Eine Verletzung liegt nach Art. 4 Ziff. 12 DSGVO vor bei einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Dabei ist es irrelevant, wer oder was für die Verletzung ursächlich war oder ist oder ob Dritte von den personenbezogenen Daten Kenntnis erlangten.

Die Meldepflicht entfällt, soweit kein Risiko für die Rechte und Freiheiten der betroffenen Person vorliegt.

Die Feststellung dazu setzt eine Prognoseentscheidung des Verantwortlichen voraus, für deren Richtigkeit er die Verantwortung trägt. Zu berücksichtigen sind dabei alle Folgen für die Persönlichkeitsentfaltung des Betroffenen sowie drohende physische, materielle und immaterielle Schäden. Die Überlegungen bedürfen einer jeweiligen Betrachtung der konkreten Umstände des Einzelfalls.

Die Meldung an den BfDI kann formlos erfolgen. Allerdings ist im Hinblick auf die Dokumentations- und Rechenschaftspflichten des Verantwortlichen die Schriftform angezeigt.

Der Mindestinhalt der Meldung ergibt sich aus Art. 33 Abs. 3 DSGVO und umfasst:

a) die Art der Verletzung – wenn möglich Angabe der Kategorien – hinsichtlich der Betroffenen, der Datensätze und der ungefähren Anzahl der Betroffenen,

b) Namen und Kontaktdaten des DSB oder einer sonstigen Anlaufstelle für weitere Informationen,

c) die Beschreibung der wahrscheinlichen Folgen der Verletzung der personenbezogenen Daten,

d) die Beschreibung, was der Verantwortliche getan hat oder welche Maßnahmen vorgeschlagen werden, um die Verletzung zu beheben oder nachteilige Auswirkungen abzumildern.

Die Angaben müssen den BfDI in die Lage versetzen, den Sachverhalt sowie die Angemessenheit der ergriffenen Maßnahmen beurteilen zu können.

Die Meldung soll unverzüglich nach Kenntnis von der Datenschutzverletzung erfolgen, möglichst binnen 72 Stunden. Dabei kann sie auch in mehreren Schritten vorgenommen werden. Ein solches Vorgehen empfiehlt sich in den Fällen, in denen einzelne, erforderliche Angaben nur mit Zeitverzug ermittelt werden können. Soweit die Frist nicht eingehalten werden kann, ist die Verzögerung zu begründen.

1.5.2 Voraussetzungen der Verpflichtung zur Benachrichtigung der von der Verletzung betroffenen Person nach Art. 34 DSGVO

Der für die Datenverarbeitung Verantwortliche, nicht der Auftragsverarbeiter, hat die Betroffenen über die Verletzung zu benachrichtigen, wenn diese voraussichtlich mit einem hohen Risiko für die persönlichen Rechte und Freiheiten der Betroffenen verbunden ist. Davon ist dann auszugehen, wenn die Verletzung entweder mit einem hohen Grad der Wahrscheinlichkeit eintreten kann oder wenn der potentielle Schaden für die betroffenen Personen sehr hoch ist.

Diese Benachrichtigung, die Höhe des Schadensausmaßes und das Risiko sind in die Prognoseentscheidung des Verantwortlichen einzubeziehen. Für deren Richtigkeit trägt er die Verantwortung. Zu berücksichtigen sind dabei alle Folgen für die Persönlichkeitsentfaltung des Betroffenen sowie drohende physische, materielle und immaterielle Schäden. Die Überlegungen bedürfen einer jeweiligen Betrachtung der konkreten Umstände des Einzelfalls.

Unter bestimmten Voraussetzungen, die im Ergebnis die Vermeidung oder Verhinderung von Folgeschäden garantieren, kann von einer Benachrichtigung der Betroffenen abgesehen werden. Dies ist unter den in Art. 34 Abs. 3 DSGVO vorgesehenen Umständen der Fall, wenn

- der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese auf die von der Verletzung betroffenen Daten angewandt hat, insbesondere solche, die die Verfügbarkeit für unberechtigte Personen verhindern (etwa Verschlüsselung);

- der Verantwortliche sichergestellt hat, dass das hohe Risiko nach Art. 34 Abs. 1 DSGVO nicht mehr besteht;
- oder der Aufwand einer Benachrichtigung unverhältnismäßig wäre. In diesem Fall ist ersatzweise durch eine öffentliche Bekanntmachung oder ähnliche Maßnahme sicherzustellen, dass die Betroffenen informiert werden.

Die Benachrichtigung soll in klarer und einfacher Sprache erfolgen, die mindestens die Informationen aus Art. 33 Abs. 3 lit. b), c) und d) DSGVO enthalten sollte. Sie hat unverzüglich nach Kenntnis von der Datenschutzverletzung zu erfolgen.

1.5.3 Dokumentationspflichten im Zusammenhang mit Art. 33 und 34 DSGVO

Den Verantwortlichen trifft u. a. nach Art. 33 Abs. 5 DSGVO eine umfangreiche Dokumentationspflicht hinsichtlich der Datenschutzverletzung einschließlich der Auswirkungen, Abhilfemaßnahmen und aller Umstände, die mit dem Vorgang im Zusammenhang stehen. Sie soll der Aufsichtsbehörde die Überprüfung der Bestimmungen der DSGVO ermöglichen und dürfte daher in der Regel umfassender als der Mindestinhalt der Meldepflicht sein.

1.5.4 Empfehlung der zur Sicherstellung der Meldepflichten erforderlichen organisatorischen Maßnahmen des Verantwortlichen nach Art. 33 und 34 DSGVO

Auch unter Berücksichtigung der Erwägungsgründe zur DSGVO (vgl. insbes. EG 87) sollte der Verantwortliche Strukturen schaffen, mit denen er im Falle einer Datenschutzverletzung den Verpflichtungen der DSGVO aus Art. 33 und Art. 34 nachkommen kann.

Dies setzt neben einer Sensibilisierung der Beschäftigten Folgendes voraus:

- Festlegung von internen Verantwortlichkeiten (wer bewertet wann, was?) und Ansprechpartnern (intern sowie gegenüber der Aufsichtsbehörde und ggf. den Betroffenen);

- Festlegung von internen Meldeverfahren und Kommunikationswegen (wann ist wer, auf welchem Weg einzubinden?);

→ Etablierung eines Systems zur Feststellung von Datenschutzverletzungen (z. B. betreffend IT-Verfahren, in denen Datenschutzverletzungen nicht unmittelbar für jeden Anwender erkennbar sind oder diese im Zusammenhang mit dem Umgang mit personenbezogenen Daten trotz Sensibilisierung nicht erkannt werden);

- Festlegungen zur Dokumentation des Vorfalls sowie der getroffenen Maßnahmen;

→ Sicherstellung geeigneter Dokumentationen der Auftragsverarbeiter.

1.6 Auftragsverarbeitung nach Art. 28 DSGVO

1.6.1 Einführung

Art. 28 DSGVO regelt die Anforderungen und Verpflichtungen des Verantwortlichen sowie des Auftragsverarbeiters. Der Auftragsverarbeiter ist neben dem Verantwortlichen eigenständiger Adressat der DSGVO.

Die Wartung von Datenverarbeitungsanlagen und Verfahren durch externe Dienstleister ist grundsätzlich dann als Auftragsverarbeitung anzusehen, wenn die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten besteht. Auch in diesen Fällen sind daher die in Art. 28 DSGVO vorgegebenen Anforderungen – wie etwa der Abschluss einer Vereinbarung – zu beachten. Lediglich bei der rein technischen Wartung der Infrastruktur einer IT durch Dienstleister (z. B. Arbeiten an der Stromzufuhr, Kühlung oder Heizung), aber auch bei Hilfstätigkeiten wie der Reinigung von Räumen mit Datenverarbeitungsanlagen, ist nicht von einer Auftragsverarbeitung auszugehen. Hier hat der Verantwortliche durch technische und organisatorische Maßnahmen vielmehr dafür Sorge zu tragen, dass ein Dienstleister keinen Zugriff auf personenbezogene Daten erhält.

Die Auftragsverarbeitung bietet den Vorteil, dass es innerhalb des Verarbeitungsverhältnisses für eine Weitergabe von Daten keiner eigenen Rechtsgrundlage, keines Erlaubnistatbestands bedarf. Vielmehr wird der Auftragsverarbeiter datenschutzrechtlich nicht als Dritter, sondern als der „verlängerte Arm“ und quasi interne Stelle des Verantwortlichen

ohne eigenen Wertungs- und Entscheidungsspielraum betrachtet. Der datenschutzrechtliche Erlaubnistatbestand, auf den sich der Verantwortliche beruft, gilt ebenso für den Auftragsverarbeiter.

Der Auftragsverarbeiter ist für die Einhaltung der technisch-organisatorischen Maßnahmen (mit-)verantwortlich und muss hinreichend Garantien dafür vorsehen, dass die von ihm getroffenen technischen und organisatorischen Maßnahmen einen wirksamen Schutz der Daten bieten. Dies setzt genügend Fachwissen, Zuverlässigkeit und Ressourcen auf seiner Seite voraus.

Die Garantien können durch genehmigte Verhaltensregeln des Auftragsverarbeiters nach Art. 40 DSGVO oder Zertifizierungen nach Art. 42 DSGVO nachgewiesen werden. Liegen diese vor, führt dies jedoch noch nicht zwingend zum Nachweis der Einhaltung der Garantien der DSGVO, es stellt jedoch einen „Faktor“ für die Beurteilung dar.

Mit Blick auf die in Art. 28 Abs. 3 DSGVO enthaltene Formvorgabe ist zu beachten, dass hier nicht allein vom deutschen Rechtsverständnis ausgegangen und die geforderte „Schriftlichkeit“ mit einem strengen Schriftformerfordernis des § 126 BGB bzw. der qualifizierten elektronischen Form gemäß § 126a BGB gleichgesetzt werden kann. Vielmehr wird bereits im Gesetzestext auf die Möglichkeit der elektronischen Form (z. B. per E-Mail bzw. online) hingewiesen sowie auf die Möglichkeit, die Auftragsverarbeitung auf Grundlage eines anderen Rechtsinstrumentes durchzuführen. Daraus ist zu schließen, dass hier die Textform im Sinne von § 126b BGB als ausreichend zu erachten ist.

Ein weiteres Formerfordernis wird in Bezug auf die Genehmigung durch den Verantwortlichen von weiteren Auftragsverarbeitern, also Unterauftragsverarbeitern, aufgestellt: Art. 28 Abs. 2 S. 1 und 2 DSGVO nennen dabei die elektronische Form nicht als Alternative, ohne dass ersichtlich wäre, weshalb die Einbindung weiterer Auftragsverarbeiter strengeren Anforderungen unterliegen sollte als die ursprüngliche Beauftragung. Auch hier ist daher die Textform als ausreichend anzusehen.

Im Übrigen bedarf die Einschaltung von Unterauftragsverarbeitern gemäß Art. 28 Abs. 2 DSGVO der vorherigen Genehmigung durch den Verantwortlichen. Diese kann entweder jeweils einzeln oder allgemein – etwa in der Vereinbarung zwischen Verantwortlichem und Auftrags-

verarbeiter – erteilt werden. Die Genehmigung darf sich nicht pauschal auf die Beauftragung weiterer Auftragsverarbeiter beschränken, sondern diese müssen ausdrücklich bekannt sein. Der Auftragsverarbeiter muss den Verantwortlichen sowohl bei einer Einzelgenehmigung als auch bei einer allgemeinen Genehmigung über jede Ersetzung oder Hinzuziehung von Unterauftragsverarbeitern informieren, wogegen der Verantwortliche ein Einspruchsrecht hat. Ein Einspruch des Verantwortlichen muss datenschutzrechtlich relevant sein und substantiiert begründet werden. Er ist insbesondere dann zulässig, wenn

- die Rechtsposition des Verantwortlichen nach dem Vertrag durch die Änderung verschlechtert wird,
- der Verantwortliche begründeten Anlass zu Bedenken hinsichtlich der Einhaltung der gesetzlichen Pflichten des Datenschutzes und/oder der Informationssicherheit durch den jeweiligen Unterauftragsverarbeiter hat oder
- tatsächliche Anhaltspunkte für ein nicht rechtskonformes Verhalten des Unterauftragsverarbeiters vorliegen, das geeignet ist, das Vertrauen in seine generelle Zuverlässigkeit zu erschüttern.

Nach einem Einspruch müssen Verantwortlicher und Auftragsverarbeiter das weitere Vorgehen klären. Bis zu einer Klärung darf der Unterauftragsverarbeiter nicht eingesetzt werden.

1.6.2 Bestandsaufnahme, Prüfung bestehender Verträge hinsichtlich Konformität mit DSGVO

In Deutschland – insbesondere im Bereich der Bundesverwaltung – dürften für alle Auftragsverarbeitungen schriftliche Verträge mit den jeweiligen Auftragnehmern vorliegen. Hieraus ergibt sich für die Praxis die Frage, ob bestehende Verträge der Auftragsverarbeitung, die vor dem Geltungsbeginn der DSGVO, d. h. unter der Geltung des BDSG (alt), abgeschlossen worden waren, auch nach dem seit 25. Mai 2018 geltenden Datenschutzrecht verwendet werden dürfen und insofern Bestand haben. Eine pauschale Betrachtung gibt es hierzu nicht. Vielmehr war/ist es erforderlich, jeden bestehenden Vertrag auf DSGVO-Konformität zu prüfen. Hierbei sind insbesondere die Umsetzung der sicherheitstechnischen Anforderungen der DSGVO,

- die Umsetzung der organisatorischen Anforderungen der DSGVO,

- die vorhandenen Regelungen zur Vertraulichkeit oder gesetzlichen Verschwiegenheit,
- die Bestimmungen bzgl. Unterauftragsverhältnissen,
- die Informationspflichten:
  - die Hinweispflicht des Auftragverarbeiters bei rechtswidrigen Weisungen durch den Auftraggeber/Verantwortlichen,
  - die Hinweispflicht des Auftragverarbeiters bzgl. Übermittlung in ein Drittland,
- die Dokumentationspflichten des Auftragverarbeiters:
  - die Dokumentation bzgl. des Verzeichnisses von Verarbeitungstätigkeiten,
  - die Dokumentationspflicht hinsichtlich der Weisungen,
- die Unterstützungspflichten des Auftragverarbeiters:
  - die Dokumentation bzgl. des Verzeichnisses von Verarbeitungstätigkeiten durch den Auftraggeber/Verantwortlichen,
  - bei der Zusammenarbeit mit den Aufsichtsbehörden,
  - bei der Meldung von Datenpannen,
  - bei der DSFA,
  - bei Prüfungen durch den Verantwortlichen oder dessen Beauftragten,
- der Umgang mit der Datenverarbeitung in einem Drittland, insbesondere der diesbezüglichen Weisungsabhängigkeit des Auftragverarbeiters,
- die Pflicht zur Rückgabe bzw. zur Löschung ggf. vom Auftragverarbeiter erhaltener personenbezogener Daten

zu prüfen.

Ferner müssen die Verträge bzgl. der Pflichten des Auftraggebers insbesondere hinsichtlich

- des dokumentierten Weisungsrechts des Verantwortlichen,

→ der Darlegung der grundsätzlichen Informationen, was in der Auftragsverarbeitung geschehen soll, das heißt hinsichtlich

- der Art und dem Zweck der Verarbeitung,
- der Art der personenbezogenen Daten und Kategorien von betroffenen Personen,
- der Beschreibung des Auftrags bzw. der Verarbeitung der personenbezogenen Daten durch den Auftragverarbeiter

überprüft werden.

1.6.3 Neuabschluss von Verträgen zur Auftragsverarbeitung nach Art. 28 DSGVO

Für den Abschluss neuer Verträge von Auftragsverarbeitungen sieht Art. 28 DSGVO neben einem individuellen Vertrag auch die Verwendung von Standardvertragsklauseln vor.

Die Standardvertragsklauseln, die einer europaweiten Vereinheitlichung der vertraglichen Regelungen dienen würden, müssen zuvor jedoch von der EU-Kommission bzw. von den Aufsichtsbehörden im Kohärenzverfahren festgelegt werden. Einzelne Mitgliedstaaten der EU haben zwischenzeitlich solche Standardvertragsklauseln geschaffen, Deutschland jedoch bislang nicht.

Daraus ergibt sich die Notwendigkeit, dass Verantwortliche und Auftragverarbeiter noch für längere Zeit individuell ausgehandelte, DS-GVO-konforme Verträge zur Auftragsverarbeitung abschließen müssen.

2 Datenschutzbeauftragte (DSB) nach Art. 37, 38 und 39 DSGVO

2.1 Regelungen der DSGVO für den DSB

2.1.1 Benennung/Rechtsstellung des DSB nach Art. 37 und 38 DSGVO

Alle öffentlichen Stellen des Bundes sind gemäß Art. 37 Abs. 1 lit. a) DSGVO unmittelbar verpflichtet, einen DSB zu benennen. Ausgenommen hiervon sind Gerichte und unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit. Um einen Gleichklang der Regelungen zu den DSB auch für solche öffentlichen Stellen des Bundes herzustellen, die nicht unter den Anwendungsbereich der DSGVO fallen, finden sich in den §§ 5 bis 7 BDSG Regelungen, die mit den Art. 37 bis 39 DSGVO weitgehend identisch sind.

Der DSB wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere seines Fachwissens sowohl auf dem Gebiet des Datenschutzrechts als auch auf dem Gebiet der Datenschutzpraxis benannt.

Gemäß Art. 37 Abs. 6 DSGVO/§ 5 Abs. 4 BDSG kann der DSB Beschäftigter der öffentlichen Stelle sein oder aufgrund eines Dienstleistungsvertrages benannt werden. Somit können auch Externe zum DSB benannt werden. Diese müssen nicht Beschäftigte öffentlicher Stellen, sondern können auch Private sein.

Die DSGVO und das BDSG sehen die Benennung nur eines DSB vor. Dafür sprechen in erster Linie die individuellen Schutzvorschriften (z. B. Benachteiligungsverbot, Abberufungsschutz, Weisungsfreiheit),

die auf eine Person zugeschnitten sind. Sofern der DSB seine Aufgaben nicht allein bewältigen kann, muss ihm der Verantwortliche weitere personelle Ressourcen zur Verfügung stellen, die dann als Mitarbeiter ausschließlich dem DSB unterstehen. Unabhängig davon sollte es einen Vertreter für den DSB geben.

Weder in der DSGVO noch im BDSG sind besondere Vorgaben enthalten, die die strukturelle Anbindung des DSB in der Aufbauorganisation der Behörde betreffen. In Art. 38 Abs. 3 S. 3 DSGVO und § 6 Abs. 3 S. 2 BDSG ist jedoch geregelt, dass der DSB in seiner Funktion als DSB weisungsfrei handelt und ein unmittelbares Vortragsrecht bei der höchsten Leitungsebene hat. Daher erweist es sich in der Praxis als sinnvoll, den DSB organisatorisch unmittelbar der Hausleitung zu unterstellen und dies auch im Organisationsplan und im Geschäftsverteilungsplan der Behörde zu spiegeln.

Der Verantwortliche (bzw. der Auftragsverarbeiter) muss gemäß Art. 38 Abs. 3 S. 1 DSGVO/§ 6 Abs. 3 S. 1 BDSG sicherstellen, dass der DSB bei der Erfüllung seiner Aufgaben keine Anweisungen erhält. Er muss also seiner Funktion unabhängig und ohne sachfremde Einflussnahme nachkommen können.

Der DSB darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden, siehe Art. 38 Abs. 3 S. 2/§ 6 Abs. 3 S. 3 BDSG. § 6 Abs. 4 S. 1 BDSG konkretisiert dies insoweit, als eine Abberufung nur aus wichtigem Grund in entsprechender Anwendung des § 626 BGB zulässig ist.

Es besteht ein strenger arbeitsrechtlicher Kündigungsschutz. Dieser ist als arbeitsrechtliche Vorschrift nicht in der DSGVO, wohl aber in § 6 Abs. 4 S. 2 und 3 BDSG geregelt. Danach ist eine Kündigung des Arbeitsverhältnisses des DSB nur zulässig, wenn Tatsachen vorliegen, die zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Zudem besteht nach dem Ende der Tätigkeit als DSB ein Jahr Kündigungsschutz, soweit nicht die o. g. Ausnahme vorliegt.

Gemäß Art. 38 Abs. 2 DSGVO/§ 6 Abs. 2 BDSG stellt die verantwortliche Stelle dem DSB die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung. Dies bedeutet, dass dem DSB auch die not-

wendigen Fortbildungen auf Kosten der öffentlichen Stelle des Bundes zu ermöglichen sind.

Der DSB ist an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden. Die Verschwiegenheitspflicht des DSB bezieht sich nach § 6 Abs. 5 S. 2 BDSG auf die Identität der betroffenen Personen sowie auf Umstände, die Rückschlüsse auf die betroffenen Personen zulassen. Diese Pflicht bezieht sich selbstverständlich – und vor allem – auf die Verschwiegenheit gegenüber dem Verantwortlichen.

Wenn der DSB Kenntnis von Daten erhält, für die der Leitung der öffentlichen Stelle aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht gemäß § 6 Abs. 6 BDSG auch dem DSB und den ihm unterstellten Beschäftigten zu. Die Vorschrift enthält darüber hinaus ein Beschlagnahmeverbot für die Akten und andere Dokumente des DSB.

Die öffentliche Stelle stellt dem DSB die für die Erfüllung seiner Aufgaben erforderlichen Ressourcen zur Verfügung, Art. 38 Abs. 2 DSGVO/§ 6 Abs. 2 BDSG. Mit Blick auf die hohe Arbeitsbelastung des DSB infolge der ihm durch die DSGVO bzw. das BDSG übertragenen Aufgaben (Überwachung der DSFA, Angemessenheitsprüfung mit Berücksichtigung von Art, Umfang, Umständen und Zweck der Verarbeitung, Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für diese) empfiehlt der BfDI die vollständige Freistellung des DSB von anderen Aufgaben für die Wahrnehmung seiner Funktion als DSB ab einer Anzahl von 500 Beschäftigten.

Die öffentliche Stelle gewährt dem DSB gemäß Art. 38 Abs. 2 DSGVO/§ 6 Abs. 2 BDSG den Zugang zu allen Dokumenten, die er für die Erfüllung seiner Aufgaben benötigt. Sie räumt ihm dafür entsprechende Zugriffsrechte ein.

Die DSGVO und das BDSG verlangen von der öffentlichen Stelle die ordnungsgemäße und frühzeitige Einbindung des DSB bei allen Fragen im Zusammenhang mit dem Schutz personenbezogener Daten, Art. 38 Abs. 1 DSGVO/§ 6 Abs. 1 BDSG. Hierzu muss die öffentliche Stelle sicherstellen, dass die für Datenschutzaufgaben fachlich zuständigen Organisationseinheiten (Fachreferate und die Organisationseinheit „administrativer Datenschutz“) den DSB unmittelbar bei allen datenschutzrelevanten Vorgängen ordnungsgemäß und frühzeitig beteiligen,

um ihm die Möglichkeit der Wahrnehmung seiner Beratungs- und Unterrichtungsaufgabe zu geben und mit Blick auf Überprüfungsaufgaben des DSB spätere Beanstandungen zu vermeiden. Die Pflicht zur frühzeitigen Einbindung des DSB verlangt eine Beteiligung bereits in den Phasen der Planung, Ausschreibung und Entwicklung von datenschutzrelevanten Systemen/Verarbeitungen. Es bietet sich an, die Einbindung des DSB standardmäßig in die entsprechenden Ablaufplanungen (Workflows) zwingend vorzusehen.

Die öffentliche Stelle des Bundes ist gemäß Art. 37 Abs. 7 DSGVO/§ 5 Abs. 5 BDSG verpflichtet, die Kontaktdaten des DSB zu veröffentlichen, diese in das Verzeichnis der Verarbeitungstätigkeiten aufzunehmen und dem BfDI mitzuteilen. Bei der Veröffentlichung der Kontaktdaten genügt es, wenn die telefonische und elektronische Erreichbarkeit in Form eines Funktionspostfaches bekanntgegeben wird. Eine Veröffentlichung des Namens des DSB ist nicht notwendig. Die Meldung an den BfDI hingegen umfasst auch den Namen. Der BfDI stellt für diese Meldung ein Formular zur Verfügung, zu finden unter www.bfdi.bund.de/kontakt.

Dem DSB können andere Aufgaben und Pflichten übertragen werden. Dabei ist sicherzustellen, dass dies nicht zu einem Interessenkonflikt führt, Art. 38 Abs. 6 DSGVO/§ 7 Abs. 2 BDSG. Ein Interessenkonflikt ist z. B. bei der Übernahme von Aufgaben des administrativen Datenschutzes durch den DSB gegeben, da der DSB dadurch in die Situation geraten könnte, dass er von ihm fachlich getroffene Maßnahmen selbst kontrollieren müsste, was mit seinem gesetzlichen Auftrag unvereinbar wäre. Ein Konflikt kann aber auch dann gegeben sein, wenn die Übertragung weiterer Aufgaben dazu führt, dass der DSB gleichzeitig in mehreren Referaten eingesetzt wird oder er in einem Umfang mit anderen Aufgaben so belastet wird, dass er seine Funktion als DSB nicht mehr nach den eigenen Prioritäten ausüben kann. Andere – auch dringliche – Aufgaben müssen jedoch zurückstehen, denn die Ausübung seiner Funktion als DSB hat Priorität. Die Leitung einer öffentlichen Stelle des Bundes hat bei der Übertragung anderer Aufgaben daher von vornherein darauf achten, dass ein Interessenkonflikt ausgeschlossen ist.

2.1.2 Aufgaben des DSB nach Art. 39 DSGVO

Der DSB hat die Organisationseinheiten der öffentlichen Stelle und die Beschäftigten im Hinblick auf ihre datenschutzrechtlichen Pflichten zu unterrichten und zu beraten, siehe Art. 39 Abs. 1 lit. a) DSGVO/§ 7 Abs. 1 Nr. 1 BDSG. Diese Aufgabe schließt das Recht ein, Maßnahmen zur Einhaltung bzw. Umsetzung der Datenschutzvorschriften vorzuschlagen. Die Pflicht des DSB zur Unterrichtung und Beratung umfasst auch die Sensibilisierung aller Beteiligten. Er hat jedoch keine rechtliche Verpflichtung, Schulungen und Fortbildungen der Beschäftigten selbst durchzuführen. Diese Verpflichtung besteht nur für die öffentliche Stelle, Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO. Der DSB ist hingegen verpflichtet, die Schulungen zu überwachen. Nach eigenem Ermessen kann er Schulungen und Fortbildungen der Beschäftigten im Rahmen seiner Beratungsaufgabe aber auch selbst durchführen.

Eine der wichtigsten Aufgaben des DSB ist somit die Überwachung und Einhaltung der datenschutzrechtlichen Vorschriften gemäß Art. 39 Abs. 1 lit. b) DSGVO/§ 7 Abs. 1 Nr. 2 BDSG. Bei der dem DSB obliegenden Überwachungsaufgabe handelt es sich um eine Compliance-Aufgabe. Gegenstand der Kontrolle ist nicht nur die Einhaltung des Datenschutzrechts, sondern auch die Einhaltung der Strategien und Regeln (einschließlich der Zuständigkeitsverteilung), die sich die verantwortliche Stelle im Bereich Datenschutz selbst gegeben hat. Der DSB ist hingegen nicht für die Einhaltung der datenschutzrechtlichen Vorschriften im rechtlichen Sinne verantwortlich. Diese Verantwortung verbleibt bei der öffentlichen Stelle, also dem Verantwortlichen. Zu den zulässigen Kontrollverfahren der verantwortlichen Stelle kann der DSB beratend hinzugezogen werden.

Die öffentliche Stelle muss dafür sorgen, dass der DSB bei DSFA zu Rate gezogen wird. Der DSB hat die DSFA nach Art. 39 Abs. 1 lit. c) DSGVO/§ 7 Abs. 1 Nr. 3 BDSG zu überwachen.

Betroffene Personen können den DSB bei allen mit der Verarbeitung ihrer Daten bestehenden Fragen sowie bei der Ausübung ihrer Betroffenenrechte zu Rate ziehen (Ansprechpartnerfunktion des DSB), Art. 38 Abs. 4 DSGVO/§ 6 Abs. 5 BDSG.

Auch für die Tätigkeit des DSB gilt der so genannte risikobasierte Ansatz. Der DSB führt im Rahmen seiner Einbindung eine Angemessenheitsprüfung durch, um dem mit der jeweiligen Verarbeitung verbundenen Risiko Rechnung zu tragen. Er berücksichtigt dabei die Art, den Umfang, die Umstände und den Zweck der Verarbeitung.

2.2 Zusammenarbeit des DSB mit dem BfDI/ Anlaufstelle für den BfDI nach Art. 39 Abs. 1 lit. d) DSGVO

Nach Art. 39 Abs. 1 lit. d) DSGVO/§ 7 Abs. 1 Nr. 4 BDSG obliegt dem DSB die Aufgabe der umfassenden Kooperation mit der Aufsichtsbehörde. Hierdurch hat er die Befugnis zum Außenkontakt mit der Aufsichtsbehörde. Aufgrund der Funktion des DSB als Anlaufstelle ist der BfDI nicht gehalten, sich für Fragen im Zusammenhang mit Verarbeitungsvorgängen sowie im Verfahren der vorherigen Konsultation nach Art. 36 DSGVO zwingend zuerst an die verantwortliche Stelle zu wenden. Der BfDI kann sich vielmehr unmittelbar mit dem DSB in Verbindung setzen. Soweit sich der BfDI unmittelbar mit der öffentlichen Stelle in Verbindung setzt, unterrichtet der BfDI den DSB in der Regel nachrichtlich. Darüber hinaus kann sich der DSB mit dem BfDI bei allen Fragen im Zusammenhang mit der Umsetzung des Datenschutzes in der verantwortlichen Stelle beraten.

Die Aufgabe des DSB, dem BfDI als Ansprechpartner zur Verfügung zu stehen, enthebt den Verantwortlichen allerdings nicht von seinen Verpflichtungen, mit dem BfDI zu kooperieren und zusammenzuarbeiten, vgl. Art. 31 DSGVO. So ist z. B. für die Durchführung der Meldungen von Datenschutzverletzungen nach Art. 33 Abs. 1 DSGVO der Verantwortliche zuständig; dies gehört nicht zu den Aufgaben des DSB, sondern ist Teilaufgabe des administrativen Datenschutzes, der durch den Verantwortlichen ausgeübt wird.

2.3 Verantwortlichkeitsverteilung DSB – Verantwortlicher nach Art. 5 Abs. 2, Art. 24 und Art. 39 Abs. 1 lit. a) DSGVO

Adressat der Pflichten aus der DSGVO bzw. dem BDSG ist der Verantwortliche, also die öffentliche Stelle des Bundes, nicht der DSB. Die öffentliche Stelle muss nachweisen, dass sie die personenbezogenen Daten rechtmäßig verarbeitet hat und ihren datenschutzrechtlichen Pflichten nachgekommen ist. Hierzu sind die zur Einhaltung des Datenschutzes getroffenen technischen und organisatorischen Maßnahmen zu dokumentieren. Die Maßnahmen sind regelmäßig zu überprüfen und ggf. zu aktualisieren.

Aufgabe des DSB ist es, den Verantwortlichen und dessen Beschäftigte hinsichtlich seiner datenschutzrechtlichen Pflichten zu beraten bzw. zu unterrichten sowie die Einhaltung der Pflichten zu überwachen. Ggf. muss er im Rahmen dieser Aufgaben auf die Verletzung des Datenschutzrechts sowie auf die Anforderungen an eine rechtmäßige Datenverarbeitung hinweisen. Beschäftigte und Organisationseinheiten müssen sich bei allen Fragen im Zusammenhang mit der Verarbeitung personenbezogener Daten unmittelbar an den DSB wenden können.

Die Wahrnehmung der Datenschutzbelange ist durch die öffentliche Stelle aufbauorganisatorisch bei der jeweiligen Fachaufgabe anzusiedeln. Datenschutzaufgaben sollten als Auffangzuständigkeit (administrativer Datenschutz bzw. Fachaufgabe Datenschutz) bei einer Organisationseinheit angesiedelt werden. Der DSB ist von allen Organisationseinheiten, die datenschutzrelevante Vorgänge bearbeiten, sowie von der für die Fachaufgabe Datenschutz zuständige Organisationseinheit ordnungsgemäß und frühzeitig zu beteiligen.

3 Rechtsgrundlagen

3.1 Systematik des Datenschutzrechts

3.1.1 Vorrang der DSGVO

Hinsichtlich der Systematik der Rechtsgrundlagen haben die öffentlichen Stellen im Anwendungsbereich der DSGVO einen gesetzlichen Dreiklang zu beachten. Die DSGVO selbst ist als europäische Verordnung unmittelbar in den Mitgliedstaaten geltendes Recht. Damit kommt ihr ein Anwendungsvorrang vor jedem mitgliedstaatlichen Recht zu. Den nationalen Gesetzgebern ist es verwehrt, abweichende Vorschriften zu erlassen oder auch nur die Vorschriften aus der Verordnung zu wiederholen, sofern dies nach EG 8 der DSGVO zur besseren Verständlichkeit der Regelungen nicht ausnahmsweise zugelassen ist. Ist also die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu beurteilen, muss der erste Blick immer in die DSGVO selbst gehen, deren Regelungen unmittelbar anzuwenden sind.

Das BDSG ist in doppelter Hinsicht nachrangiges Recht. Im Verhältnis zur DSGVO gelten seine Regelungen nur dann, soweit die DSGVO nicht unmittelbar gilt (§ 1 Abs. 5 BDSG). Darüber hinaus gilt das BDSG auch dann nicht, wenn es andere – speziellere – Rechtsvorschriften des Bundes über den Datenschutz gibt. Diese anderen – bereichsspezifischen – Datenschutzvorschriften gehen den Vorschriften des BDSG vor. Nur wenn sich dort keine oder keine abschließende Regelung findet, kommen die Vorschriften des BDSG zur Anwendung (§ 1 Abs. 2 BDSG). Im Anwendungsbereich der DSGVO gelten insoweit die Teile 1 und 2 des BDSG.

Wegen des Anwendungsvorrangs der DSGVO enthält das BDSG im Anwendungsbereich der DSGVO nur solche Regelungen, bei denen die DSGVO selbst den Erlass mitgliedstaatlichen Rechts erlaubt. Die DSGVO enthält dabei sowohl Regelungsaufträge, die zwingend zu erfüllen sind, als auch Regelungsoptionen, von denen der Mitgliedstaat Gebrauch machen kann oder auch nicht. Zu ersteren gehören insbesondere die Vorschriften über den BfDI (§§ 8 bis 16 BDSG) und zur Zusammenarbeit der Aufsichtsbehörden in Bund und Ländern (§§ 17 bis 19 BDSG). Zu letzteren gehört vor allem der überwiegende Teil der §§ 22 ff. BDSG.

Einen weiten Regelungsspielraum gemäß Art. 6 Abs. 2 und 3 DSGVO haben die Mitgliedstaaten vor allem bei der Verarbeitung personenbezogener Daten im öffentlichen Bereich. Hier ist es den Mitgliedstaaten möglich, die Rechtsgrundlagen für die Verarbeitung zu konkretisieren. Dem trägt das bereichsspezifische materielle Datenschutzrecht Rechnung.

Zusammenfassend lässt sich festhalten, dass die Rechtmäßigkeit der Verarbeitung personenbezogener Daten wegen ihres Anwendungsvorrangs zuerst nach der DSGVO zu beurteilen ist. Lässt die DSGVO einen Regelungsspielraum, ist in einem weiteren Schritt zu prüfen, ob es bereichsspezifisches Datenschutzrecht gibt, z. B. im SGB X, in der Abgabenordnung (AO) oder im Bundesbeamtengesetz (BBG). Ist dies nicht der Fall oder sind die bereichsspezifischen Vorschriften nicht abschließend, gilt ergänzend das BDSG. Als Auffangrechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes steht § 3 BDSG zur Verfügung.

3.1.2 Anwendungsbereich der JI-Richtlinie

Im Anwendungsbereich der JI-Richtlinie 2016/680 stellt sich die Situation anders dar. Unter diesen fallen alle öffentlichen Stellen des Bundes, die personenbezogene Daten für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten verarbeiten. Die Verhütung von Straftaten schließt in diesem Kontext auch die Gefahrenabwehr ein. Außerdem fallen die für die Vollstreckung von Strafen oder anderer strafrechtlicher Maßnahmen zuständigen Stellen unter den Anwendungsbereich der JI-Richtlinie. Erfasst sind beispielsweise das Bundeskriminalamt, die Bundespolizei,

der Generalbundesanwalt, das Zollkriminalamt oder die Tätigkeiten anderer öffentlicher Stellen als Verwaltungsbehörde im Sinne des Ordnungswidrigkeitenrechts. Da die Richtlinie nicht unmittelbar geltendes Recht ist, musste sie in nationales Recht umgesetzt werden. Dies ist durch die Teile 1 und 3 des BDSG geschehen. Selbstverständlich gilt auch hier, dass bereichsspezifisches Datenschutzrecht vorgeht, z. B. die datenschutzrechtlichen Vorschriften des BKAG oder des BPolG.

3.1.3 Öffentliche Stellen außerhalb des Anwendungsbereichs des EU-Rechts nach § 1 Abs. 8 BDSG

Für die öffentlichen Stellen, die nicht unter das Unionsrecht fallen, gilt nach wie vor ausschließlich nationales Datenschutzrecht. Dies betrifft vor allem die Nachrichtendienste des Bundes oder den Bereich der Verteidigung. Sofern kein vorrangiges bereichsspezifisches Datenschutzrecht besteht (z. B. BVerfSchG, BNDG, MADG oder G10), gelten die Vorschriften der Teile 1 und 4 des BDSG. Außerdem gelten gemäß § 1 Abs. 8 BDSG die Vorschriften der DSGVO und des Teils 2 des BDSG entsprechend, sofern keine abweichenden Regelungen getroffen werden.

3.2 Zulässigkeit der Datenverarbeitung nach der DSGVO

3.2.1 Allgemeines

Die zentrale Vorschrift für die Zulässigkeit der Verarbeitung personenbezogener Daten findet sich in Art. 6 DSGVO. Sie enthält in Abs. 1 S. 1 lit. a) bis f) sechs verschiedene Tatbestände, bei deren Vorliegen eine Verarbeitung personenbezogener Daten erlaubt ist. Auch wenn die sechs Tatbestände grundsätzlich gleichrangig nebeneinander stehen, kommt nicht jeder von ihnen für die Datenverarbeitung durch öffentliche Stellen in gleicher Weise als Rechtsgrundlage in Betracht.

3.2.2 Die einzelnen Zulässigkeitstatbestände der DSGVO nach Art. 6 DSGVO

Für die Verarbeitung personenbezogener Daten durch öffentliche Stellen kommen in erster Linie Art. 6 Abs. 1 S. 1 lit. c) und e) DSGVO als Rechtsgrundlage in Frage. Art. 6 Abs. 1 S. 1 lit. c) DSGVO erlaubt die

Verarbeitung dann, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Eine solche rechtliche Verpflichtung kann sich aus Vorschriften des Unionsrechts oder des nationalen Rechts ergeben. Hierunter fallen beispielsweise Meldepflichten oder auch die Verpflichtung zur Herausgabe personenbezogener Daten nach dem IFG. Art. 6 Abs. 1 S. 1 lit. c) DSGVO ist nicht auf öffentliche Stellen beschränkt, erfasst diese aber.

Noch stärker auf die Verarbeitung personenbezogener Daten durch öffentliche Stellen zugeschnitten ist Art. 6 Abs. 1 S. 1 lit. e) DSGVO. Danach dürfen personenbezogene Daten dann verarbeitet werden, wenn dies zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt. Art. 6 Abs. 1 S. 1 lit. e) DSGVO verankert insbesondere das aus dem Verhältnismäßigkeitsgrundsatz folgende Erforderlichkeitsprinzip.

Ergänzend regelt Art. 6 Abs. 3 DSGVO, dass sich in den Fällen der lit. c) und e) des Art. 6 Abs. 1 S. 1 DSGVO die Rechtsgrundlage für die Verarbeitung entweder aus dem Unionsrecht oder dem mitgliedstaatlichen Recht ergeben muss. Im Unionsrecht können sich die Rechtsgrundlagen insbesondere aus EU-Verordnungen ergeben, da sie unmittelbar anwendbar sind. Ein Beispiel ist etwa die Veröffentlichung der Empfänger von Agrarsubventionen auf der Grundlage der entsprechenden EU-Verordnungen. Im mitgliedstaatlichen Recht hat der Gesetzgeber auf Bundesebene mit Blick auf Art. 6 Abs. 3 DSGVO dafür Sorge getragen, dass lückenlose Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes geschaffen worden sind, sodass ein unmittelbarer Rückgriff auf Art. 6 Abs. 1 S. 1 lit. c) und e) nicht notwendig ist. Die Rechtsgrundlage für eine Verarbeitung personenbezogener Daten ergibt sich aus dem bereichsspezifischen Datenschutzrecht und subsidiär aus § 3 BDSG.

Für die Verarbeitung personenbezogener Daten durch öffentliche Stellen kommt die Einwilligung des Betroffenen gemäß Art. 6 Abs. 1 S. 1 lit. a) DSGVO in Betracht. Dieses Instrument ist im öffentlichen Bereich allerdings mit großer Zurückhaltung anzuwenden, denn eine Einwilligung ist nur wirksam, wenn sie freiwillig erteilt worden ist, siehe Art. 4 Nr. 11 DSGVO. Freiwilligkeit ist dann nicht gegeben, wenn zwischen dem Verantwortlichen und der betroffenen Person ein klares Ungleichgewicht besteht. Behörden treten gegenüber den betroffenen Personen

in der Regel als Hoheitsträger auf, Staat und Bürger befinden sich in einem Über-/Unterordnungsverhältnis. Daher besteht in der Regel ein klares Ungleichgewicht zwischen dem Verantwortlichen und der betroffenen Person, sodass gemäß EG 43 eine Einwilligung gegenüber Behörden in der Regel als Rechtsgrundlage ausscheidet.

Eine Einwilligung kann ggf. als Rechtsgrundlage dienen, wenn die Verarbeitung personenbezogener Daten im konkreten Fall grundsätzlich im Zusammenhang mit den Aufgaben der Behörde steht und den betroffenen Personen keinerlei Nachteile bei einer Verweigerung der Einwilligung entstehen. Beispielsweise kann die Speicherung personenbezogener Daten für die Zusendung von Informationen über Newsletter auf eine Einwilligung gestützt werden, wenn die gleichen Informationen, z. B. auch über die Homepage zugänglich sind. Hier kann die betroffene Person frei entscheiden, ob sie ein solches Angebot einer Behörde nutzen möchte oder nicht, ohne dass Nachteile zu befürchten wären.

Wird die Verarbeitung auf eine Einwilligung gestützt, ist u. a. zu beachten, dass deren Erteilung gemäß Art. 7 Abs. 1 DSGVO nachgewiesen werden muss und die betroffene Person auf die Möglichkeit des Widerrufs der Einwilligung hinzuweisen ist.

Darüber hinaus ist nach Art. 6 Abs. 1 S. 1 lit. d) DSGVO eine Verarbeitung personenbezogener Daten immer auch dann erlaubt, wenn sie zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich ist. Bei dieser Rechtsgrundlage handelt es sich um eine Ausnahme, die nur dann greift, wenn es in konkreten Einzelfällen um den Schutz höchstpersönlicher Rechtsgüter, wie Leben oder körperliche Unversehrtheit, geht und eine andere Rechtsgrundlage (z. B. die Einwilligung oder eine Erforderlichkeit i. S. v. Art. 6 Abs. 1 S. 1 lit. c) oder e) DSGVO) nicht in Betracht kommt.

Außerdem kann die Verarbeitung personenbezogener Daten auch im öffentlichen Bereich auf Art. 6 Abs. 1 S. 1 lit. b) DSGVO gestützt werden. Diese Vorschrift erlaubt die Verarbeitung dann, wenn sie zur Erfüllung eines Vertrages mit der betroffenen Person oder zur Erfüllung vorvertraglicher Pflichten erforderlich ist. Üblicherweise handelt die öffentliche Verwaltung gegenüber den Bürgerinnen und Bürgern nicht in der Form von Verträgen, sondern in verschiedenen Formen hoheitlichen Handelns, sodass Art. 6 Abs. 1 S. 1 lit. b) DSGVO für diese

Fälle nicht als Rechtsgrundlage in Betracht kommt. Im Bereich des fiskalischen Handelns der Verwaltung kann die Verarbeitung personenbezogener Daten jedoch durchaus auf diese Vorschrift gestützt werden.

Art. 6 Abs. 1 S. 1 lit. f) DSGVO kommt als Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen hingegen grundsätzlich nicht in Betracht. Dessen Anwendung wird durch Art. 6 Abs. 1 S. 2 DSGVO für Behörden in Erfüllung ihrer Aufgaben explizit ausgeschlossen. Daher können sich Behörden und öffentliche Stellen bei ihrer Datenverarbeitung nicht auf überwiegende berechtigte Interessen berufen, denn letztlich dient jede Verarbeitung personenbezogener Daten der Erfüllung ihrer Aufgaben.

3.3 Beschäftigtendatenschutz

3.3.1 Beschäftigtendatenschutz gemäß Art. 88 DSGVO und § 26 BDSG

Art. 88 Abs. 1 DSGVO enthält eine Öffnungsklausel für die Datenverarbeitung im Beschäftigungskontext, die es den Mitgliedstaaten erlaubt, durch Rechtsvorschriften oder Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung von personenbezogenen Beschäftigtendaten vorzusehen. Gemäß Art. 88 Abs. 2 DSGVO müssen alle nationalen Vorschriften so ausgestaltet sein, dass die Grundrechte und Interessen der Betroffenen hinreichend geschützt sind. Dem Wortlaut von Art. 88 Abs. 1 DSGVO ist zudem eindeutig zu entnehmen, dass der nationale Gesetzgeber lediglich „spezifischere Vorschriften“ erlassen kann. Eine Abweichung vom Schutzstandard der DSGVO ist damit nicht möglich. Die nationalen Rechtsvorschriften müssen die Würde des Menschen sowie die berechtigten Interessen und die Grundrechte der betroffenen Person wahren.

Der nationale Gesetzgeber hat von der Regelungsoption des Art. 88 Abs. 1 DSGVO Gebrauch gemacht und mit § 26 BDSG eine nationale Regelung für den Beschäftigtendatenschutz geschaffen. Soweit § 26 BDSG keine spezifischeren Vorschriften zur Verarbeitung von Beschäftigtendaten enthält, sind die Vorschriften der DSGVO anzuwenden.

3.3.2 Übersicht über den Regelungsinhalt von § 26 BDSG

§ 26 Abs. 1 BDSG enthält die Rechtsgrundlage für die Verarbeitung personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses (S. 1) sowie zur Aufdeckung von Straftaten (S. 2).

Welche Personengruppen vom Begriff des „Beschäftigten" erfasst sind, gibt § 26 Abs. 8 BDSG vor mit der Klarstellung, dass der Leiharbeitnehmer im Verhältnis zum Entleiher als Beschäftigter i. S. d. § 26 BDSG einzuordnen ist.

§ 26 Abs. 2 BDSG enthält eine Regelung zur Einwilligung im Beschäftigungskontext und benennt insbesondere Fallgruppen, in denen die Freiwilligkeit der Einwilligung angenommen werden kann.

§ 26 Abs. 3 BDSG trifft eine Sonderregelung für die Verarbeitung besonderer Kategorien personenbezogener Daten i. S. v. Art. 9 DSGVO für Zwecke des Beschäftigungsverhältnisses.

Darüber hinaus verweist § 26 Abs. 4 BDSG auf die Regelungskompetenz der Kollektivparteien und nimmt Bezug auf die vom Verantwortlichen zu ergreifenden Maßnahmen zur Sicherstellung der in Art. 5 DSGVO dargelegten Grundsätze und stellt in § 26 Abs. 6 BDSG klar, dass Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt bleiben.

§ 26 Abs. 7 BDSG gilt auch dann, wenn personenbezogene Daten nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

3.3.3 Spezifische Regelungen für Beamte nach §§ 106 ff. BBG

Weitere „spezifische" Vorschriften i. S. d. Art. 88 DSGVO finden sich u. a. in §§ 106 ff. BBG, die personalaktenrechtliche Regelungen enthalten. Diese speziellen bundesgesetzlichen Datenschutzregelungen haben Vorrang vor den allgemeinen Datenschutzregelungen des BDSG.

4 Umsetzung der Betroffenenrechte

Die in Kapitel III der DSGVO garantierten Rechte der betroffenen Personen sind ein Kernbestandteil des Datenschutzrechts. Sie dienen der Transparenz und der praktischen Umsetzung der informationellen Selbstbestimmung der Bürgerinnen und Bürger. Die internen Prozesse und Verfahren müssen dem Rechnung tragen und so gestaltet werden, dass höchstmögliche Transparenz gewährleistet wird, die betroffenen Personen ihre Rechte umfassend und wirksam ausüben können und die öffentlichen Stellen die Anforderungen zugleich effizient und unbürokratisch umsetzen können.

4.1 Informationspflichten nach Art. 13 und 14 DSGVO

Der Verantwortliche muss geeignete Maßnahmen ergreifen, um der betroffenen Person alle Informationen nach Art. 13 und 14 DSGVO zur Verfügung zu stellen. Die betroffene Person muss die Möglichkeit haben, diese Informationen wahrzunehmen. Es wird zwischen Informationspflichten bei der Direkterhebung (siehe 4.1.1) und bei Dritterhebung (siehe 4.1.2) unterschieden.

4.1.1 Informationspflicht bei Direkterhebung nach Art. 13 DSGVO

Der Umfang der zu erteilenden Informationen nach Art. 13 DSGVO ist hoch:

- → Namen und Kontaktdaten des Verantwortlichen, also der öffentlichen Stelle,
  - Hier genügen in der Regel die Angaben aus der Anbieterkennzeichnung (Impressum).
- → Kontaktdaten des DSB,
  - Hier genügen die Angaben nach Art. 37 Abs. 7 DSGVO/§ 5 Abs. 5 BDSG (siehe 2.1.1).
- → Zwecke und Rechtsgrundlagen für die Verarbeitung personenbezogener Daten,
- → Empfänger oder Kategorien von Empfängern der personenbezogenen Daten,
  - Sofern konkrete Empfänger bekannt sind, besteht kein Wahlrecht, sondern diese sind zu nennen
- → falls Daten in Drittländer übermittelt werden, die geeigneten Garantien zum Schutz der Daten,
  - Hier sind in erster Linie die Instrumente aus Kapitel V der DSGVO zu nennen, auf denen die Übermittlung beruht.

Die Nennung der berechtigten Interessen des Verantwortlichen gemäß Art. 13 Abs. 1 lit. d) DSGVO, falls die Verarbeitung auf Art. 6 Abs. 1 lit. f) DSGVO beruht, dürfte für Behörden in aller Regel nicht relevant sein, da diese Rechtsgrundlage weitgehend ausscheidet.

Zusätzlich sind nach Art. 13 Abs. 2 DSGVO zur Gewährung einer fairen und transparenten Verarbeitung die folgenden Informationen zu erteilen:

- → Dauer der Speicherung; falls nicht möglich die Kriterien für die Festlegung dieser Dauer,
  - das Bestehen der Rechte betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Widerspruch aufgrund besonderer Situation einer betroffenen

Person, sofern die Verarbeitung auf Einwilligung beruht, das Recht zum jederzeitigen Widerruf,

→ Recht auf Beschwerde bei der Aufsichtsbehörde,

- Zwar muss die konkret zuständige Aufsichtsbehörde nicht genannt werden. Es wird den öffentlichen Stellen des Bundes aber empfohlen, konkret den BfDI und dessen Kontaktdaten zu nennen.

→ ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist,

- sofern einschlägig: die Vornahme einer automatisierten Entscheidungsfindung, einschließlich Profiling, sowie Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der Verarbeitung für die betroffene Person.

Die vorangegangenen, dargestellten Informationen müssen den betroffenen Personen zum Zeitpunkt der Erhebung zur Verfügung gestellt werden.

In den Fällen unverlangter Mitteilungen oder Zusendungen von personenbezogenen Daten hat grundsätzlich eine Information an die betroffenen Personen nach Art. 13 DSGVO zu erfolgen. Art. 13 DSGVO löst die Informationspflicht bereits durch den Vorgang der Datenerhebung aus. Nach Art. 5 Abs. 1 lit. b) DSGVO ist die Erhebung personenbezogener Daten mit der Festlegung der Verarbeitungszwecke verknüpft. Entscheidend ist aber, dass durch den Beginn der Verarbeitung von unverlangt zugesandten Daten, z. B. durch Bearbeitung einer Bürgeranfrage, ein Datenverarbeitungsprozess mit einer Speicherung der Daten durch den Verantwortlichen begonnen wird. Im Hinblick auf den Zweck der Informationspflicht, Datenverarbeitungsprozesse transparent zu gestalten, besteht daher eine grundsätzliche Verpflichtung, auch in derartigen Fällen den betroffenen Personen, die nach Art. 13 DSGVO mitzuteilenden Informationen zur Verfügung zu stellen.

Dabei kann (teilweise) auf die Information verzichtet werden, wenn die betroffene Person bereits über die Informationen verfügt (siehe

4.1.4). Medienbrüche sollten möglichst vermieden werden; möglich ist aber z. B. eine kurze Erstinformation per E-Mail mit einem Verweis auf weitere Erläuterungen auf einer Homepage.

4.1.2 Datenerhebung bei Dritten im Hinblick auf Art. 14 DSGVO

Art. 14 DSGVO unterscheidet auch bei Dritterhebung von personenbezogenen Daten zwischen mitzuteilenden Informationen (Abs. 1) und zusätzlichen Informationen, die zur Gewährung einer fairen und transparenten Verarbeitung zur Verfügung zu stellen sind (Abs. 2). Diese Informationen entsprechen im Wesentlichen den Informationen, die bei einer Direkterhebung der Daten mitzuteilen sind. Hinzu kommt die Mitteilung über die Kategorien personenbezogener Daten, die verarbeitet werden, da die betroffene Person im Gegensatz zur Direkterhebung keine Kenntnis darüber hat, welche Daten erhoben wurden. Zudem ist bei der Dritterhebung die Herkunft der personenbezogenen Daten mitzuteilen.

Die Informationen sind den betroffenen Personen innerhalb einer angemessenen Frist nach Erlangung der Daten, spätestens innerhalb eines Monats, mitzuteilen. Werden die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet, sind ihr diese Informationen spätestens zum Zeitpunkt der ersten Kontaktaufnahme mitzuteilen. Falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, sind die Informationen spätestens zum Zeitpunkt der ersten Offenlegung zur Verfügung zu stellen.

4.1.3 Informationen bei Zweckänderung nach Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO

Sowohl bei Direkterhebungen als auch bei Dritterhebungen sind die betroffenen Personen über Zweckänderungen nach Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO vorab zu informieren. Eine Zweckänderung kann z. B. mit einer Übermittlung der personenbezogenen Daten an Dritte verbunden sein.

4.1.4 Ausnahmen nach Art. 13 Abs. 4 und 14 Abs. 5 DSGVO sowie §§ 32 und 33 BDSG

Verfügt die betroffene Person bereits über die Informationen, so bestehen die Informationspflichten nach Art. 13 und 14 DSGVO nicht. Im

Falle einer Dritterhebung besteht die Informationspflicht auch dann nicht, wenn sich die Informationserteilung als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, die Erlangung der Daten durch Rechtsvorschrift ausdrücklich geregelt ist oder die Daten einem Berufsgeheimnis unterliegen. §§ 32 und 33 BDSG enthalten weitere Ausnahmen von den Informationspflichten.

4.1.5 Implementierung der Informationspflichten nach Art. 12 DSGVO

Die Informationen sind nach Art. 12 Abs. 1 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die Informationen können schriftlich auf dem Papierweg oder elektronisch übermittelt werden, z. B. durch Versenden einer standardisierten Eingangsbestätigung. Wird auf eine elektronisch verfügbare Information, z. B. auf der Internetseite der verantwortlichen Stelle, Bezug genommen, dann muss diese leicht auffindbar sein. Bei schriftlicher Korrespondenz auf dem Papierweg sollte eine Bezugnahme auf Informationen auf der Internetseite nur erfolgen, wenn davon ausgegangen werden kann, dass diese Informationen für die betroffene Person leicht zugänglich sind. Dies muss durch die öffentlichen Stellen des Bundes geprüft und entsprechend den konkreten Gegebenheiten festgelegt werden.

Bei der verantwortlichen Stelle ist ein Prozess einzuführen, der sicherstellt, dass den betroffenen Personen die Informationen in geeigneter Form zur Verfügung gestellt werden. Bei der Prozessgestaltung ist neben den Ablaufregelungen auch die Festlegung der Zuständigkeiten festzuschreiben. Die Erbringung der Information ist zu dokumentieren (Art. 5 Abs. 1 lit. a) und Abs. 2 DSGVO).

4.2 Auskunftsrecht nach Art. 15 DSGVO

Art. 15 DSGVO sieht ein Auskunftsrecht für betroffene Personen vor. Der betroffenen Person ist danach auf Antrag Auskunft darüber zu geben, ob personenbezogene Daten zu ihrer Person verarbeitet werden. Das bedeutet, dass auch eine Negativauskunft zu erteilen ist, wenn keine personenbezogenen Daten verarbeitet werden. Weiterhin muss über die verarbeiteten personenbezogenen Daten und über die folgenden Informationen Auskunft erteilt werden:

- → die Verarbeitungszwecke,
- → die Kategorien personenbezogener Daten, die verarbeitet werden,
- → die Empfänger oder Kategorien von Empfängern
  - die Dauer der Speicherung; falls nicht möglich die Kriterien für die Festlegung dieser Dauer,
  - das Bestehen der Rechte betroffener Personen auf Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Widerspruch aufgrund der besonderen Situation einer betroffenen Person,
- → das Recht auf Beschwerde bei der Aufsichtsbehörde,
- → bei Dritterhebung Informationen über die Herkunft der Daten,
  - sofern einschlägig: die Vornahme einer automatisierten Entscheidungsfindung einschließlich Profiling sowie Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der Verarbeitung für die betroffene Person,
- → sofern einschlägig: bei Datenübermittlung in ein Drittland Informationen über die geeigneten Garantien zum Schutz der Daten.

4.2.1 Ausnahmen nach § 34 BDSG

Nach § 34 Abs. 1 Nr. 1 BDSG besteht das Recht auf Auskunft für öffentliche Stellen nicht, wenn die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben oder die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde. Nach § 34 Abs. 1 Nr. 2 BDSG besteht die Auskunftspflicht auch dann nicht, wenn die gespeicherten Daten aufgrund von gesetzlichen oder satzungsmäßigen Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich zu Zwecken der Datensicherung und der Datenschutzkontrolle dienen und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde. Bei der Ermittlung des Aufwands hat der Verantwortliche die bestehenden technischen Möglichkeiten, gesperrte und archivierte Daten der betroffenen Person im Rahmen der Auskunftserteilung verfügbar zu machen, zu berücksichtigen. Der Verantwortliche hat sicherzustellen, dass durch geeigne-

te technische und organisatorische Maßnahmen eine Verwendung der Daten zu anderen Zwecken ausgeschlossen ist.

4.2.2 Form und Frist der Auskunftserteilung nach Art. 15 Abs. 3 DSGVO

Nach Art. 15 Abs. 3 DSGVO stellt der Verantwortliche der betroffenen Person eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Dies kann durch Übersendung in Papierform erfolgen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen.

Nach Art. 12 Abs. 2 DSGVO muss der Verantwortliche der betroffenen Person Informationen über die ergriffenen Maßnahmen unverzüglich, in jedem Fall innerhalb eines Monats nach Eingang des Antrags, zur Verfügung stellen.

4.2.3 Implementierung eines Auskunftsprozesses nach Art. 12 DSGVO

Zur Gewährleistung einer zuverlässigen und zügigen Beantwortung von Auskunftsverlangen ist ein strukturierter Prozess erforderlich, der den Ablauf und die Zuständigkeiten innerhalb der verantwortlichen Stelle festlegt. Dazu gehören, z. B. die Erfassung der Anfrage in einem Dokumentationssystem, die Versendung einer Eingangsbestätigung, die Prüfung, ob personenbezogene Daten verarbeitet werden sowie die Zusammenstellung und Beantwortung. Dabei sollten auch technische Maßnahmen berücksichtigt werden, die ein schnelles Auffinden und Bereitstellen der Daten ermöglichen.

4.3 Recht auf Berichtigung nach Art. 16 DSGVO

Nach Art. 16 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten oder – unter Berücksichtigung der Zwecke der Verarbeitung – die Vervollständigung unvollständiger personenbezogener Daten zu verlangen. Gegenstand des Berichtigungsrechts sind grundsätzlich Informationen, die objektiv nicht mit der Realität übereinstimmen, z. B. ein falscher Name oder ein falsches

Geburtsdatum. Dabei hat grundsätzlich die betroffene Person die Darlegungs- und Beweislast für das Vorliegen einer Unrichtigkeit. Können weder die betroffene Person noch der Verantwortliche die Richtigkeit oder Unrichtigkeit beweisen, ist die Verarbeitung der personenbezogenen Daten nach Art. 18 Abs. 1 lit. a) DSGVO einzuschränken. Die Berichtigung unrichtiger personenbezogener Daten muss unverzüglich, das heißt ohne schuldhaftes Zögern, erfolgen.

4.4 Recht auf Löschung („Recht auf Vergessenwerden“) nach Art. 17 DSGVO

Nach Art. 17 Abs. 1 DSGVO hat die betroffene Person unter den in der Vorschrift genannten Voraussetzungen das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden. Löschen bedeutet, dass die personenbezogenen Daten unkenntlich gemacht werden müssen. Bei technischen Löschungsmechanismen sind dabei technische Standards, z. B. DIN, zu berücksichtigen. Grundsätzlich muss die Löschung auf allen Datenträgern erfolgen.

Nach Art. 17 Abs. 1 lit. a) DSGVO besteht ein Löschungsanspruch, wenn die Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Nach den übrigen in Art. 17 Abs. 1 lit. b) bis f) DSGVO genannten Voraussetzungen sind die personenbezogenen Daten zu löschen, wenn für ihre Verarbeitung keine Rechtsgrundlage (mehr) besteht. Dies ist u. a. der Fall, wenn die Einwilligung widerrufen wird, auf die sich die Verarbeitung stützte, die Daten unrechtmäßig verarbeitet wurden oder die Daten aufgrund einer Rechtsvorschrift gelöscht werden müssen. In sämtlichen der in Art. 17 Abs. 1 lit. b) bis f) DSGVO genannten Fälle ist eine weitere Speicherung der Daten unzulässig.

Daneben gilt das „Recht auf Vergessenwerden“ nach Art. 17 Abs. 2 DSGVO. Danach besteht eine Informationspflicht der Stelle, die personenbezogene Daten öffentlich gemacht hat, wenn die Daten auf Verlangen der betroffenen Person nach Art. 17 Abs. 1 DSGVO gelöscht werden müssen. Die Stelle, die die Daten veröffentlicht hat, hat unter Berücksichtigung der verfügbaren Technologie und der Implemen-

tierungskosten angemessene Maßnahmen zu treffen, um die für die Datenverarbeitung verantwortlichen Stellen darüber zu informieren, dass die betroffene Person eine Löschung der sie betreffenden Daten verlangt hat.

Ein Anspruch auf Löschung von personenbezogenen Daten besteht nach Art. 17 Abs. 3 DSGVO in den Fällen nicht, in denen aufgrund entgegenstehender Interessen das Recht der betroffenen Person auf Löschung im Einzelfall eingeschränkt werden kann, u. a. wenn die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Zu berücksichtigen ist, dass personenbezogene Daten nicht nur auf Antrag der betroffenen Person zu löschen sind, sondern grundsätzlich nach Art. 5 Abs. 1 lit. e) i. V. m. Art. 6 Abs. 1 und Art. 17 Abs. 1 lit. a) DSGVO eine Pflicht des Verantwortlichen zur Löschung personenbezogener Daten besteht, wenn die Daten zur Erreichung der Zwecke, für die sie verarbeitet werden, nicht mehr erforderlich sind. Insbesondere sind personenbezogene Daten unverzüglich zu löschen, wenn ihre Verarbeitung unrechtmäßig ist, Art. 17 Abs. 1 lit. d) DSGVO.

4.5 Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO

Nach Art. 4 Abs. 3 DSGVO handelt es sich bei der Einschränkung der Verarbeitung um die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Die Einschränkung der Verarbeitung hat nach Art. 18 Abs. 1 DSGVO auf Antrag des Betroffenen zu erfolgen, wenn die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen. Die Einschränkung muss außerdem erfolgen, wenn die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der Daten verlangt.

Die Verarbeitung personenbezogener Daten ist ferner einzuschränken, wenn der Verantwortliche die personenbezogenen Daten nicht länger für Zwecke der Verarbeitung benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt (Art. 18 Abs. 1 lit. c) DSGVO). Auch in diesem Fall stehen einer Löschung schutzwürdige Interessen der betroffenen Person entgegen. Das Recht auf Einschränkung der Verarbeitung besteht außerdem, wenn die betroffene Person Widerspruch gegen die Verarbeitung gemäß Art. 21 DSGVO eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

In Fällen, in denen einer Löschung Aufbewahrungsfristen entgegenstehen, die sich aus Gesetzen, Satzungen oder Verträgen ergeben, ist eine weitere Verarbeitung nach Art. 6 i. V. m. Art. 5 Abs. 1 lit. b) DSGVO nur für die jeweiligen Aufbewahrungszwecke zulässig.

Die DSGVO enthält keine Regelung zur Einschränkung der Verarbeitung, wenn eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Dieser Sachverhalt ist jedoch von § 35 Abs. 1 BDSG erfasst.

Personenbezogene Daten, deren Verarbeitung auf Verlangen der betroffenen Person eingeschränkt worden ist, dürfen nach Art. 18 Abs. 2 DSGVO nur mit deren Einwilligung oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte anderer Personen oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.

4.6 Mitteilungspflicht über Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung nach Art. 19 DSGVO

Art. 19 DSGVO begründet eine Pflicht des Verantwortlichen, Empfänger, denen personenbezogene Daten offengelegt wurden, über jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung der Daten zu informieren. Diese Pflicht besteht nicht, wenn diese Information unmöglich oder mit

einem unverhältnismäßigen Aufwand verbunden wäre. Allerdings entfällt die Mitteilungspflicht nicht, wenn schutzwürdige Interessen der betroffenen Person entgegenstehen. Der Verantwortliche muss die betroffene Person zudem über die Empfänger unterrichten, wenn die betroffene Person dies verlangt.

4.7 Widerspruchsrecht nach Art. 21 DSGVO

Art. 21 DSGVO räumt der betroffenen Person das Recht ein, aus Gründen, die sich aus ihrer besonderen Situation ergeben, rechtmäßigen und auf gesetzlicher Grundlage erfolgenden Datenverarbeitungen zu widersprechen. Dies gilt gerade auch gegenüber Behörden. Kann der Verantwortliche nicht nachweisen, dass seine Interessen, Rechte oder Freiheiten die der betroffenen Person überwiegen oder die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient, dürfen die personenbezogenen Daten nicht mehr verarbeitet werden.

Das Widerspruchsrecht besteht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt oder eine Rechtsvorschrift zur Verarbeitung verpflichtet (Art. 21 Abs. 1 S. 1 DSGVO/§ 36 BDSG).

4.8 Automatisierte Einzelfallentscheidung nach Art. 22 DSGVO

Nach Art. 22 DSGVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise beeinträchtigt. Dieses Recht besteht nicht, wenn eine ausdrückliche Einwilligung der betroffenen Person vorliegt oder die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist, oder wenn sie nach Rechtsvorschriften der Union oder eines Mitgliedstaates zulässig ist, und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Betroffenenrechte enthalten.

4.9 Implementierung von Prozessen zur Gewährleistung der Betroffenenrechte entsprechend Art. 12 DSGVO

Zur Gewährleistung der Betroffenenrechte sind durch die Verantwortlichen technische und organisatorische Maßnahmen zu ergreifen. Dazu gehören neben der Festlegung von Zuständigkeiten und dem Verfahrensablauf, einschließlich im Einzelfall notwendiger Identitätsprüfungen, auch Protokollierungspflichten, wer wann welche Verarbeitungsschritte durchgeführt hat. Löschkonzepte müssen erstellt und überprüft werden. Zu berücksichtigen ist, dass Schadensersatzansprüche oder Sanktionen nicht nur durch die Nichtgewährung der Betroffenenrechte, sondern auch z. B. durch eine fehlerhafte Berichtigung oder Löschung ausgelöst werden können. Es ist sinnvoll, die Umsetzung dieser technischen und organisatorischen Maßnahmen durch entsprechende Hausanordnungen verbindlich und transparent zu regeln.

Nach Art. 12 DSGVO sowie EG 59 sollen Modalitäten festgelegt werden, die einer betroffenen Person die Ausübung ihrer Rechte erleichtern. Verantwortliche sollen dafür sorgen, dass Anträge elektronisch gestellt werden können. Außerdem sollen die Verantwortlichen Anträge der betroffenen Personen zur Ausübung ihrer Betroffenenrechte unverzüglich, spätestens innerhalb eines Monats nach Eingang, beantworten und begründen, warum der Antrag ggf. abgelehnt wird. Alle Informationen und Mitteilungen an die betroffene Person, die sich auf die Verarbeitung ihrer personenbezogenen Daten beziehen, müssen in transparenter, verständlicher und leicht zugänglicher Form erfolgen.

www.bfdi.bund.de