Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Die DSGVO in der Bundesverwaltung

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 997799-5550
E-Mail: referat11@bfdi.bund.de
Internet: http://www.datenschutz.bund.de

Stand: April 2018

Realisation: Appel & Klinger Druck und Medien GmbH
Bildnachweis: adobe stock

Die DSGVO in der Bundesverwaltung

Inhaltsverzeichnis

Vorwort

Mit dem 25. Mai 2018 ist die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) anzuwenden. Am gleichen Tage treten auch das neue Bundesdatenschutzgesetz (BDSG) sowie erhebliche Änderungen der Datenschutzvorschriften in den Sozialgesetzbüchern I und X und in der Abgabenordnung in Kraft.

Es ist nicht übertrieben, diesen Moment als eine Zeitenwende im europäischen und deutschen Datenschutzrecht zu bezeichnen. Die bislang in mitgliedstaatliches Recht umzusetzende Richtlinie 95/46/EG tritt außer Kraft und wird durch eine unmittelbar geltende EU-Verordnung ersetzt. Das BDSG und die bereichsspezifischen Datenschutzvorschriften in Deutschland gelten nur noch ergänzend und insoweit, wie die Datenschutz-Grundverordnung dies zulässt. Zudem wird auch der Datenschutz für polizeiliche und justizielle Datenverarbeitung auf eine neue Grundlage gestellt, indem mit dem 5. Mai 2018 die Richtlinie (EU) 2016/680 umgesetzt sein muss, die einen entsprechenden Rahmenbeschluss der EU aus dem Jahre 2008 ersetzt.

Die mit dem neuen Recht einhergehenden Änderungen erfordern auch in der Bundesverwaltung erhebliche Anpassungen. So wird der Schutz personenbezogener Daten einen noch höheren Stellenwert in der täglichen Arbeit der öffentlichen Stellen des Bundes und nicht zuletzt auch ihrer behördlichen Datenschutzbeauftragten bekommen. Die DSGVO und das neue BDSG legen einen deutlich höheren Wert auf die Dokumentation der Verarbeitung personenbezogener Daten und den darauf basierenden Nachweis der Einhaltung der datenschutzrechtlichen Bestimmungen.

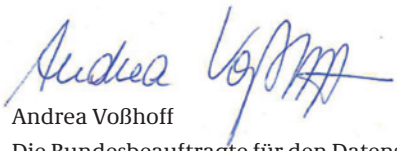
Dies macht es für die Behörden notwendig, sämtliche internen Verfahren und Prozesse im Zusammenhang mit der Verarbeitung personenbezogener Daten auf den Prüfstand zu stellen und in vielen Fällen zu überarbeiten.

Schließlich werden mit den neuen Regelungen die Befugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zur Durchsetzung des Datenschutzrechts in der Bundesverwaltung deutlich erweitert. Anders als bisher ist die BfDI im Anwendungsbereich künftig nicht mehr auf die oft folgenlose Beanstandung beschränkt. Sie

wird vielmehr rechtsverbindliche Anordnungen zur Durchsetzung der datenschutzrechtlichen Bestimmungen treffen können. Auch wenn diese Abhilfemaßnahmen gegenüber Behörden nicht in gleicher Weise vollstreckt werden können wie gegenüber Unternehmen, werden die öffentlichen Stellen des Bundes angehalten sein, den Empfehlungen und Anordnungen der BfDI in sehr viel stärkerem Maße Folge zu leisten, als dies bisher der Fall war. Mehr denn je wird die BfDI ihren Auftrag aber auch als einen beratenden verstehen und die öffentlichen Stellen des Bundes bei der Umsetzung der oft abstrakt gehaltenen rechtlichen Anforderungen unterstützen.

Der vorliegende Leitfaden soll einen ersten praktischen Überblick über die umzusetzenden Vorgaben geben. Er richtet sich in erster Linie an diejenigen Organisationseinheiten aller öffentlichen Stellen des Bundes, die vor Ort für die Einhaltung des Datenschutzes Sorge tragen und gibt darüber hinaus auch den Datenschutzbeauftragten aller öffentlichen Stellen des Bundes ein Werkzeug zur Erfüllung ihrer Aufgaben an die Hand.

Bonn, im April 2018



Andrea Voßhoff
Die Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

1 Anforderungen an und Anpassung von Verfahren

1.1 Nachweis- und Rechenschaftspflichten nach Art. 5 Abs. 2, Art. 24 DSGVO und weiteren Vorschriften

Nach dem Grundsatz der Rechenschaftspflicht in Art. 5 Abs. 2 DSGVO ist der Verantwortliche[1] verpflichtet, die Grundsätze in Art. 5 Abs. 1 DSGVO nicht nur einzuhalten, sondern die Einhaltung auch nachzuweisen. Konkretisiert wird die Rechenschaftspflicht 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.

Der Verantwortliche hat eine Dokumentation zu erstellen, mit der er nachweist, dass er rechtmäßig handelt. Durch die Dokumentationspflicht wird der Verantwortliche angehalten, die Einhaltung der genannten Grundsätze zu prüfen. Den Aufsichtsbehörden sowie den betrieblichen und behördlichen Datenschutzbeauftragten wird dadurch die Prüfung, ob der Verantwortliche personenbezogene Daten rechtmäßig verarbeitet, erleichtert. Die Rechenschaftspflicht wird mit der DSGVO neu eingeführt, eine entsprechende Dokumentation war jedoch schon bisher aus den genannten Gründen angeraten.

Die Rechenschaftspflicht bezieht sich auf die Grundsätze in Art. 5 Abs. 1 DSGVO und damit auf viele weitere Vorschriften der DSGVO. Die Pflichten in den Art. 24 und 25 beziehen sich auf die gesamte DSGVO. Im Einzelnen ist daher insbesondere die Einhaltung der folgenden Vorschriften der DSGVO nachzuweisen:

- Art. 5 Abs. 1 a (Rechtmäßigkeit der Datenverarbeitung), Art. 6 bis 10 (Rechtsgrundlagen)
- Art. 5 Abs. 1 a (Verarbeitung nach Treu und Glauben und Transparenz), Art. 12 bis 15 (Information und Auskunft)
- Art. 5 Abs. 1 b (Zweckbindung), Art. 6 Abs. 4 (Weiterverarbeitung)
- Art. 5 Abs. 1 c (Datenminimierung)

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

- Art. 5 Abs. 1 d (Richtigkeit), Art. 16, 18 (Berichtigung und Einschränkung der Verarbeitung)
- Art. 5 Abs. 1 e (Speicherbegrenzung), Art. 17 (Löschung)
- Art. 5 Abs. 1 f (Integrität und Vertraulichkeit), Art. 32 (Sicherheit der Verarbeitung)

Die DSGVO macht keine Angaben über die Art und Weise der Dokumentation. Es sollte jedoch in einem möglichst frühen Stadium der Entwicklung des Verfahrens ein aussagekräftiges Datenschutzkonzept erstellt werden. 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 Satz 1 DSGVO und des Erwägungsgrunds (EG) 76 ist der sog. 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).

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 – im Unter-

schied zum bisherigen Verfahrensverzeichnis nach dem BDSG (alt) – nichtautomatisierte Verarbeitungen, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Damit wird das nach den bisherigen Vorgaben des BDSG (alt) zu führende Verfahrensverzeichnis abgelöst.
Die Verpflichtung zur Führung des Verzeichnisses erstreckt sich nunmehr auf sämtliche Verarbeitungstätigkeiten einer öffentlichen Stelle. Die bisher in § 18 Abs. 2 Satz 3 BDSG (alt) enthaltene Ausnahme für allgemeinen Verwaltungszwecken dienende Verarbeitungen entfällt künftig, sodass auch diese in ein Verzeichnis aufzunehmen sind. Als Verarbeitungstätigkeit ist bei öffentlichen Stellen die Erfüllung einer bestimmten Aufgabe auf geeignetem Abstraktionsniveau zu verstehen (z. B. „Erteilung von strom- und schifffahrtspolizeilichen Genehmigungen", „Zulassung von Arzneimitteln", „Bewilligung von Beihilfe" oder „Bearbeitung von Bürgerbeschwerden"). Die Verarbeitungstätigkeit ist dabei grundsätzlich an eine aus einer zu erfüllenden Aufgabe folgende Zweckbestimmung gebunden.

Die Verpflichtung zur Führung des Verzeichnisses von Verarbeitungstätigkeiten soll dem Nachweis der Einhaltung der Verordnung dienen (vgl. Erwägungsgrund 82 DSGVO) und konkretisiert damit als ein Baustein die allgemeine Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO.[2]

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

Es ist nach Art. 30 Abs. 4 DSGVO auf Anfrage der BfDI als für die öffentlichen Stellen des Bundes zuständige Aufsichtsbehörde zur Verfügung zu stellen.

Der Aufsichtsbehörde und dem behördlichen Datenschutzbeauftragten dient es als Ausgangspunkt ihrer Kontrollmaßnahmen. Es kann aber in der Regel nur eine vorläufige Rechtmäßigkeitsprüfung ermöglichen.[3]

---

2 siehe: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Kurzpapier_Verzeichnis%20von%20Verarbeitungstaetigkeiten.pdf?__blob=publicationFile&v=3 Kurzpapier Nr. 1 der DSK (Stand 29.06.2017), https://www.lda.bayern.de/media/baylda_dsgvo_5_processing_activities.pdf BayLDA-Kurzpapier Nr. 5 zur DS-GVO.

3 vgl. Paal, Pauly, Kommentar zur DS-GVO, Art. 30 Rn 2.

Das Verzeichnis ist nicht öffentlich zugänglich; die bisher im BDSG (alt) vorgesehene Trennung in ein internes und ein externes Verzeichnis entfällt.

Das Verzeichnis ist schriftlich oder elektronisch zu führen (Art. 30 Abs. 3 DSGVO). Auch Auftragsverarbeiter 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.[4]

1.2.1 Adressat der Erstellungs- und Führungspflicht

Adressat der in Art. 30 DSGVO normierten Verpflichtung zur Erstellung und Führung des Verzeichnisses von Verarbeitungstätigkeiten ist der oder sind die Verantwortliche(n) und ggf. deren Vertreter. Die Erstellung der einzelnen Beiträge über die Verarbeitungsprozesse sollte am besten von den Fachreferaten und / oder Organisationseinheiten geleistet werden können, die mit diesen befasst sind. Auch die Verpflichtung zur Erstellung und Aktualisierung des Verfahrensverzeichnisses nach dem BDSG (alt) war keine Aufgabe des behördlichen Datenschutzbeauftragten. Die Artikel-29-Gruppe erachtet es jedoch als zulässig, eine Übertragung von Tätigkeiten im Zusammenhang mit der Erstellung und Führung des Verarbeitungsverzeichnisses auf behördliche Datenschutzbeauftragte vorzunehmen.[5]

Es dürfte unstreitig sein, dass die mit der Verpflichtung verbundene Verantwortung zur Rechenschaftspflicht nach der DSGVO nicht vom Verantwortlichen auf den behördlichen Datenschutzbeauftragten übertragen werden kann. Denn der Datenschutzbeauftragte hat die Einhaltung der Verordnung und damit auch die Erfüllung eben dieser Verpflichtung durch den Verantwortlichen zu überwachen (vgl. Art. 39 Abs. 1 b) DSGVO). Zwar kann der Verantwortliche grundsätzlich dem Datenschutzbeauftragten zusätzliche Aufgaben übertragen (vgl. Art. 38 Abs. 6 DSGVO), dabei sollte jedoch die Vermeidung möglicher Interessenkollisionen beachtet werden.[6] Deshalb sollte grundsätzlich davon Abstand genommen werden, dem Datenschutzbeauftragten unmittelbar die Führung der Verzeichnisse als Aufgabe zu übertragen.

Davon unbenommen bleibt selbstverständlich die Beratungsfunktion des Datenschutzbeauftragten im Sinne des Art. 39 Abs. 1 DSGVO. Auf Grund seiner Fachkompetenz dürfte es

4 https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/Muster_Verzeichnis_Verarbeitungstaetigkeiten.html?nn=5217040

5 Artikel 29 Gruppe, WP 243, Leitlinien in Bezug auf Datenschutzbeauftragte, zu 4.5, Seite 22 f.

6 vgl. Dr. Philipp Kramer, Datenschutz im Fokus, Nr. 06/2017, S. 126, Was muss der Datenschutzbeauftragte nach der DSGVO erledigen?

vorteilhaft sein, diesen in den Prozess der Erstellung und Aktualisierung des Verzeichnisses einzubinden. Zudem gehört die Überwachung der Vollständigkeit und Rechtmäßigkeit der Verzeichnisse zu den Aufgaben des Datenschutzbeauftragten.

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 Satz 2, Art. 49 Abs. 6 DSGVO:

- Namen und Kontaktdaten des / der gemeinsam Verantwortlichen sowie deren Vertreter. Neu ist, dass Angaben und Kontaktdaten der behördlichen Datenschutzbeauftragten aufgenommen werden müssen.
- 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 Datenschutzbeauftragten aber auch für die BfDI leichter erkennbar, ob eine Beauftragung vorliegt und ob hierbei die gesetzlichen Anforderungen eingehalten worden sind.

1.3 Anforderungen an die Datensicherheit, Art. 25, 32 DSGVO

1.3.1 Privacy by Default und Privacy by Design

Art. 25 DSGVO führt mit den Prinzipien „Datenschutz durch Technikgestaltung“ (Privacy by Design) und „Datenschutz durch datenschutzfreundliche Voreinstellungen“ (Privacy by

Default) Anforderungen an die Gestaltung und den Betrieb von Verfahren ein, bei denen personenbezogene Daten verarbeitet werden. Auf diese Weise soll der Verantwortliche für die Datenverarbeitung dazu verpflichtet werden, 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 im Regelfall (die Übersetzung „durch Voreinstellung" für „by Default" erscheint an dieser Stelle nicht so günstig) nur solche personenbezogenen Daten verarbeitet werden, die für den jeweils bestimmten Verarbeitungszweck notwendig sind und dass diese Daten im Regelfall auch nicht einer unbestimmten Zahl von Personen zugänglich gemacht werden.

Art. 25 DSGVO schreibt auf diese Weise ebenfalls das aus dem BDSG (alt) bekannte Prinzip der Datensparsamkeit fort (vgl. auch Art. 5 DSGVO„Datenminimierung").

1.3.2 Technische und organisatorische Maßnahmen

Art. 32 DSGVO verpflichtet sowohl den Verantwortlichen als auch einen möglichen Auftragsverarbeiter dazu, angemessene 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 noch engere Verbindung zwischen Datenschutz und IT-Sicherheit bzw. IT-Sicherheitsmanagement her, als dies bisher der Fall war.

Als konkretes Beispiel für mögliche Maßnahmen nennen Art. 25 und 32 DSGVO die Pseudonymisierung sowie Art. 32 DSGVO zusätzlich die Verschlüsselung personenbezogener Daten. Eine Aufteilung in konkretere Kontrollbereiche, wie sie bisher im Anhang zu § 9 Satz 1 BDSG (alt) zu finden war, macht die DSGVO nicht.

1.3.3 Stand der Technik und Angemessenheit 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, und dass die Beurteilung der Angemessenheit der Maßnahmen insbesondere auch unter Berücksichtigung des Implementierungsaufwands und der bestehenden Risi-

ken erfolgen soll. Auf diese Weise wird der risikobasierte Ansatz bei der Beurteilung von Verfahren zur Verarbeitung personenbezogener Daten nun quasi 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. Hier werden alle Beteiligten gefordert sein, eine nachvollziehbare und pragmatische Definition zu finden, die außerdem berücksichtigt, dass sich der Stand der Technik selbstverständlich mit der Zeit ändert.

1.3.4 Zertifizierung und genehmigte Verfahrensregeln

Beide Artikel nennen die Einhaltung genehmigter Verfahrensregeln oder die Zertifizierung nach den Artikeln 40 bzw. 42 DSGVO als mögliche Nachweise für die Erfüllung der aufgestellten Anforderungen.

Da derzeit noch keine entsprechenden genehmigten Verfahrensregeln oder Zertifizierungsverfahren existieren, kann im Moment noch keine Aussage darüber getroffen werden, wie sich der dafür entstehende Mehraufwand für den Zertifizierungsprozess im Verhältnis zu der Vereinfachung gegenüber einem individuellen Nachweis der Erfüllung der Anforderungen verhält.

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

1.4.1 Unterschiede zur Vorabkontrolle nach § 4d Abs. 5 BDSG (alt)

Im Gegensatz zur bisherigen Vorabkontrolle liegt die Zuständigkeit für die Durchführung einer DSFA beim Verantwortlichen und nicht beim Datenschutzbeauftragten. Der Verantwortliche hat allerdings die Verpflichtung, bei der Durchführung der DSFA den Rat des Datenschutzbeauftragten einzuholen.

Im Rahmen der DSFA sind neben der Rechtmäßigkeit der Datenverarbeitung auch die Risiken aus den Verarbeitungsvorgängen zu identifizieren und zu bewerten sowie ggf. Maßnahmen zur Abhilfe zu treffen. Anders als die Vorabkontrolle soll im Rahmen der DSFA die Entwicklung und Gestaltung einer Datenverarbeitung beeinflusst werden.

Während die Vorabkontrolle nur automatisierte Verarbeitungen erfasst, bezieht sich die DSFA auf sämtliche Verarbeitungen, solange diese ein hohes Risiko für die Betroffenen beinhalten.

Für die Vorabkontrolle besteht ferner ein Ausnahmevorbehalt, d.h. sie findet nicht statt, wenn eine gesetzliche Verpflichtung besteht, eine Einwilligung der Betroffenen vorliegt oder die Datenverarbeitung aus bestimmten Gründen erforderlich ist. Für die DSFA fasst

Art. 35 DSGVO den Ausnahmebereich jedoch deutlich enger und regelt die Erforderlichkeit und die Anforderungen grundsätzlich unmittelbar.
Während Art. 36 DSGVO im Anschluss an die Durchführung einer DSFA eine Konsultation der Aufsichtsbehörde in bestimmten Fällen zwingend vorsieht, hat sich der Datenschutzbeauftragte nach durchgeführter Vorabkontrolle nur in Zweifelsfällen an die Aufsichtsbehörde zu wenden.

Ferner unterliegt die Dokumentation der Vorabkontrolle keinen inhaltlichen Anforderungen – anders als die Dokumentation der DSFA.

Schließlich sehen die Regelungen zur Vorabkontrolle anders als bei der DSFA keine Pflicht zur Überwachung des Ergebnisses vor.

Somit geht der Umfang einer DSFA deutlich über den der bisherigen Vorabkontrolle hinaus.

1.4.2 Welche Verarbeitungen erfordern eine DSFA?

Eine DSFA ist grundsätzlich durchzuführen, wenn sich aus einem Verarbeitungsvorgang hohe Risiken ergeben. Dies ist in der Regel dann der Fall, wenn mindestens zwei der folgenden Kriterien erfüllt sind:[7]

- Systematische und umfassende Bewertung der Persönlichkeit, die die Grundlage von Entscheidungen mit Rechtswirkungen für den Einzelnen bildet.
- Verarbeitung sensitiver Daten nach Art. 9 Abs. 1 oder Art. 10 DSGVO.
- Großflächige Videoüberwachung.
- Einsatz von Verarbeitungsverfahren, bei denen den Betroffenen die Ausübung ihrer Rechte erschwert wird (insbesondere bei wenig transparenten Verfahren).
- Einsatz von Verarbeitungsverfahren, die ein hohes Risiko für die Rechte und Freiheiten der Betroffenen mit sich bringen, insbesondere neue Verfahren .
- Verarbeitung großer Mengen personenbezogener Daten (große Anzahl von Betroffenen).
- Verarbeitung personenbezogener Daten aufgrund des Ungleichgewichts der Parteien[8].
- Datentransfer außerhalb der EU[9].
- Vergleich oder Kombination von Datensätzen.

7 Art. 29 Datenschutzgruppe, 2017, WP 248.
8 Erwägungsgrund 75 zur DSGVO.
9 Erwägungsgrund 116 zur DSGVO.

1.4.3 Mindestinhalt der DSFA

- Systematische Beschreibung der geplanten Verarbeitungsvorgänge
- Beschreibung des Zwecks der Verarbeitung
- Rechtsgrundlagen der Verarbeitung
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen
- Zur Bewältigung dieser Risiken geplante Abhilfemaßnahmen.

1.4.4 Anforderungen an die DSFA

- Nachvollziehbarkeit / Überprüfbarkeit (Einhaltung der rechtlichen Vorgaben; Überprüfbarkeit für Dritte)
- Vergleichbarkeit (Vergleich standardisierter DSFA für verschiedene Verarbeitungen)
- Effizienz (standardisiertes, technologieneutrales Verfahren verringert den Aufwand für die Erstellung der DSFA).

1.4.5 Vorgehen bei der Durchführung der DSFA

Vorbereitungsphase

- Festlegung der Zuständigkeiten: Durchführung durch Organisationseinheit des Verantwortlichen – ggf. unter Einbeziehung des Auftragsverarbeiters –, obligatorische Beteiligung des behördlichen Datenschutzbeauftragten
- Beschreibung des Prüfgegenstandes (Verfahren, Datenflüsse, Zwecke)
- Identifikation der Rechtsgrundlagen
- Prüfung der Notwendigkeit einer DSFA (Relevanzschwelle)
- Dokumentation des Ergebnisses im Rahmen des Datenschutzmanagementsystems
- Prüfungsplanung.

Bewertungsphase

- Identifikation der Bewertungsmaßstäbe anhand der Schutz- bzw. Gewährleistungsziele des Standarddatenschutzmodells (= Transparenz, Nicht-Verkettbarkeit, Datensparsamkeit, Intervenierbarkeit, Integrität, Vertraulichkeit)[10]
- Identifikation möglicher Angreifer, Angriffsmotive und -ziele oder organisatorischer Schwachstellen
- Festlegung der Eintrittswahrscheinlichkeit

10 Hier wird als Bewertungsmaßstab das sachgerecht erscheinende SDM vorgeschlagen. Da die Frage nach der Methodik noch offen ist, kommen alternativ ein Vorgehen nach BSI-Grundschutz oder ein Vorgehen nach SDM und BSI-Grundschutz in Betracht.

- Bestimmung der Eingriffsintensität und des Schutzbedarfs (= normal bei personenbezogenen Daten; hoch bei besonderen personenbezogenen Daten, erheblichen Konsequenzen für die Personen und / oder wenn keine effektiven Interventionsmöglichkeiten bestehen; sehr hoch bei existenzieller Abhängigkeit der Personen und keiner Transparenz für diese)
- Bewertung, ob Verarbeitung notwendig und verhältnismäßig ist
- Bewertung der Risiken für die Rechte der Betroffenen.

Maßnahmenphase

- Dokumentation der Bewertungsergebnisse
- Identifikation und Auswahl passender Schutzmaßnahmen
- Implementierung der Schutzmaßnahmen
- Test und Dokumentation der Wirksamkeit der Schutzmaßnahmen
- Nachweis über die Einhaltung der DSGVO
- Ergibt die Folgenabschätzung, dass die Verarbeitung ein hohes Risiko für Betroffene zur Folge hätte und verbliebe trotz Gegenmaßnahmen ein zu hohes Restrisiko, ist vor Beginn der Verarbeitung eine Verständigung des Verantwortlichen – unter Beteiligung des DSB – mit BfDI erforderlich.

Berichtsphase / Überprüfung

- Erstellung eines DSFA-Berichts und Maßnahmenplans
- Dokumentation im Verzeichnis der Verarbeitungstätigkeiten
- Ggf. unabhängige Überprüfung der Ergebnisse
- Erstellung eines Überprüfungskonzeptes (Festlegung von Überprüfungsintervallen: in der Regel 6 Monate bei Kernprozessen, 12 Monate bei Standardprozessen).

Hinsichtlich der Durchführung einer DSFA wird im Übrigen auf die Beispiele der Verfahren für Privacy Impact Assessments verwiesen.

1.4.6 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. Dies gilt allerdings nur dann, wenn bei diesen Verfahren nach altem Recht eine Vorabkontrolle stattgefunden hat. Denn in allen Fällen, in denen nach der DSGVO eine DSFA durchzuführen ist, sind auch die Voraussetzungen des bisherigen § 4d Abs. 5 BDSG (alt) erfüllt.

Unabhängig davon wird mit Blick auf einen einheitlichen Datenschutzstandard der Behörde empfohlen, bei aufgrund von Änderungen der Verfahren erforderlich werdenden An-

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

1.4.7 Positiv- und Negativlisten der Aufsichtsbehörden

Gem. Art. 35 Abs. 4 DSGVO erstellen die Aufsichtsbehörden Listen von Verarbeitungsvorgängen, bei denen Datenschutz-Folgenabschätzungen durchzuführen sind und veröffentlichen diese. Die unabhängigen Datenschutzbehörden des Bundes und der Länder erstellen gegenwärtig eine gemeinsame Liste der deutschen Aufsichtsbehörden, die (auch) auf der Homepage der BfDI (www.datenschutz.bund.de) veröffentlicht wird.

Die gem. Art. 35 Abs. 5 DSGVO nicht obligatorische Liste von Verarbeitungsvorgängen, bei denen keine DSFA durchzuführen ist, werden die deutschen Aufsichtsbehörden vorerst nicht erstellen.

1.4.8 Hinweise zur Vorabkonsultation der 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. Dabei sind der Aufsichtsbehörde Informationen nach Art. 36 Abs. 3 DSGVO vorzulegen. Diese Pflicht besteht allerdings nur dann, wenn der Verantwortliche dieses Risiko nicht durch entsprechende Gegenmaßnahmen eindämmen oder ausschließen kann. Eine Konsultation der Aufsichtsbehörde ist mithin nur dann erforderlich, wenn nach den Gegenmaßnahmen ein Restrisiko verbleibt und dieses als zu hoch eingestuft wird.

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 Buchst. 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 die BfDI und ggf. zusätzlich eine Benachrichtigung an die von der Verletzung betroffene Person zu erfolgen.

Das BDSG (alt) hat bislang ebenfalls vergleichbare Regelungen enthalten, die jedoch öffentliche Stellen nur in bestimmten Fällen – insbesondere nach § 83a Sozialgesetzbuch (SGB) X – verpflichteten. Die DSGVO erweitert und verschärft diese Verpflichtungen, die nunmehr für alle öffentlichen Stellen gelten.

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

Der für die Datenverarbeitung Verantwortliche, nicht der Auftragsverarbeiter (AV), hat der BfDI die Datenschutzverletzung zu melden. Der AV ist jedoch verpflichtet, eine Verletzung – soweit sie im Rahmen seiner Tätigkeit eingetreten ist – an den Verantwortlichen mitzuteilen, damit dieser ggf. seiner Verpflichtung gegenüber der BfDI nachkommen kann.

Grundsätzlich löst die Verletzung des Schutzes jedes personenbezogenen Datums die Meldepflicht aus. Eine Verletzung liegt nach Art. 4 Ziffer 12 DSGVO vor, wenn eine 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 werden.

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

Soweit kein Risiko für die Rechte und die Freiheit der betroffenen Person vorliegt, entfällt die Meldepflicht.

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, drohende physische, materielle und immaterielle Schäden. Die Überlegungen bedürfen einer jeweiligen Betrachtung der konkreten Umstände des Einzelfalls.

Eine bestimmte Form der Meldung an die BfDI ist nicht vorgeschrieben. Im Hinblick auf die Dokumentations- und Rechenschaftspflichten des Verantwortlichen ist jedoch 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 Datenschutzbeauftragten 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 die 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 Verletzungen mit einem hohen Grad der Wahrscheinlichkeit eintreten können.

Diese Benachrichtigung, die Höhe des Schadensausmaßes und das Risiko sind in die Prognoseentscheidung des Verantwortlichen einzubeziehen, für deren Richtigkeit er die Verantwortung trägt. Zu berücksichtigen sind dabei alle Folgen für die Persönlichkeitsentfaltung des Betroffenen, 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 den Zugang unberechtigter Personen verhindern (etwa Verschlüsselung);

- der Verantwortliche sichergestellt hat, dass das hohe Risiko nach Art. 34 Abs. 1 DSGVO nicht mehr besteht;
- 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. 2, b, c und d DSGVO enthalten sollte. Sie ist unverzüglich nach Kenntnis von der Datenschutzverletzung vorzunehmen.

1.5.3 Dokumentationspflichten im Zusammenhang mit Art. 33 und 34 DSGVO

Den Verantwortlichen trifft 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

Auch unter Berücksichtigung der Erwägungsgründe zur DSGVO (vgl. insbes. EG 87) sollte der Verantwortliche Strukturen etablieren, die ihm ermöglichen, im Falle einer Datenschutzverletzung den Verpflichtungen der DSGVO aus Art. 33 und Art. 34 nachzukommen. 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 (bspw. in IT-Verfahren, in denen Datenverletzungen nicht unmittelbar für jeden Anwender erkennbar sind oder 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

Die Auftragsverarbeitung ist in Art. 28 DSGVO geregelt; die Anforderungen und Verpflichtungen, die sich dabei für den Verantwortlichen (bisher: Auftraggeber) ergeben, entsprechen dabei weitgehend dem jetzigen deutschen Recht (§ 11 BDSG (alt)), zum Teil sind Lockerungen vorgesehen. Insbesondere wird der Verantwortliche hinsichtlich der Kontrollpflichten bei der Überprüfung der technisch-organisatorischen Maßnahmen entlastet. Dem korrespondiert zum einen eine stärkere Fokussierung auf den Nachweis durch Zertifikate und ähnliche Nachweise, zum anderen aber auch eine stärkere Einbindung in die Verantwortlichkeit des Auftragsverarbeiters (zuvor: Auftragnehmer). Für diesen ergeben sich zum Teil weitreichende Änderungen sowohl im Hinblick auf seine datenschutzrechtlichen Verantwortlichkeiten als auch auf seine Haftung. Der Auftragsverarbeiter ist nunmehr neben dem Verantwortlichen eigenständiger Adressat der DSGVO. Dabei geht die Auftragsverarbeitung bei der (Auf-)Teilung der Verantwortlichkeiten nicht so weit wie die ebenfalls in der DSGVO (Art. 26) vorgesehene gemeinsame Verantwortlichkeit („Joint controllership"), bietet aber ein größeres Anwendungsspektrum als die oftmals eng verstandene „alte" Auftragsdatenverarbeitung, bei der zum Teil gefordert wurde, dass die Auftragsausführung sich ausschließlich auf die technische Durchführung des Datenverarbeitungsprozesses beschränken dürfe. Ein solch enges Verständnis ist jedenfalls nach der DSGVO nicht aufrecht zu halten – vielmehr ist dem Auftragsverarbeiter ein gewisser Spielraum beispielsweise über die eingesetzten Mittel einzuräumen, ohne dass er dadurch automatisch zum Verantwortlichen wird. [11]

Die DSGVO eröffnet zum einen bei der Frage der Abgrenzung zur „Joint controllership" weitreichende Möglichkeiten der Ausgestaltung arbeitsteiliger Datenverarbeitungsprozesse und bietet zum anderen die Möglichkeit, das gesetzlich nicht geregelte, bisher aber regelmäßig zur Abgrenzung herangezogene Institut der Funktionsübertragung einer kritischen Prüfung zu unterziehen. Es ist davon auszugehen, dass nach der DSGVO bisherige Fälle der Funktionsübertragung auch künftig in den meisten Fällen als Verarbeitung durch zwei verschiedene Verantwortliche oder als „Joint controllership" mit gemeinsamer Verantwortung nach Art. 26 DSGVO angesehen werden. Eine Auftragsverarbeitung wird in diesen Fällen nur dann vorliegen, wenn es sich um eine weisungsgebundene Tätigkeit des Auftragsverarbeiters handelt und die Verantwortung – unter Einräumung der o. g. Spielräume – beim Verantwortlichen verbleibt.

---

11 Kommentar Gola zur DS-GVO Art. 28 Rn. 3
Kommentar Gola zur DS-GVO Art. 28 Rn. 5; Hartung in Kühling/Buchner DS-GVO (2017) Art. 28 Rn. 44.

Auch künftig ist die Wartung von Datenverarbeitungsanlagen und Verfahren durch externe Dienstleister 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 hat.

Auch nach dem neuen europäischen Datenschutzrecht bietet die Auftragsverarbeitung den Vorteil, dass es innerhalb des Verarbeitungsverhältnisses für eine Weitergabe von Daten keiner eigenen Rechtsgrundlage, keines Erlaubnistatbestands bedarf – vielmehr wird der Auftragsverarbeiter datenschutzrechtlich auch weiterhin nicht als Dritter, sondern als der „verlängerte Arm“ und quasi interne Stelle des Verantwortlichen ohne eigenen Wertungs- und Entscheidungsspielraum betrachtet.[12] Der datenschutzrechtliche Erlaubnistatbestand, auf den sich der Verantwortliche beruft, gilt ebenso für den Auftragsverarbeiter.

Wie eingangs erwähnt, ist eine wesentliche Änderung bei der Auftragsverarbeitung die nunmehr beim Auftragsverarbeiter liegende (Mit-)Verantwortung für die Einhaltung der technisch-organisatorischen Maßnahmen. Der Auftragsverarbeiter muss hinreichend Garantien dafür bieten, dass die von ihm getroffenen technischen und organisatorischen Maßnahmen einen wirksamen Schutz der Daten bieten; sie setzen 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 sie vor, führt dies jedoch noch nicht zwingend zum Nachweis der Einhaltung der Garantien der DSGVO, es stellt jedoch einen „Faktor“ für die Beurteilung dar.[13]

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

12 Kommentar Plath zur DS-GVO Art. 28 Rn. 2

13 Kommentar Plath zur DS-GVO Art. 28 Rn. 15

im Gesetzestext auf die Möglichkeit der elektronischen Form (z. B. per E-Mail bzw. online)[14] hingewiesen sowie auf die Möglichkeit, die Auftragsverarbeitung auf Grundlage eines anderen Rechtsinstrumentes durchzuführen. Daraus ist zu schließen, dass hier die Textform 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 Satz 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[15]. Auch hier ist daher die Textform als ausreichend anzusehen.

Im Übrigen bedarf die Einschaltung von Unterauftragsverarbeitern gem. 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 Auftragsverarbeiter – 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.

1.6.2 Bestandsaufnahme, Prüfung bestehender Verträge und Erfordernis von Anpassungen an die Regelungen der DSGVO

In Deutschland – insbesondere im Bereich der Bundesverwaltung – dürften für alle Auftragsdatenverarbeitungen schriftliche Verträge mit den jeweiligen Auftragnehmern vorliegen. Hieraus ergibt sich für die Praxis die Frage, ob bestehende Auftragsdaten-Verarbeitungsverträge, die unter der Geltung des BDSG (alt) abgeschlossen worden sind, auch unter der DSGVO weiter verwendet werden dürfen. Hierauf lässt sich keine pauschale Antwort geben. Vielmehr wird es erforderlich sein, jeden bestehenden Vertrag daraufhin zu prüfen, ob er den Vorgaben der DSGVO genügt.[16] Hierbei sind insbesondere

- die Umsetzung der sicherheitstechnischen Anforderungen der DSGVO
- die Umsetzung der organisatorischen Anforderungen der DSGVO

14 Kommentar Plath zur DS-GVO Art. 28 Rn. 17
15 Kommentar Plath zur DS-GVO Art. 28 Rn. 9
16 Kommentar Plath zur DS-GVO Art. 28 Rn. 13

- die vorhandenen Regelungen zur Vertraulichkeit oder gesetzlichen Verschwiegenheit
- die Bestimmungen bzgl. Unterauftragsverhältnissen
- die Informationspflichten:
  - die Hinweispflicht seitens des Auftragsverarbeiters bei rechtswidrigen Weisungen durch den Auftraggeber / Verantwortlichen
  - die Hinweispflicht des Auftragsverarbeiters bzgl. Übermittlung in ein Drittland
- die Dokumentationspflichten des Auftragsverarbeiters:
  - die Dokumentation bzgl. des Verzeichnisses von Verarbeitungstätigkeiten
  - die Dokumentationspflicht hinsichtlich der Weisungen
- die Unterstützungspflichten des Auftragsverarbeiters:
  - die Dokumentation bzgl. des Verzeichnisses von Verarbeitungstätigkeiten durch den Auftraggeber/ Verantwortlichen
  - bei der Zusammenarbeit mit den Aufsichtsbehörden
  - bei der Meldung von Datenpannen
  - bei der Datenschutz-Folgenabschätzung
  - bei Prüfungen durch den Verantwortlichen oder dessen Beauftragten
- der Umgang mit der Datenverarbeitung in einem Drittland, insbesondere der diesbezüglichen Weisungsabhängigkeit des Auftragsverarbeiters
- die Pflicht zur Rückgabe bzw. Löschung ggf. vom Auftraggeber 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, d. h.
  - der Art und 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 Auftragsverarbeiter

überprüft werden[17].

17 Empfehlungen zur Datenverarbeitung im Auftrag im Gesundheitswesen (DKG, BVD, GMDS, GDD und bvitg) vom 14.06.2017, Ziff. 7

1.6.3 Neuabschluss von Verträgen zur Auftragsverarbeitung

Für künftige, neue Verträge von Auftragsverarbeitungen nach der DSGVO 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. Nach derzeitigem Stand ist nicht abzusehen, ob und wann solche standardisierten Vertragsklauseln vorliegen und verwendet werden können.

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

2 Behördliche Datenschutzbeauftragte (bDSB)

2.1 Regelungen der DSGVO für den bDSB

2.1.1 Bestellung / Rechtsstellung des bDSB

Alle öffentlichen Stellen des Bundes sind gem. Art. 37 Abs. 1 Buchst. a) DSGVO unmittelbar verpflichtet, einen bDSB zu benennen. Ausgenommen hiervon sind Gerichte und unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit.[18] Um einen Gleichklang der Regelungen zu den bDSB auch für solche öffentlichen Stellen des Bundes herzustellen, die nicht unter den Anwendungsbereich der DSGVO fallen, finden sich in den §§ 5 bis 7 BDSG mit den Art. 37 bis 39 DSGVO identische Regelungen.

Der bDSB 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. Die Anforderungen sind daher mit den bisherigen Anforderungen an die Fachkunde weitgehend identisch.

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

Während der bDSB bisher der Leitung der öffentlichen Stelle unmittelbar zu unterstellen war, verlangen Art. 38 Abs. 3 Satz 3 DSGVO und § 6 Abs. 3 Satz 2 BDSG, dass der bDSB unmittelbar der höchsten Leitungsebene berichtet. Daraus folgt faktisch, dass er wie bisher in dieser Funktion unmittelbar der Behördenleitung zu unterstellen ist. Die Aufgaben des bDSB sind im Geschäftsverteilungsplan sowie der Geschäftsordnung der verantwortlichen Stelle darzustellen.

Wie schon nach der bisherigen Rechtslage muss der Verantwortliche (bzw. der Auftragsverarbeiter) gem. Art. 38 Abs. 3 Satz 1 DSGVO / § 6 Abs. 3 Satz 1 BDSG sicherstellen, dass der

18 Soweit es um Verwaltungstätigkeiten geht, unterliegen auch die Gerichte und unabhängige Justizbehörden der Pflicht zur Benennung eines bDSB (vgl. § 7 Abs. 1 BDSG -neu-).

bDSB bei der Erfüllung seiner Aufgaben keine Anweisungen erhält. Er muss also seiner Funktion unabhängig und ohne sachfremde Einflussnahme nachkommen können.

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

Neben der sehr eingeschränkten Möglichkeit, den bDSB abzuberufen, besteht außerdem ein strenger arbeitsrechtlicher Kündigungsschutz. Dieser ist als arbeitsrechtliche Vorschrift nicht in der DSGVO, wohl aber wie bisher im BDSG (§ 6 Abs. 4 Sätze 2 und 3) geregelt. Danach ist eine Kündigung des Arbeitsverhältnisses des bDSB unzulässig, wenn nicht Tatsachen vorliegen, die zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Zudem besteht nach dem Ende der Tätigkeit als bDSB ein Jahr Kündigungsschutz, soweit nicht die o. g. Ausnahme vorliegt.

Gem. Art. 38 Abs. 2 DSGVO / § 6 Abs. 2 BDSG stellt die verantwortliche Stelle dem bDSB die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung. Dies bedeutet, dass dem bDSB auch weiterhin die notwendigen Fortbildungen auf Kosten der öffentlichen Stelle des Bundes zu ermöglichen sind.

Der bDSB ist an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden. Die Verschwiegenheitspflicht des bDSB bezieht sich nach § 6 Abs. 5 Satz 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 bDSB Kenntnis von Daten erhält, für die der Leitung der öffentlichen Stelle aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht gem. § 6 Abs. 6 BDSG auch dem bDSB und den ihm unterstellten Beschäftigten zu. Die Vorschrift enthält darüber hinaus ein Beschlagnahmeverbot für die Akten und andere Dokumente des bDSB.

Die öffentliche Stelle stellt dem bDSB die für die Erfüllung seiner Aufgaben erforderlichen Ressourcen zur Verfügung, Art. 38 Abs. 2 DSGVO / § 6 Abs. 2 BDSG. Mit Blick auf die erhöhte Arbeitsbelastung des bDSB 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) ist die Personalausstattung des bDSB in den öffentli-

chen Stellen des Bundes anzupassen. Die bisherige Bemessungsmarge als Grundlage für die Personalausstattung (mindestens 1 Vollzeitstelle ab 1.000 Beschäftigte) ist aufgrund des veränderten Aufgabenkatalogs des bDSB nicht mehr ausreichend. Die BfDI empfiehlt die vollständige Freistellung des bDSB ab einer Anzahl von 500 Beschäftigten.

Die öffentliche Stelle gewährt dem bDSB gem. 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 bDSB bei allen Fragen im Zusammenhang mit dem Schutz personenbezogener Daten, Art. 38 Abs. 1 DSGVO / § 6 Abs. 1 BDSG. Hierzu muss sie sicherstellen, dass die für Datenschutzaufgaben fachlich zuständigen Organisationseinheiten (Fachreferate und Referat „administrativer Datenschutz“) den bDSB 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 bDSB spätere Beanstandungen zu vermeiden. Die Pflicht zur frühzeitigen Einbindung des bDSB verlangt eine Beteiligung bereits in den Phasen der Planung, Ausschreibung und Entwicklung von datenschutzrelevanten Systemen / Verarbeitungen. Es bietet sich an, die Einbindung des bDSB standardmäßig in die entsprechenden Ablaufplanungen (Workflows) zwingend vorzusehen.

Die öffentliche Stelle des Bundes ist gem. Art. 37 Abs. 7 DSGVO / § 5 Abs. 5 BDSG verpflichtet, die Kontaktdaten des bDSB zu veröffentlichen, in das Verzeichnis der Verarbeitungstätigkeiten aufzunehmen und der 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 bDSB ist hingegen nicht notwendig. Bei der Meldung an die BfDI sollte der Name hingegen mitgeteilt werden. Die BfDI wird für die Meldung der Kontaktdaten ein Formular zur Verfügung stellen.

Dem bDSB 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 solcher ist z. B. bei der Übernahme von Aufgaben des administrativen Datenschutzes durch den bDSB gegeben. Er kann aber auch dann gegeben sein, wenn die Übertragung weiterer Aufgaben etwa dazu führt, dass der bDSB gleichzeitig in mehreren Referaten eingesetzt wird oder er in einem Umfang mit anderen Aufgaben belastet wird, dass er seine Funktion nicht mehr nach den eigenen Prioritäten ausüben kann. Es muss jederzeit sichergestellt sein, dass der bDSB diese Funktion nach seinen Prioritäten ausüben

kann. Andere – auch dringliche – Aufgaben müssen dann zurückstehen. Deshalb sollte die Leitung einer öffentlichen Stelle des Bundes bei der Übertragung anderer Aufgaben von vornherein darauf achten, dass solche Konfliktsituationen beherrscht werden können oder besser gar nicht erst entstehen.

2.1.2 Aufgaben des bDSB

Der bDSB hat die Organisationseinheiten der öffentlichen Stelle und die Beschäftigten über ihre datenschutzrechtlichen Pflichten zu unterrichten und zu beraten, Art. 39 Abs. 1 Buchst. a) DSGVO / § 7 Abs. 1 Nr. 1 BDSG. Die Aufgabe schließt das Vorschlagen von Maßnahmen zur Einhaltung bzw. Umsetzung der Datenschutzvorschriften ein. Die Pflicht des bDSB zur Unterrichtung und Beratung schließt auch die Sensibilisierung und damit auch die Schulung der Beschäftigten ein. Schulungen und Fortbildungen der Beschäftigten sind daher eine Aufgabe, die der bDSB nach eigenem Ermessen und dem bestehenden Bedarf durchführen kann. Eine Verpflichtung hierzu hat er jedoch nicht. Eine solche besteht nur für die öffentliche Stelle und folgt aus Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO.

Eine der wichtigsten Aufgaben des bDSB ist die Überwachung und Einhaltung der datenschutzrechtlichen Vorschriften gem. Art. 39 Abs. 1 Buchst. b) DSGVO / § 7 Abs. 1 Nr. 2 BDSG. Bei der dem bDSB 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. Schließlich gehört dazu auch die Überwachung der Durchführung von notwendigen Schulungen der Beschäftigten. Der bDSB 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 bDSB im Übrigen beratend hinzugezogen werden.

Die öffentliche Stelle muss dafür sorgen, dass der bDSB bei Datenschutz-Folgenabschätzungen zu Rate gezogen wird. Der bDSB hat die DSFA nach Art. 39 Abs. 1 Buchst. c) DSGVO / § 7 Abs. 1 Nr. 3 BDSG zu überwachen. Anders als bei der bisherigen Vorabkontrolle muss er die DSFA hingegen nicht selbst durchführen.

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

Auch für die Tätigkeit des bDSB gilt der so genannte risikobasierte Ansatz. Der bDSB 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 bDSB mit der BfDI / Anlaufstelle für die BfDI

Während der bDSB nach dem alten BDSG eine rein intern wirkende Kontrollinstanz war, obliegt ihm nach Art. 39 Abs. 1 Buchst. d) DSGVO / § 7 Abs. 1 Nummer 4 BDSG die Aufgabe der umfassenden Kooperation mit der Aufsichtsbehörde. Der bDSB hat hierdurch die Befugnis zum Außenkontakt mit der Aufsichtsbehörde erhalten. Aufgrund der Funktion des bDSB als Anlaufstelle ist die 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. Sie kann sich vielmehr unmittelbar mit dem bDSB in Verbindung setzen. Soweit sich die BfDI unmittelbar mit der öffentlichen Stelle in Verbindung setzt, unterrichtet sie hierüber den bDSB in der Regel nachrichtlich. Darüber hinaus hat der bDSB die BfDI bei allen Fragen im Zusammenhang mit der Umsetzung des Datenschutzes in der verantwortlichen Stelle zu beraten, wenn diese einen konkreten Beratungswunsch äußert.

2.3 Verantwortlichkeitsverteilung bDSB – Verantwortlicher

Adressat der Pflichten aus der DSGVO bzw. dem BDSG ist der Verantwortliche, also die öffentliche Stelle des Bundes, nicht der bDSB. 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 bDSB ist es, den Verantwortlichen und dessen Beschäftigte hinsichtlich seiner datenschutzrechtlichen Pflichten zu beraten bzw. zu unterrichten sowie deren Einhaltung 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 bDSB wenden können.

Die Wahrnehmung der Datenschutzbelange ist durch die öffentliche Stelle aufbauorganisatorisch bei der jeweiligen Fachaufgabe anzusiedeln. Nicht aufgabenakzessorische Datenschutzaufgaben sollten als Auffangzuständigkeit (administrativer Datenschutz bzw. Fachaufgabe Datenschutz) bei einer Organisationseinheit angesiedelt werden. Der bDSB ist von allen Organisationseinheiten, die aufgabenakzessorisch datenschutzrelevante Vorgänge bearbeiten sowie von der für die Fachaufgabe Datenschutz zuständigen Organisationseinheit ordnungsgemäß und frühzeitig zu beteiligen. Der bDSB gibt seine Stellungnahmen im Rahmen der Beteiligung (Einbindung) immer unmittelbar gegenüber den o. g. Organisationseinheiten ab.

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 künftig 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 Erwägungsgrund 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). Wie bisher gilt es darüber hinaus auch dann nicht, wenn es andere 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 und Regelungsoptionen, von denen der Mitgliedstaat Gebrauch machen kann oder nicht. Zu ersteren gehören insbesondere die Vorschriften über die 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 gem. 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 konkre-

tisieren. Dem trägt das bereichsspezifische materielle Datenschutzrecht Rechnung, das in seiner Substanz im Wesentlichen erhalten bleiben kann.

Zusammenfassend lässt sich festhalten, dass die Rechtmäßigkeit der Verarbeitung personenbezogener Daten wegen ihres Anwendungsvorrangs zuerst nach der DSGVO zu beurteilen ist. Lässt diese einen Regelungsspielraum, ist in einem weiteren Schritt zu prüfen, ob es bereichsspezifisches Datenschutzrecht gibt, z. B. im SGB X, in der AO oder im 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 für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten personenbezogene Daten 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 BKA, die Bundespolizei, der Generalbundesanwalt, das Zollkriminalamt oder die Tätigkeit anderer öffentlicher Stellen als Verwaltungsbehörde im Sinne des Ordnungswidrigkeitenrechts. Da die Richtlinie nicht unmittelbar geltendes Recht ist, muss 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

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, den Bereich Verteidigung oder besondere Verfassungsorgane wie den parlamentarischen Bereich des Deutschen Bundestages. Sofern kein vorrangiges bereichsspezifisches Datenschutzrecht besteht (z. B. BVerfSchG, BNDG, MADG oder G10), gelten die Vorschriften der Teile 1 und 4 des neuen BDSG. Außerdem gelten gem. § 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 Absatz 1 Satz 1 Buchst. 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

Für die Verarbeitung personenbezogener Daten durch öffentliche Stellen kommen in erster Linie Art. 6 Abs. 1 Satz 1 Buchst. c) und e) DSGVO als Rechtsgrundlage in Frage. Art. 6 Abs. 1 Satz 1 Buchst. 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 auch personenbezogener Daten nach dem Informationsfreiheitsgesetz. Art. 6 Abs. 1 Satz Buchst. 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 Satz 1 Buchst. 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. Dies entspricht sehr weitgehend der Struktur der §§ 12 ff. des BDSG (alt). Art. 6 Abs. 1 Satz 1 Buchst. e) verankert insbesondere das aus dem Verhältnismäßigkeitsgrundsatz folgende Erforderlichkeitsprinzip.

Ergänzend regelt Art. 6 Abs. 3 DSGVO, dass sich in den Fällen der Buchst. c) und e) des Art. 6 Abs. 1 Satz 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 Satz 1 Buchst. c) und e) nicht notwendig ist. Wie bereits oben

(unter 4.1) dargestellt, wird sich die Rechtsgrundlage für eine Verarbeitung personenbezogener Daten weiterhin aus dem bereichsspezifischen Datenschutzrecht und subsidiär aus § 3 BDSG ergeben.

Auch künftig kommt für die Verarbeitung personenbezogener Daten durch öffentliche Stellen die Einwilligung des Betroffenen gem. Art. 6 Abs. 1 Satz 1 Buchst. a) DSGVO in Betracht. Wie bisher ist dieses Instrument im öffentlichen Bereich allerdings mit großer Zurückhaltung anzuwenden. Eine Einwilligung ist nur wirksam, wenn sie freiwillig erteilt worden ist, Art. 4 Nr. 11 DSGVO. Eine 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. Aus diesem Grunde besteht in der Regel ein klares Ungleichgewicht zwischen dem Verantwortlichen und der betroffenen Person, sodass gem. Erwägungsgrund 43 eine Einwilligung gegenüber Behörden in der Regel als Rechtsgrundlage ausscheidet. Im Ausnahmefall kann eine Einwilligung aber durchaus als Rechtsgrundlage dienen, sofern 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 bspw. auch über die Homepage zugänglich sind. Hier kann die betroffene Person frei entscheiden, ob sie ein solches Angebot einer Behörde nutzen will oder nicht, ohne irgendwelche Nachteile befürchten zu müssen. Auch im Beschäftigtenverhältnis können Einwilligungen unter bestimmten Umständen als freiwillig angesehen werden (s. u. 4.3). Wird die Verarbeitung auf eine Einwilligung gestützt, ist unter anderem zu beachten, dass deren Erteilung gem. 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 Satz 1 Buchst. 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 um den Schutz höchstpersönlicher Rechtsgüter wie Leben oder körperliche Unversehrtheit geht und eine andere Rechtsgrundlage (z. B. die Einwilligung oder eine Rechtsgrundlage i. S. v. Art. 6 Abs. 1 Satz 1 Buchst. c) oder e) DSGVO) nicht in Betracht kommt.

Weiterhin kann die Verarbeitung personenbezogener Daten auch im öffentlichen Bereich auf Art. 6 Abs. 1 Satz 1 Buchst. b) DSGVO gestützt werden. Diese Vorschrift erlaubt die Verar-

beitung 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 Satz 1 Buchst. 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 Satz 1 Buchst. 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 Satz 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.

3.3 Beschäftigtendatenschutz

3.3.1 Beschäftigtendatenschutz gem. 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. Gem. 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 menschliche Würde 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 (neu) eine nationale Regelung für den Beschäftigungsdatenschutz geschaffen, die die bisherige Regelung in § 32 BDSG (alt) ablösen wird. Soweit § 26 BDSG (neu) 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 (Satz 1) sowie zur Aufdeckung von Straftaten (Satz 2).

Welche Personengruppen vom Begriff des „Beschäftigten" erfasst sind, gibt § 26 Abs. 8 BDSG vor, wobei der nationale Gesetzgeber hierbei im Wesentlichen den Katalog aus § 3 Abs. 11 BDSG (alt) übernommen hat, der den Begriff der Beschäftigten definiert. Neu ist insoweit die Klarstellung, dass der Leiharbeitnehmer im Verhältnis zum Entleiher als Beschäftigter i. S. d. § 26 BDSG einzuordnen ist. Dies war nach bisheriger Rechtslage umstritten.

§ 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 Arten personenbezogener Daten 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 Änderungen gegenüber § 32 BDSG (alt)

§ 26 BDSG orientiert sich inhaltlich im Wesentlichen an der Vorgängerregelung in § 32 BDSG (alt). Dabei knüpft § 26 Abs. 1 Satz 1 BDSG mit den Erlaubnistatbeständen für die Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses an § 32 Abs. 1 Satz 1 BDSG (alt) an, während § 26 Abs. 1 Satz 2 BDSG die bislang in § 32 Abs. 1 Satz 2 BDSG (alt) enthaltene Regelung zur Datenverarbeitung für Zwecke der Aufdeckung von Straftaten im Beschäftigungsverhältnis fortführt.

Neu ist hingegen die in § 26 Abs. 1 Satz 1 BDSG hervorgehobene Möglichkeit der Datenverarbeitung zur Ausübung oder Erfüllung gesetzlicher oder kollektivvertraglicher Rechte und Pflichten der Interessenvertretungen.

Unter Geltung des BDSG (alt) war bislang umstritten, ob der Arbeitnehmer wirksam in die Verarbeitung seiner personenbezogenen Daten einwilligen kann. § 26 BDSG stellt nunmehr klar, dass die Einwilligung grundsätzlich auch im Beschäftigungsverhältnis möglich ist und konkretisiert die Anforderungen an eine wirksame Einwilligung unter Verweis auf die besonders zu berücksichtigende Freiwilligkeit der Einwilligung. Hinsichtlich der Einwilligung Beschäftigter in die Verarbeitung besonderer Kategorien personenbezogener Daten setzt § 26 Abs. 3 BDSG voraus, dass sich die Einwilligung ausdrücklich auf diese Daten bezieht. Über den Verweis auf die entsprechende Anwendung des § 22 Abs. 2 BDSG ist der Verantwortliche dazu verpflichtet, angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen.

Unverändert ist gem. § 26 Abs. 6 BDSG die Feststellung, dass die Beteiligungsrechte der Interessenvertretungen unberührt bleiben. § 26 Abs. 6 BDSG führt insofern die Regelung in § 32 Abs. 3 BDSG (alt) fort.

3.3.4 Spezifische Regelungen für Beamte

Weitere „spezifische" Vorschriften i. S. d. Art. 88 DSGVO finden sich u.a. in §§ 106 ff. BBG, die personalaktenrechtliche Regelungen enthalten. Wie nach bisheriger Rechtslage gilt auch künftig, dass spezielle bundesgesetzliche Datenschutzregelungen den allgemeinen Datenschutzregelungen des BDSG vorgehen.

4 Umsetzung der Betroffenenrechte

Die notwendige Umsetzung der Anforderungen der DSGVO sollte zum Anlass genommen werden, eine Bestandsaufnahme der bisherigen Verfahren zur Gewährleistung der Betroffenenrechte innerhalb der verantwortlichen Stelle durchzuführen. Die internen Prozesse und Verfahren sollten überprüft und gegebenenfalls unter Berücksichtigung der nachstehenden Ausführungen angepasst und erweitert werden.

4.1 Informationspflichten

Nach der DSGVO muss der Verantwortliche geeignete Maßnahmen ergreifen, um der betroffenen Person alle Informationen nach den Artikeln 13 und 14 zu übermitteln. Die betroffene Person muss die Möglichkeit haben, diese Informationen wahrzunehmen. Auch künftig wird zwischen Informationspflichten bei der Direkterhebung (5.1.1) und bei Dritterhebung (5.1.2) unterschieden.

4.1.1 Informationspflicht bei Direkterhebung

Nach Art. 13 DSGVO hat sich der Umfang der zu erteilenden Informationen gegenüber dem sich bisher aus § 4 Abs. 3 BDSG ergeben Umfang erheblich erhöht. Neu sind folgende nach Art. 13 Abs. 1 DSGVO zu erteilenden Informationen:

- Kontaktdaten des Datenschutzbeauftragten
- Rechtsgrundlage für die Verarbeitung personenbezogener Daten einschließlich der Nennung der berechtigten Interessen des Verantwortlichen, falls die Verarbeitung damit nach Art. 6 Absatz 1 Buchst. f) DSGVO begründet wird
- falls Daten in Drittländer übermittelt werden, die geeigneten Garantien zum Schutz der Daten

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
- ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für eine Vertragsabschluss erforderlich ist
- sofern einschlägig: die Vornahme einer automatisierten Entscheidungsfindung einschließlich Profiling sowie Information über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der Verarbeitung für die betroffene Person

Daneben sind weiterhin wie nach § 4 Abs. 3 BDSG (alt) der Name und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters, die Zwecke der Datenverarbeitung sowie die Empfänger oder Kategorien von Empfängern mitzuteilen.

Die oben dargestellten Informationen müssen den betroffenen Personen zum Zeitpunkt der Erhebung zur Verfügung gestellt werden. Die DSGVO enthält im Gegensatz zum BDSG (alt) keine Definition des Begriffs des Erhebens. Nach § 3 Abs. 3 BDSG (alt) besteht eine Erhebung von personenbezogenen Daten in einer Aktivität der verantwortlichen Stelle, durch die die erhebende Stelle sich zielgerichtet Kenntnis von den Daten verschafft. Der Begriff des Beschaffens enthält nach der Definition ein aktives und subjektives Element. Daran fehlt es, wenn personenbezogene Daten der verantwortlichen Stelle unaufgefordert ohne deren eigenes Zutun zugeleitet werden, z. B. bei Anfragen und Eingaben von Bürgern bei Behörden. Bisher erfolgt eine Information der betroffenen Personen nach § 4 Abs. 3 BDSG (alt) durch die verantwortlichen Stellen in derartigen Fällen daher in der Regel nicht.

In den Fällen unverlangter Mitteilungen oder der unverlangten Zusendung von personenbezogenen Daten sollte ebenfalls grundsätzlich eine Information der betroffenen Person nach Art. 13 DSGVO erfolgen. Art. 13 DSGVO löst die Informationspflicht bereits durch den Vorgang der Datenerhebung aus. Nach Art. 5 Abs. 1 Buchst. b) DSGVO ist die Erhebung personenbezogener Daten mit der Festlegung der Verarbeitungszwecke verknüpft. Die Erhebung könnte daher auch nach der DSGVO als eine bewusste Handlung der verantwortlichen Stelle verstanden werden, mit der bestimmte personenbezogene Daten erstmals beschafft werden, um sie weiter zu verarbeiten. Andererseits wird 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. 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 (s. 5.1.4). Ebenso kann ein Medienbruch in Kauf genommen werden, z. B. durch eine kurze Erstinformation per E-Mail mit einem Verweis auf weitere Erläuterungen auf einer Homepage.

4.1.2 Datenerhebung bei Dritten

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

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. in einer Übermittlung der personenbezogenen Daten an Dritte liegen.

4.1.4 Ausnahmen

Verfügt die betroffene Person bereits über die Informationen, so bestehen die Informationspflichten nach den Artikeln 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

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 Buchst. a) und Abs. 2 DSGVO).

4.2 Auskunftsrecht

Art. 15 DSGVO sieht wie § 19 BDSG (alt) ein Auskunftsrecht für betroffene Personen vor. Der betroffenen Person ist danach auf Antrag Auskunft zu geben über:

- 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 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. Wie in § 19 Abs. 2 BDSG (alt) besteht nach § 34 Abs. 1 Nr. 2 BDSG 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. In Erweiterung der bisherigen Rechtslage nach § 19 Abs. 2 BDSG (alt) hat der Verantwortliche jedoch sicherzustellen, dass durch geeignete 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 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

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 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 Buchst. 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 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 Buchst. 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. Dies entspricht § 20 Abs. 2 Nr. 2 BDSG (alt), wonach die Löschungspflicht besteht, wenn die Kenntnis der Daten zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben nicht mehr erforderlich ist. Nach den übrigen in Art. 17 Abs. 1 Buchst. 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 Buchst. b) bis f) DSGVO genannten Fälle ist eine weitere Speicherung der Daten unzulässig, so dass inhaltlich keine wesentlichen Änderungen gegenüber der bisher in § 20 Abs. 2 Nr. 1 BDSG (alt) geregelten Löschungspflicht bestehen.

Neu ist hingegen 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 Implementierungskosten 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 Buchst. e) i.V.m. Art. 6 Abs. 1 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.

4.5 Recht auf Einschränkung der Verarbeitung

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. Diese Definition entspricht der Definition des Sperrens in § 3 Abs. 4 Nr. 4 BDSG (alt). 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 Sperrung 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. Dieser Fall entspricht dem Tatbestand des § 20 Abs. 3 Nr. 2 BDSG (alt), wonach personenbezogene Daten zu sperren sind, wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden. 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 Buchst. 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 gem. Art. 21 DSGVO eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Die bisher in § 20 Abs. 3 Nr. 1 und 3 BDSG (alt) für öffentliche Stellen geregelten Sperrverpflichtungen sind in Art. 18 DSGVO nicht mehr enthalten. Dies betrifft die Sperrung, soweit einer Löschung Aufbewahrungsfristen entgegenstehen, die sich aus Gesetzen, Satzungen oder Verträgen ergeben. In diesen Fällen ist jedoch ohnehin eine weitere Verarbeitung nach Art. 6 i. V. m. Art. 5 Abs. 5 Buchst. b) DSGVO nur für 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. Diese Ausnahme ist jedoch wie in der bisherigen Regelung in § 20 Abs. 3 Nr. 3 BDSG (alt) in § 35 Abs. 1 BDSG aufgenommen worden.

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

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 die Information unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden wäre. Die Vorschrift entspricht der in § 20 Abs. 8 BDSG (alt) geregelten Mitteilungspflicht durch den Verantwortlichen. Allerdings entfällt im Gegensatz zu dieser Regelung die Mitteilungspflicht nicht mehr, 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

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. Das Widerspruchsrecht aus Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben, ist für Datenverarbeitungen durch öffentliche Stellen des Bundes bisher in § 20 Abs. 5 Satz 1 BDSG (alt) geregelt. 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 wie bisher auch künftig 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 Satz 1 DSGVO, § 36 BDSG).

4.8 Automatisierte Einzelfallentscheidung

Die Regelung in § 6a BDSG (alt) zu automatisierten Einzelentscheidungen wird durch Art. 22 DSGVO erweitert. 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. Das 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

Zur Gewährleistung der Betroffenenrechte sind durch die verantwortlichen Stellen technische und organisatorische Maßnahmen zu ergreifen, die in behördeneigenen Datenschutzrichtlinien abgebildet werden sollten. Dazu gehören neben der Festlegung von Zu-

ständigkeiten 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.

Nach der DSGVO (Erwägungsgrund 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 gegebenenfalls begründen, warum der Antrag abgelehnt wird. Alle Informationen und alle Mitteilungen an die betroffene Person, die sich auf die Verarbeitung ihrer personenbezogenen Daten beziehen, müssen in transparenter, verständlicher und leicht zugänglicher Form erfolgen.