Senatsverwaltung
für Inneres und Sport

Berlin

# Anwendungshinweise

zur

Neugestaltung des Datenschutzrechts

im Zusammenhang mit der

Datenschutz-Grundverordnung

Stand: 03.09.2018

Inhalt

## 1. Vorwort

Die vorliegenden Anwendungshinweise sollen einen Überblick über einige wesentliche Regelungen geben, die auf den seit Mai 2018 anzuwendenden europäischen Datenschutzregelungen und der hierzu vorgenommenen Anpassung des Berliner Datenschutzgesetzes beruhen. Für viele Fragen im Zusammenhang mit den neuen Regelungen existiert noch keine Rechtsprechung, so dass eine Auslegung dieser Regelungen, wie sie auch in den nachfolgenden Ausführungen vorgenommen wird, erforderlich ist.

Die Anwendungshinweise orientieren sich mit dessen freundlicher Genehmigung an den Anwendungshinweisen des Ministeriums des Innern und für Kommunales Brandenburg. Im Rahmen der Ausführungen wird an einigen Stellen eine eigene Auslegung der neuen Regelungen vorgenommen.

Die europäischen Regelungen machen eine umfassende Prüfung und gegebenenfalls Anpassung der Datenschutzregelungen in allen Rechtsnormen der Mitgliedsstaaten erforderlich. Nach einer grundlegenden Anpassung des allgemeinen Datenschutzrechts, auf Bundesebene durch die Neufassung des Bundesdatenschutzgesetzes im Jahr 2017 und in Berlin durch die Neufassung des Berliner Datenschutzgesetzes vom 13. Juni 2018, erfolgt gegenwärtig auf Bundesebene und in den Bundesländern die Anpassung der besonderen datenschutzrechtlichen Regelungen in den bereichsspezifischen Gesetzen und untergesetzlichen Regelungen.

Die Aktualisierung der Anwendungshinweise aufgrund fortschreitender Erkenntnisse im Rahmen der Anwendung der neuen Datenschutzregelungen bleibt vorbehalten. Die jeweils aktuelle Version wird auf der Internetseite der Senatsverwaltung für Inneres und Sport veröffentlicht: (https://www.berlin.de/sen/inneres/buerger-und-staat/datenschutz-und-informationsfreiheit/datenschutz/artikel.30301.php).

Ergänzend zu den in diesen Hinweisen enthaltenen Informationen wird auf die Veröffentlichungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hingewiesen, die unter dem folgenden Link abgerufen werden können:

https://www.datenschutz-berlin.de/kurzpapiere.html.

## 2. Einführung

### 2.1 Die Datenschutzreform der Europäischen Union

#### 2.1.1 Die Datenschutz-Grundverordnung

Im Jahr 2016 wurde das Datenschutzrecht auf europäischer Ebene reformiert, indem die bisherige Datenschutz-Richtlinie 95/46/EG durch die Datenschutz-Grundverordnung[1] (DSGVO) ersetzt wurde. Zugleich wurde eine zweijährige Übergangsfrist vorgesehen, in der sich die Rechtsunterworfenen auf die neuen Regelungen einstellen und die Mitgliedstaaten ihre Rechtsvorschriften anpassen konnten. Seit dem 25. Mai 2018 gibt die DSGVO die wesentlichen Rechte und Pflichten in Bezug auf den Datenschutz vor. Als europäische Verordnung ist die DSGVO in allen Mitgliedstaaten der EU unmittelbar geltendes Recht und gilt

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

unter anderem auch für die öffentlichen Stellen des Landes Berlin. Die DSGVO genießt Anwendungsvorrang gegenüber nationalem Recht, so dass Regelungen in Gesetzen, Rechtsverordnungen, Verwaltungsvorschriften etc., die den Vorgaben der DSGVO widersprechen, nicht mehr angewendet werden dürfen (dazu nachfolgend Ziffer 2.1.1.2).

Zur Berücksichtigung von Besonderheiten in den Mitgliedstaaten enthält die DSGVO an einigen Stellen die Möglichkeit, Abweichungen von einzelnen Regelungen vorsehen zu können. Die Abweichungen werden in den Mitgliedstaaten durch Rechtsvorschriften vorgenommen. Zudem enthält die DSGVO konkrete Regelungsaufträge, die von den Mitgliedstaaten umzusetzen sind.

#### 2.1.1.1 Der Anwendungsbereich der DSGVO

Der sachliche Anwendungsbereich der DSGVO ist in deren Artikel 2 geregelt. Danach gilt die DSGVO für die automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Der Begriff des Dateisystems wird in Artikel 4 Nummer 6 DSGVO definiert. Darunter ist jede strukturierte Sammlung personenbezogener Daten zu verstehen, die nach bestimmten Kriterien (z.B. Aktenzeichen, Jahreszahl, Thema, Name oder auch nur eine fortlaufende Nummerierung) zugänglich ist. Aus der Verwendung des Plurals in Artikel 4 Nummer 6 DSGVO (Kriterien) kann abgeleitet werden, dass zumindest zwei Kriterien für eine Strukturierung vorliegen müssen. Dabei wird der Anwendungsbereich der DSGVO technikneutral sehr weit gefasst. Auch Schriftstücke oder Zettel mit personenbezogenen Daten, die noch unsortiert in einer Ablage aufbewahrt werden, fallen bereits dann unter den Anwendungsbereich der DSGVO, wenn sie später in eine entsprechende Akte einsortiert werden sollen. Lediglich Akten oder Aktensammlungen, die nicht nach bestimmten Kriterien geordnet sind, fallen nicht in den Anwendungsbereich der DSGVO (vgl. Erwägungsgrund 15 DSGVO). Für die praktische Anwendung ist die Frage, ob personenbezogene Daten wegen Speicherung in einem Dateisystem den Regelungen der DSGVO unterfallen, jedoch nicht von Relevanz. Denn die Verarbeitung personenbezogener Daten, die nicht in einem Dateisystem gespeichert werden sollen, durch öffentliche Stellen, fällt jedenfalls in den Anwendungsbereich des BlnDSG, welches in § 2 Absatz 9 eine entsprechende Anwendung der DSGVO anordnet.

Darüber hinaus wird der Anwendungsbereich der DSGVO in deren Artikel 2 Absatz 2 negativ abgegrenzt. Insbesondere fallen nicht in den Anwendungsbereich:

- Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen (z.B. Tätigkeit der Abgeordneten im Abgeordnetenhaus, Tätigkeit der Verfassungsschutzbehörde),
- Tätigkeiten, die die gemeinsame Außen- und Sicherheitspolitik der Mitgliedstaaten betreffen (Anwendungsbereich von Titel V, Kapitel 2 des Vertrags der Europäischen Union),
- ausschließlich persönliche oder familiäre Tätigkeiten natürlicher Personen,
- die Verarbeitung personenbezogener Daten im Zusammenhang mit Straf- und Ordnungswidrigkeitenverfahren (dazu nachfolgend Ziffer 2.1.2).

Die DSGVO enthält neben ihren 99 Artikeln auch insgesamt 173 Erwägungsgründe, die den Artikeln vorangestellt sind. Die Erwägungsgründe dienen in erster Linie der Begründung der einzelnen Verordnungsnormen. Aus ihnen können direkt zwar keine Rechte und

Pflichten abgeleitet werden, allerdings dienen sie der Auslegung der einzelnen Artikel und bestimmen so Zweck, Reichweite und Inhalt der einzelnen Artikel mit.

- Eine Übersicht, welche Erwägungsgründe welchen Artikeln zugeordnet sind, enthält Anlage 1.

#### 2.1.1.2 Der Anwendungsvorrang der DSGVO

Da die DSGVO unmittelbar, also ohne weiteren Umsetzungsakt gilt, ist sie künftig innerhalb ihres Anwendungsbereiches die zentrale Vorschrift für den Datenschutz. Allerdings gibt es auch ergänzende bundes- oder landesrechtliche Vorschriften über den Datenschutz. In Berlin ergänzt insbesondere das BlnDSG (BlnDSG) die DSGVO um allgemeine datenschutzrechtliche Regelungen. Andere spezielle datenschutzrechtliche Regelungen bleiben grundsätzlich erhalten und müssen erforderlichenfalls an die DSGVO angepasst werden.

Für die Rechtsanwendung folgt daraus:

- Das Verständnis datenschutzrechtlicher Begriffe ergibt sich im Wesentlichen aus den Definitionen der DSGVO (vor allem aus Artikel 4 und 9 Absatz 1 DSGVO), zum Teil enthält das BlnDSG spezifische Definitionen (dazu nachfolgend Ziffer 4).
- Die Pflichten, die den öffentlichen Stellen als Verantwortliche (dazu nachfolgend Ziffer 3) für die Verarbeitung personenbezogener Daten obliegen, sind im Wesentlichen in der DSGVO verankert (siehe insbesondere Artikel 5, 24 ff., 32 ff. DSGVO). Ergänzende Pflichten können auch aus dem BlnDSG oder aus anderen Gesetzen folgen.
- Gleichzeitig sind auch die Rechte der betroffenen Personen im Wesentlichen unmittelbar in der DSGVO normiert. Ausnahmen von diesen Rechten enthält entweder die DSGVO selbst oder sie können in engen Grenzen durch nationale Gesetze, Rechtsverordnungen oder Satzungen zugelassen sein. Zusätzliche Rechte können sich aus nationalem Recht ergeben (z.B. das Recht auf Akteneinsicht in § 24 Absatz 6 BlnDSG).
- Ausgangspunkt der Prüfung, ob eine Verarbeitung personenbezogener Daten rechtmäßig erfolgt, wird künftig Artikel 6 Absatz 1 DSGVO sein. Eine Ausnahme besteht, wenn besondere Kategorien personenbezogener Daten Gegenstand der Verarbeitung sind. Insoweit enthält Artikel 9 DSGVO neben der Definition der besonderen Kategorien auch besondere Anforderungen und Rechtsgrundlagen (jeweils in Verbindung mit Artikel 6 DSGVO) an bzw. für die Verarbeitung. Wie sich die Prüfungsreihenfolge im Zusammenspiel mit nationalen spezialgesetzlichen Regelungen gestaltet, wird nachfolgend unter Ziffer 5 dargestellt.
- Soweit die Verarbeitung auf einer Einwilligung der betroffenen Person beruht, ergeben sich die Bedingungen für die Einwilligung aus der DSGVO (siehe dazu Artikel 7 und 8 DSGVO und die Ausführungen unter Ziffer 5.1).
- Die DSGVO schreibt für öffentliche Stellen zwingend vor, dass eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter zu benennen ist und legt zugleich die Aufgaben fest (Artikel 37 ff. DSGVO). Das BlnDSG wiederholt in § 4 diese Regelung, um einheitliche Datenschutzstandards auch für diejenigen Berliner Behörden zu schaffen, die nicht dem Anwendungsbereich der DSGVO unterfallen und sieht zusätzlich auch die obligatorische Benennung einer Stellvertretung vor (§ 4 Absatz 3 BlnDSG).

- Die Aufgaben und Befugnisse der Aufsichtsbehörde ergeben sich unmittelbar aus der DSGVO (siehe Artikel 57 und 58 DSGVO). Das BlnDSG wiederholt auch diese Regelungen, für die Schaffung einheitlicher Datenschutzstandards für die Berliner Behörden, die nicht dem Anwendungsbereich der DSGVO unterfallen.
- Soweit Vorschriften des nationalen Rechts identische Regelungen wie die DSGVO enthalten, sind die Maßnahmen auf die Regelungen der DSGVO zu stützen.

### 2.1.2 Die JI-Richtlinie

Wie unter Ziffer 2.1.1.1 bereits erwähnt, unterfällt die Verarbeitung personenbezogener Daten im Zusammenhang mit Strafverfahren nicht der DSGVO. Hintergrund dessen ist, dass im Zusammenhang mit Strafverfahren, insbesondere im Ermittlungsverfahren, die in der DSGVO enthaltenen Rechte und Pflichten durch besondere Regelungen angepasst werden sollen, die sowohl die Rechte und Freiheiten der betroffenen Personen berücksichtigen, gleichzeitig aber auch das Strafverfolgungsinteresse der Allgemeinheit nicht gefährden sollen. Für diese Zwecke enthält die sogenannte JI-Richtlinie[2] die entsprechenden Vorgaben. Anders als die DSGVO gelten diese jedoch nicht unmittelbar, sondern müssen zuvor in nationales Recht übernommen werden. Zur Umsetzung der Vorgaben der JI-Richtlinie wurde im BlnDSG – vergleichbar mit dem Bundesdatenschutzgesetz (BDSG) – ein eigener Teil (Teil 3) aufgenommen, der ausschließlich für die Verarbeitung personenbezogener Daten im Zusammenhang mit Strafverfahren anwendbar ist und quasi ein eigenes Gesetz innerhalb des BlnDSG darstellt.

Der Anwendungsbereich der JI-Richtlinie erfasst jedoch - anders als die Bezeichnung vermuten lässt - nicht nur Straftaten, sondern auch Ordnungswidrigkeiten. Der europarechtliche Begriff der Straftat ist nicht deckungsgleich mit dem deutschen Begriff der Straftat. Während in Deutschland anhand einer gesetzgeberischen Wertung aufgrund des abgestuften sozialethischen Unwertgehalts zwischen Straftaten und Ordnungswidrigkeiten unterschieden wird, erfolgt in anderen EU-Mitgliedstaaten keine solche Unterscheidung. Stattdessen wird dort lediglich zwischen Straftaten und Nicht-Straftaten getrennt, so dass die deutsche Einschränkung auf Straftaten im engeren Sinne den Anwendungsbereich der JI-Richtlinie zu stark einschränken würde, was neben den damit verbundenen Abgrenzungsproblemen auch dem Ziel einer möglichst europaweiten Harmonisierung der Anwendungsbereiche von DSGVO und JI-Richtlinie entgegenstehen würde.

Vorrangig gelten für die Verarbeitung personenbezogener Daten im Zusammenhang mit Straf- oder Ordnungswidrigkeitenverfahren die bereichsspezifischen Regelungen der StPO und des OWiG (Artikel 31 des Grundgesetzes sowie § 2 Absatz 8 BlnDSG) und ergänzend dazu die Regelungen in Teil 3 des BlnDSG (solange der Bundesgesetzgeber durch eine zukünftige Anpassung keine anderweitige Regelung trifft).

## 2.2 Das neue Berliner Datenschutzgesetz

Das bis zum Ablauf des 23.06.2018 geltende BlnDSG (BlnDSG-alt) enthielt an vielen Stellen Regelungen, die sich nunmehr unmittelbar aus der DSGVO ergeben. Wegen des umfangreichen Anpassungsbedarfes an die neuen Datenschutzvorschriften wurde das BlnDSG voll-

[2] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

ständig aufgehoben und neu gefasst. Bei dieser Gelegenheit wurde auch die JI-Richtlinie für die Verarbeitung personenbezogener Daten im Zusammenhang mit Straf- und Ordnungswidrigkeitenverfahren in das Berliner Landesrecht umgesetzt (vgl. dazu Ziffer 2.1.2).

Dem BlnDSG liegt folgende Struktur zugrunde:

Teil 1: Gemeinsame Regelungen

In Teil 1 wurden die Regelungen zusammengefasst, die für Verarbeitungen personenbezogener Daten durch öffentliche Stellen des Landes Berlin gelten, unabhängig davon, ob die Verarbeitung in den Anwendungsbereich der DSGVO oder der JI-Richtlinie fällt oder ob die Verarbeitung personenbezogene Daten betrifft, die in keinen der beiden Anwendungsbereiche fällt.

In § 2 Absatz 9 wird angeordnet, dass die Regelungen der DSGVO und der diese ergänzenden Vorschriften in Teil 2 des BlnDSG entsprechend gelten, wenn personenbezogene Daten verarbeitet werden, auch wenn weder der Anwendungsbereich der DSGVO noch der JI-Richtlinie eröffnet ist. Hierdurch soll ein möglichst einheitliches Datenschutzniveau auch in den Fällen geschaffen werden, in denen die DSGVO nicht unmittelbar gilt. Ein Anwendungsfall dieser Regelung ist beispielsweise die Verarbeitung personenbezogener Daten, die nicht automatisiert erfolgt und bei der auch keine Daten betroffen sind, die in einem Dateisystem gespeichert werden sollen. Bei einer Videoüberwachung nicht-öffentlicher Räume, bei der keine Aufzeichnung, sondern nur eine Beobachtung des Monitorbildes erfolgt, sind deshalb in jedem Fall die Regelungen der DSGVO zu beachten, ohne dass es auf die unterschiedlichen Meinungen ankommt, ob eine solche Videobeobachtung direkt der DSGVO unterfällt oder nicht.

In § 3 wurde eine allgemeine Rechtsgrundlage für die Verarbeitung personenbezogener Daten aufgenommen, die jedoch am 30.06.2020 außer Kraft tritt. Ab dem 01.07.2020 sind bereichsspezifische Rechtsgrundlagen für die Verarbeitung personenbezogener Daten erforderlich. Soweit bereits vor diesem Zeitpunkt bereichsspezifische Rechtsgrundlagen bestehen, ist die Datenverarbeitung vorrangig auf diese zu stützen. Soweit eine ergänzende Heranziehung von § 3 BlnDSG in Erwägung gezogen wird, muss zuvor geprüft werden, ob die bereichsspezifischen Regelungen nicht abschließend sind (§ 2 Absatz 8 BlnDSG).

Teil 1 enthält zudem Regelungen zu den Aufgaben und Befugnissen der Berliner Beauftragten für Datenschutz und Informationsfreiheit und für die behördlichen Datenschutzbeauftragten. Die Regelungen sind weitestgehend identisch mit denjenigen der DSGVO, gelten jedoch durch die Wiederholung im BlnDSG vor allem auch für die Fälle, die in den Anwendungsbereich der JI-Richtlinie fallen.

Teil 2: Durchführungsbestimmungen zur DSGVO

Teil 2 enthält Ergänzungen, Ausnahmen und Durchführungsbestimmungen zur DSGVO. Soweit in Teil 2 nichts anderes geregelt ist, gelten die Regelungen der DSGVO unmittelbar. Aus der systematischen Stellung der Vorschriften in Teil 2 als „Durchführungsbestimmungen zur DSGVO“ ergibt sich, dass die Regelungen im Anwendungsbereich der JI-Richtlinie nicht angewendet werden können. In Einzelfällen wurde im Teil 3 auf Regelungen aus Teil 2 Bezug genommen (§§ 40, 70).

Teil 3: Verarbeitung personenbezogener Daten im Zusammenhang mit Straf-/ Ordnungswidrigkeitenverfahren

Der Teil 3 dient der Umsetzung der JI-Richtlinie und bildet zusammen mit den gemeinsamen Bestimmungen in Teil 1 ein abgeschlossenes Regelungssystem, dem jedoch bereichsspezifische Regelungen, insbesondere in StPO und OWiG, vorgehen. Eine den Teil 3 betreffende Übergangsvorschrift findet sich in Teil 5 in § 72 Absatz 1.

Teil 4: Besondere Verarbeitungssituationen außerhalb des Anwendungsbereichs der DSGVO und der Richtlinie

Teil 4 enthält eine Befugnis zur Verarbeitung personenbezogener Daten im Zusammenhang mit öffentlichen Auszeichnungen und Ehrungen. Diese Tätigkeiten fallen als Teil der den Nationalstaaten vorbehaltenen Staatspflege nicht in den Anwendungsbereich des EU-Rechts.

Teil 5: Schluss-/Übergangsvorschriften

Eine Übersicht, welche Regelungen des BlnDSG-alt durch welche Regelungen in DSGVO, JI-Richtlinie und BlnDSG abgelöst wurden, wird nachfolgend als Anlage 2 auf der Internetseite der Senatsverwaltung für Inneres und Sport veröffentlicht.

### 2.3 Wesentliche Änderungen gegenüber der bisherigen Rechtslage

- Eine zentrale Rolle in der Betrachtung nimmt der Verantwortliche ein, dem die DSGVO zahlreiche Aufgaben und damit verbunden die Verantwortung für die Rechtmäßigkeit des Handelns nach außen zuweist.
- Begriffsbestimmungen ergeben sich zukünftig aus der DSGVO unmittelbar und gehen teilweise über die bisher bekannten Definitionen hinaus.
- Die Zulässigkeit der Verarbeitung personenbezogener Daten beurteilt sich aus einem Zusammenspiel von DSGVO, bereichsspezifischem Recht und dem neuen BlnDSG.
- Die DSGVO enthält teilweise neue bzw. gegenüber dem bisherigen Stand modifizierende verfahrensrechtliche Vorgaben und Dokumentationspflichten.
- Dem (behördlichen) Datenschutzbeauftragten werden konkrete Aufgaben zugewiesen und seine Rolle als Berater des Verantwortlichen klargestellt.
- In Bezug auf den technischen Datenschutz sind die neuen Vorgaben in Bezug auf „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ gemäß Artikel 25 DSGVO zu beachten.
- Die Betroffenenrechte sind erheblich gestärkt und um Informationspflichten bei der Datenerhebung und Zweckänderung ergänzt worden.
- Der Aufsichtsbehörde werden neue Befugnisse übertragen, die bis hin zur Untersagung von Verarbeitungen reichen können.

## 3. Rolle des Verantwortlichen nach den neuen Regelungen

Die DSGVO weist dem Verantwortlichen bei der Verarbeitung personenbezogener Daten eine zentrale Rolle zu. Verantwortlicher ist nach Artikel 4 Nummer 7 DSGVO: „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

Während in Artikel 4 Nummer 7 DSGVO neben den Behörden auch natürliche und juristische Personen genannt werden, geht die JI-Richtlinie in Artikel 3 Nummer 8 davon aus, dass nur Behörden als Verantwortliche in Betracht kommen. Die unterschiedliche Formulierung ist dadurch erklärlich, dass sich die DSGVO, anders als die Richtlinie, auch an nicht-öffentliche Stellen richtet, die eigenverantwortlich personenbezogene Daten verarbeiten (z.B. Selbständige). Die Erstreckung der Pflichten des Verantwortlichen auf natürliche Personen aber auch auf juristische Personen, Einrichtungen oder andere Stellen ist im Anwendungsbereich der DSGVO erforderlich, um einen umfassenden Datenschutz zu gewährleisten.

Aus der Formulierung in Artikel 3 Nummer 8 der Richtlinie, deren Anwendungsbereich Datenverarbeitung zu repressiven Zwecken umfasst, die nur durch staatliche Stellen erfolgt, wird deutlich, dass im öffentlichen Bereich Behörden Adressat der Pflichten des Verantwortlichen sein sollen. Weil in der DSGVO Behörden und natürliche Personen gesondert aufgezählt werden, in der JI-Richtlinie natürliche Personen jedoch fehlen, kann daraus geschlussfolgert werden, dass die Verantwortlichkeit im öffentlichen Bereich keine natürlichen Personen treffen kann, sondern immer nur eine Institution.

Zur Umsetzung von Artikel 3 Nummer 8 der JI-Richtlinie in § 31 Nummer 7 BlnDSG wurde, um Regelungslücken und Auslegungsprobleme zu vermeiden und um dadurch ein hohes Datenschutzniveau zu gewährleisten (vgl. Artikel 1 Absatz 3 JI-Richtlinie), klargestellt, dass die Verantwortlichkeit nicht nur Behörden im engeren, organisatorischen Sinne treffen kann, sondern alle öffentlichen Stellen – mit Ausnahme natürlicher Personen – welche personenbezogene Daten aufgrund ihrer Zuständigkeit zu Zwecken des § 30 BlnDSG verarbeiten.

Der Verantwortliche hat sicherzustellen, dass:

- die materiellen Vorschriften über die Zulässigkeit der Verarbeitung personenbezogener Daten durch die öffentliche Stelle eingehalten werden; die Zulässigkeit der Verarbeitung wird insbesondere in den Artikeln 5, 6 und 9 DSGVO, in den §§ 14 ff. BlnDSG und in bereichsspezifischen Datenschutzvorschriften geregelt;
- die Verfahrensvorschriften der DSGVO und ggf. ergänzender Regelungen beachtet werden; dies gilt z.B. für die Führung des Verzeichnisses von Verarbeitungstätigkeiten nach Artikel 30 DSGVO, die Melde- und Benachrichtigungspflichten nach den Artikeln 33 und 34 DSGVO und die Durchführung von Datenschutz-Folgenabschätzungen nach Artikel 35 DSGVO;
- die datenschutzrechtlichen Informationspflichten nach den Artikeln 13 und 14 DSGVO i.V.m. § 15 Absatz 3 und § 23 BlnDSG erfüllt und die Rechte der Betroffenen beachtet werden (z.B. das Auskunftsrecht nach Artikel 15 DSGVO i.V.m. § 24 BlnDSG, das Recht auf Löschung nach Artikel 17 DSGVO und das Widerspruchsrecht nach Artikel 21 DSGVO),
- geeignete technische und organisatorische Maßnahmen zum Schutz der verarbeiteten Daten und zur Befolgung des Ziels Datenschutz durch Technikgestaltung getroffen werden (Artikel 24, 25 und 32 DSGVO sowie § 26 BlnDSG) und
- geeignete sonstige Datenschutzvorkehrungen getroffen werden (z.B. Datenschutzrichtlinien oder sonstige Datenschutzanweisungen).

Wer die vielfältigen Pflichten des Verantwortlichen in der öffentlichen Stelle konkret erfüllt, also zuständig ist, ist von der Leitung der öffentlichen Stelle festzulegen. Regelmäßig ist da-

bei zwischen zentralen Ansprechpartnern für IT, Organisation und Datenschutz sowie den Fachabteilungen zu unterscheiden. Außerdem sind die Verwaltungsabläufe so zu gestalten, dass die Einhaltung datenschutzrechtlicher Bestimmungen sichergestellt ist (z.B. fristgerechte Erfüllung von Mitteilungs- und Auskunftspflichten). Die Letztverantwortlichkeit verbleibt bei der Leitung der öffentlichen Stelle.

## 4. Begriffe

Die Begriffsbestimmungen ergeben sich zukünftig im Wesentlichen unmittelbar aus Artikel 4 DSGVO. Gegenüber den bisher im BlnDSG verwendeten Begriffen ergeben sich u.a. folgende Änderungen:

| Bisheriger Begriff | Neuer Begriff |
|---|---|
| Betroffener | betroffene Person |
| Sperrung | Einschränkung der Verarbeitung |
| datenverarbeitende Stelle | Verantwortlicher |
| Datei | Dateisystem |
| automatisiertes Abrufverfahren | automatisiertes Verfahren auf Abruf |

Das BlnDSG enthält in einigen Vorschriften spezifische Definitionen, die zum Teil aber bereits im BlnDSG-alt enthalten waren, z.B.:

- § 2 Absatz 1: öffentliche Stelle,
- § 20 Absatz 1: Videoüberwachung,
- § 21 Absatz 1: gemeinsames Verfahren und
- § 22 Absatz 1: Fernmess- und Fernwirkdienste.

Im BlnDSG wird zudem der Begriff *anonymisieren* verwendet. Aus dem Erwägungsgrund 26 DSGVO ergibt sich, dass eine Anonymisierung vorliegt, wenn die betroffene Person nicht oder nicht mehr identifiziert werden kann. In Abgrenzung zur Pseudonymisierung dürfen bei einer Anonymisierung also keine Schlüssel- oder Metainformationen vorliegen, die eine Aufhebung der Trennung zwischen Daten und Person ermöglichen. Da bei einer Anonymisierung der Daten der Personenbezug erlischt, unterfallen diese nicht mehr dem Anwendungsbereich der DSGVO (vgl. Erwägungsgrund 26 DSGVO) oder des BlnDSG.

## 5. Zulässigkeit der Verarbeitung personenbezogener Daten

### 5.1 Verarbeitung aufgrund von Artikel 6 Absatz 1 DSGVO

Wie bisher gilt hinsichtlich der Zulässigkeit der Verarbeitung personenbezogener Daten das Prinzip des Verbots mit Erlaubnisvorbehalt. Die zentrale Vorschrift ist Artikel 6 DSGVO. Artikel 6 Absatz 1 DSGVO enthält einige unmittelbar geltende Erlaubnistatbestände und weitere, welche durch die Mitgliedstaaten jedoch erst zur Geltung gebracht werden müssen:

| Fall des Artikels 6 Absatz 1 Satz 1 DSGVO: | | Folgt die Rechtsgrundlage unmittelbar aus der DSGVO? |
|---|---|---|
| a) | Einwilligung<br>(vgl. auch Artikel 7 und 8 DSGVO) | Ja. |
| b) | Erforderlichkeit für die Erfüllung eines Vertrages | Ja. |
| c) | Erforderlichkeit zur Erfüllung einer rechtlichen Verpflichtung | Nein.<br>Es bedarf einer besonderen Rechtsvorschrift im EU- oder nationalen Recht.<br>(s.a. Artikel 6 Absatz 2, 3 DSGVO) |
| d) | Erforderlichkeit zur Wahrung lebenswichtiger Interessen | Ja. |
| e) | Erforderlichkeit für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt | Nein.<br>Es bedarf einer besonderen Rechtsvorschrift im EU- oder nationalen Recht.<br>(s.a. Artikel 6 Absatz 2, 3 DSGVO) |
| f) | Erforderlichkeit zur Wahrung berechtigter Interessen des Verantwortlichen | Ja. **Gilt jedoch nicht als Erlaubnis für die Verarbeitung personenbezogener Daten im Rahmen der Erfüllung behördlicher Aufgaben!**<br>(Artikel 6 Absatz 1 Satz 2 DSGVO) |

***Zur Verarbeitungsbefugnis aufgrund einer Einwilligung:***

Die Verarbeitung personenbezogener Daten kann gemäß Artikel 6 Absatz 1 Satz 1 Buchstabe a DSGVO auf der Grundlage einer Einwilligung erfolgen. Voraussetzung ist jedoch, dass die Einwilligung wirksam ist. Hierzu müssen bestimmte Voraussetzungen erfüllt sein, die sich aus den Artikeln 4 Nummer 11 und Artikel 7 (ggf. auch aus Artikel 8) DSGVO ergeben. Grundvoraussetzung für eine wirksame Einwilligung ist, dass diese freiwillig erteilt wurde. Die Freiwilligkeit wiederum setzt voraus, dass die betroffene Person Vor- und Nachteile der Entscheidung, in die Verarbeitung personenbezogener Daten einzuwilligen, gegeneinander abwägen und aufgrund dieser Abwägung zu einer eigenen und freien Entscheidung gelangen kann. Es ist deshalb unumgänglich, der betroffenen Person bereits vor der Einwilligung alle entscheidungserheblichen Informationen zukommen zu lassen. Nur dann kann eine informierte Willensbekundung im Sinne von Artikel 4 Nummer 11 DSGVO erfolgen. Welche Informationen relevant und mitzuteilen sind, richtet sich nach dem jeweiligen Einzelfall. Nach dem working paper 259, Seite 13, der Artikel-29-Arbeitsgruppe sind für eine informierte Einwilligung zumindest folgende Informationen mitzuteilen:

- die Person des Verantwortlichen,

- der jeweils beabsichtigte Verarbeitungszweck, der auf die Einwilligung gestützt werden soll; bei mehreren Verarbeitungszwecken, sind alle mitzuteilen,
- die zu verarbeitenden Daten,
- die Möglichkeit zum Widerruf der Einwilligung und die Folgen des Widerrufs (vgl. Artikel 7 Absatz 3 Satz 2 DSGVO),,
- ggf. die Verwendung der Daten für eine ausschließlich automatisierte Entscheidungsfindung (einschließlich Profiling),
- ggf. die bestehenden Risiken bei einer Einwilligung in die Übermittlung personenbezogener Daten in Drittstaaten, für die weder ein Angemessenheitsbeschluss im Sinne von Artikel 45 DSGVO noch geeignete Garantien im Sinne von Artikel 46 DSGVO vorliegen (Artikel 49 Absatz 1 Satz 1 Buchstabe a DSGVO).

Für Einwilligungen besteht zudem ein Koppelungsverbot, d.h., dass für mehrere trennbare Sachverhalte auch getrennte Einwilligungen erteilt werden müssen.

*Besonderheit: Einwilligung gegenüber Behörden*

In den Erwägungsgründen 42 und 43 zur DSGVO wird betont, dass von einer Freiwilligkeit der Einwilligung nur dann ausgegangen werden könne, wenn die betroffene Person eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

- Eine Grundvoraussetzung einer freien Wahl ist die zuvor bereits dargestellte möglichst detaillierte Aufklärung.
- Darüber hinaus kann es zweifelhaft sein, ob eine freie Wahl vorliegt, wenn ein klares Ungleichgewicht zwischen der betroffenen Person und dem Verantwortlichen besteht. Sofern es sich bei dem Verantwortlichen um eine Behörde handelt, soll ein solches Ungleichgewicht nach dem Erwägungsgrund 43 der DSGVO vermutet werden. Allerdings soll nicht jedes Ungleichgewicht automatisch zur Unwirksamkeit der Einwilligung führen, sondern es muss trotz Vorliegens eines Ungleichgewichts immer noch zusätzlich geprüft werden, ob es in Anbetracht der Umstände unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde. Damit sind in der Praxis weiterhin (Ausnahme-)Fälle vorstellbar, in denen auch eine Verarbeitung personenbezogener Daten durch Behörden aufgrund einer Einwilligung erfolgen kann.

Bereits in der Vergangenheit erteilte Einwilligungen können auch weiterhin als Grundlage einer Verarbeitung personenbezogener Daten dienen, wenn sie den Anforderungen der DSGVO entsprechen.

Anhand der dargestellten Anforderungen an die Aufklärung, die Trennung der relevanten Sachverhalte und die Freiwilligkeit wird jedoch deutlich, dass die Verarbeitung personenbezogener Daten aufgrund einer Einwilligung nachteilig für den Verantwortlichen sein kann, weil ein Risiko für eine unerkennbare rechtswidrige Verarbeitung nicht ausgeschlossen werden kann. Zudem können sich weitere Nachteile für den Verantwortlichen ergeben, da eine Einwilligung jederzeit mit Wirkung für die Zukunft frei widerruflich ist. Der Verantwortliche muss in einem solchen Fall sicherstellen, dass die weitere Verarbeitung tatsächlich umgehend beendet wird, wozu auch gehören kann, dass weitere Empfänger der Daten (andere Verantwortliche oder Auftragsverarbeiter) von dem Widerruf der Einwilligung informiert werden. Aufgrund dieser Nachteile sollte vorrangig

geprüft werden, ob die Verarbeitung personenbezogener Daten aufgrund einer gesetzlichen Erlaubnis erfolgen kann.

### 5.2 Verarbeitung mit Zweckänderung

Grundsätzlich soll die Verarbeitung personenbezogener Daten nur zu dem Zweck erfolgen, zu dem sie erhoben wurden (Artikel 5 Absatz 1 Buchstabe b DSGVO). Die Zulässigkeit der Verarbeitung zu anderen Zwecken ist unter den Voraussetzungen von Artikel 6 Absatz 4 DSGVO zulässig. Zudem enthält § 15 BlnDSG Regelungen, unter denen eine zweckändernde Verarbeitung zulässig ist.

### 5.3 Verarbeitung besonderer Kategorien personenbezogener Daten

Hinsichtlich der Verarbeitung besonderer Kategorien personenbezogener Daten enthält Artikel 9 DSGVO spezifische Anforderungen. Welche Daten zu den besonderen Kategorien gehören, ist in Artikel 9 Absatz 1 DSGVO definiert.

### 5.4 Ermittlung der Rechtsgrundlage

Mit Blick darauf, dass öffentliche Stellen in der Regel zum Zweck der Erfüllung der ihnen gesetzlich oder aufgrund Gesetzes zugewiesenen Aufgaben handeln, empfiehlt sich bei der Ermittlung einer Rechtsgrundlage für die Verarbeitung personenbezogener Daten die folgende Prüfungsreihenfolge:

1. Gibt es im bereichsspezifischen Recht eine Rechtsgrundlage bzw. Befugnisnorm?
2. Stellt das BlnDSG (§§ 3, 14 ff. BlnDSG) eine Erlaubnisnorm zur Verfügung?
3. Kann die Datenverarbeitung auf Artikel 6 Absatz 1 Buchst. a, b, d oder f DSGVO gestützt werden? Dabei ist zu beachten, dass öffentliche Stellen die Datenverarbeitung im Zusammenhang mit der Erfüllung ihrer zugewiesenen Aufgaben i.d.R. nicht auf Artikel 6 Absatz 1 Buchst. f DSGVO stützen können und Einwilligungen nur eingeschränkt als Rechtsgrundlage in Betracht kommen (dazu oben Ziffer 5.1).

In jedem Fall ist zu beachten, dass sowohl das allgemeine als auch das bereichsspezifische Datenschutzrecht häufig nur ergänzende und konkretisierende Regelungen zu den Vorgaben der DSGVO trifft. Zur Beurteilung datenschutzrechtlicher Fragestellungen werden somit die DSGVO und die Regelungen im allgemeinen sowie gegebenenfalls auch im bereichsspezifischen nationalen Datenschutzrecht (sei es im Landes-, sei es im Bundesrecht) im Zusammenhang zu lesen und anzuwenden sein.

## 6. Verfahrensänderungen

Schwerpunkt der Anpassungsaufgaben an die DSGVO und das neue BlnDSG sind die umfangreichen Verfahrensänderungen im Datenschutz:

### 6.1 Verzeichnis der Verarbeitungstätigkeiten

Das bisherige Verfahrensverzeichnis nach § 19 BlnDSG wird durch das Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 DSGVO abgelöst. Anders als nach bisherigem Recht ist ein Verzeichnis der Verarbeitungstätigkeiten unabhängig davon zu führen, ob die Verarbei-

tung automatisiert erfolgt oder nicht. Das heißt, auch soweit personenbezogene Daten in strukturierten Papierakten (dazu oben Ziffer 2.1.1.1) verarbeitet werden, ist ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Weil die DSGVO aufgrund von § 2 Absatz 9 BlnDSG entsprechend auch für sonstige personenbezogene Daten anwendbar ist, selbst wenn diese nicht unmittelbar in den Anwendungsbereich der DSGVO fallen, gibt es keine Ausnahmen von der Aufnahmeverpflichtung in das Verzeichnis.

Das Verzeichnis der Verarbeitungstätigkeiten ist vom Verantwortlichen zu führen. Der Verantwortliche hat im Rahmen seiner Organisationshoheit zu bestimmen, wer das jeweilige Verzeichnis erstellt und wer dieses führt. Die Erstellung sollte zweckmäßiger Weise durch den für die jeweilige Fachaufgabe verantwortlichen Bereich, ggf. unter Beteiligung der IT-Stelle erfolgen, in jedem Fall aber anhand einheitlicher Formulare. Die Führung des aus den jeweiligen Einzelverzeichnissen zusammengefügten Gesamtverzeichnisses sollte aber zentral geführt werden. Es ist empfehlenswert, wenn der behördliche Datenschutzbeauftragte zumindest eine Kopie der Verzeichnisse vorhält, um seine Aufgaben wahrnehmen zu können.
Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) hat zur Erstellung der Verzeichnisse eine Arbeitshilfe entwickelt, die als Anlage 3a beigefügt ist. Die Arbeitshilfe wurde zudem von der Berliner Beauftragten für Datenschutz und Informationsfreiheit unter der URL:

https://www.datenschutz-berlin.de/kurzpapiere.html

veröffentlicht. Zudem hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit unter der URL:

https://www.datenschutz-berlin.de/orientierungshilfen.html

sowohl für Verantwortliche als auch für Auftragsverarbeiter jeweils ein Muster für das Verzeichnis von Verarbeitungstätigkeiten bereitgestellt (Anlage 3b und 3c).

### 6.2 Datenschutz-Folgenabschätzung

Vor dem Einsatz „hochrisikoträchtiger“ und eingriffsintensiver Verarbeitungen ist künftig eine Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO durchzuführen. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat hierzu ergänzend eine – nicht abschließende – Liste von Verarbeitungen veröffentlicht, für die ein solches Verfahren durchzuführen ist. Für Datenverarbeitungen, die am 25. Mai 2018 bereits betrieben wurden und die in die Kategorie „hochrisikoträchtiger“ Verarbeitungen im Sinne des Artikel 35 DSGVO einzustufen wären, ist keine Datenschutz-Folgenabschätzung erforderlich, wenn:

- zuvor eine Vorabkontrolle entsprechend § 19a Absatz 1 Satz 3 Nummer 1 BlnDSG durch den behördlichen Datenschutzbeauftragten erfolgt ist,
- soweit zutreffend, die in Zweifelsfällen erforderliche Konsultation der Berliner Beauftragten für Datenschutz und Informationsfreiheit erfolgt ist (§ 19a Absatz 4 Satz 2 BlnDSG) und
- zwischenzeitlich keine wesentlichen Änderungen vorgenommen wurden.

Allerdings ist zu beachten, dass die Verfahren regelmäßig auf ihre Konformität mit der DSGVO zu überprüfen sind (Artikel 24 Absatz 1 Satz 2 DSGVO), so dass eine Artikel 35 DSGVO entsprechende Überprüfung innerhalb von zwei bis drei Jahren nach der Geltung der DSGVO, also spätestens bis zum 25. Mai 2021 durchgeführt werden sollte. Die „Artikel

29-Datenschutzgruppe“, das Vorgängergremium für den nunmehr nach Artikel 68 DSGVO eingerichteten Europäischen Datenschutzausschuss, hat Leitlinien zur Datenschutz-Folgenabschätzung entwickelt (working paper 248 Rev. 1 - Anlage 4), die nähere Ausführungen zu diesem Verfahren enthalten.

Zuständig für die Durchführung der Datenschutz-Folgenabschätzung ist der Verantwortliche. Dabei holt der Verantwortliche zwingend die Stellungnahme des behördlichen Datenschutzbeauftragten ein (Artikel 35 Absatz 2 DSGVO). Nicht DSGVO-konform wäre es, dem Datenschutzbeauftragten die Zuständigkeit für die Durchführung der Datenschutz-Folgeabschätzung zu übertragen.

## 7. Behördliche Datenschutzbeauftragte

Durch die DSGVO wurden auch die Stellung und die Aufgaben der behördlichen Datenschutzbeauftragten neu geregelt (Artikel 37 bis 39 DSGVO). Nach Artikel 37 Absatz 1 Buchst. a DSGVO hat jede öffentliche Stelle einen Datenschutzbeauftragten zu benennen. Aus § 4 Absatz 3 BlnDSG folgt zudem auch die Pflicht zur Benennung einer Stellvertretung.

Der behördliche Datenschutzbeauftragte ist auf der Grundlage der beruflichen Qualifikation und insbesondere des datenschutzrechtlichen Fachwissens zu benennen (Artikel 37 Absatz 5 DSGVO). Dazu gehören Rechtskenntnisse bezüglich der einschlägigen datenschutzrechtlichen Regelungen sowie Grundkenntnisse der eingesetzten IuK-Technik.

Der behördliche Datenschutzbeauftragte ist frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden (Artikel 38 Absatz 1 DSGVO). Er muss Zugang zum Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 DSGVO haben. Der behördliche Datenschutzbeauftragte ist berechtigt und verpflichtet, der Behördenleitung unmittelbar zu berichten (Art 38 Absatz 3 Satz 3 DSGVO).

Wesentliche Aufgaben des behördlichen Datenschutzbeauftragten gemäß Artikel 39 Absatz 1 DSGVO sind:

- die Unterrichtung und Beratung des Verantwortlichen über dessen datenschutzrechtliche Pflichten,
- die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften im Sinne eines Monitoring,
- die Überwachung der Durchführung von Sensibilisierungs- und Schulungsmaßnahmen der mit der Verarbeitung personenbezogener Daten Beschäftigten durch den Verantwortlichen
- die Zusammenarbeit mit der Aufsichtsbehörde und
- die Beratung des Verantwortlichen bei Datenschutz-Folgenabschätzungen.

Die Führung des Verzeichnisses der Verarbeitungstätigkeiten und die Durchführung der Datenschutz-Folgenabschätzung sind nach der DSGVO keine Pflichtaufgaben des behördlichen Datenschutzbeauftragten – anders als früher die Führung des Verfahrensverzeichnisses und die Durchführung der Vorabkontrolle.

Der Verantwortliche kann dem Datenschutzbeauftragten im Einklang mit der DSGVO weitere Aufgaben übertragen, allerdings dürfen diese nicht zu einem Interessenkonflikt führen. Ein Interessenkonflikt kann beispielsweise entstehen, wenn der behördliche Datenschutzbeauftragte selber wesentlich Einfluss auf die Bestimmung von Mittel und Zweck der Datenverar-

beitung hat (z.B. als Leiter der für die IT oder für Personal zuständigen Organisationseinheit) oder selber nicht nur in untergeordnetem Umfang personenbezogene Daten verarbeitet. Die Übertragung von Pflichtaufgaben des Verantwortlichen (z.B. zur Führung des Verzeichnisses der Verarbeitungstätigkeiten) auf den behördlichen Datenschutzbeauftragten dürfte bei diesem ebenfalls zu einem Interessenkonflikt führen. Aus Artikel 35 Absatz 1 Satz 1 und Absatz 2 DSGVO ergibt sich zudem, dass die Durchführung der Datenschutz-Folgenabschätzung nicht auf den behördlichen Datenschutzbeauftragten übertragen werden kann.

Zu den übertragbaren Aufgaben gehört aber beispielsweise die Vorgabe, dass vor jedem beabsichtigten Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden, die Stellungnahme des behördlichen Datenschutzbeauftragten einzuholen ist.

Dem behördlichen Datenschutzbeauftragten sind die zur Erfüllung seiner Aufgaben erforderlichen Ressourcen zur Verfügung zu stellen (Artikel 39 Absatz 2 DSGVO).

## 8. Befugnisse der Aufsichtsbehörde

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit erhält als Aufsichtsbehörde verstärkte Befugnisse bis hin zur Untersagung einzelner Datenverarbeitungen (Artikel 57 und 58 DSGVO). Ergänzend zu den Befugnissen aus der DSGVO wird in § 13 Absatz 1 BlnDSG das Beanstandungsrecht aus § 26 Absatz 1 Satz 1 BlnDSG-alt übernommen. Im Anwendungsbereich der JI-Richtlinie besteht nur das Beanstandungsrecht (§ 13 Absatz 2 BlnDSG). Im Zusammenhang mit dem Beanstandungsrecht besteht zudem eine erleichterte Möglichkeit, den für die jeweilige Behörde zuständigen Fachausschuss des Abgeordnetenhauses mit dem Grund der Beanstandung zu befassen (§ 13 Absatz 3 BlnDSG).

## 9. Rechte der betroffenen Personen und Pflichten des Verantwortlichen

Die Rechte der betroffenen Personen sind von der DSGVO erheblich gestärkt worden. Dies gilt insbesondere für die Information der betroffenen Person im Zusammenhang mit der Datenerhebung. Erweiterungen, Einschränkungen oder Modifizierungen der Betroffenenrechte können sich aus besonderen Datenschutzvorschriften (z.B. § 32c der Abgabenordnung, § 82 und § 83 des Zehnten Buches Sozialgesetzbuch [SGB X]) und aus dem BlnDSG (z.B. §§ 23 ff.) ergeben.

### 9.1 Modalitäten im Zusammenhang mit der Ausübung von Betroffenenrechten

Für Informationen und Mitteilungen zur Wahrung der Rechte der betroffenen Personen enthält Artikel 12 DSGVO allgemeine Vorgaben. Informationen über Datenerhebungen und Mitteilungen zu geltend gemachten Rechten sind der betroffenen Person danach in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln, schriftlich oder in einer anderen Form, gegebenenfalls auch elektronisch (Artikel 12 Absatz 1 DSGVO).

Artikel 12 Absatz 3 DSGVO bestimmt eine konkrete Frist zur Beantwortung von Anträgen, mit denen die betroffene Person ihre Rechte geltend macht. Die Antwort hat ohne unangemessene Verzögerung, spätestens aber innerhalb eines Monats zu erfolgen. Die Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und Anzahl von Anträgen erforderlich ist. Daneben bestimmt Artikel 12 Absatz 3 DSGVO,

dass Anträge betroffener Personen nach Möglichkeit auf elektronischem Wege zu beantworten sind, wenn sie auf diesem Wege gestellt wurden. Die Möglichkeit einer Beantwortung auf elektronischem Wege setzt allerdings eine eindeutige Identifizierung und die Sicherheit der Datenübermittlung voraus.

Eine Neuerung enthält Artikel 12 Absatz 4 DSGVO. Nach dieser Norm ist die betroffene Person über die Gründe für ein etwaiges Untätigbleiben auf einen Antrag zur Geltendmachung eines Betroffenenrechts hinzuweisen und über die Möglichkeit zur Beschwerde bei einer Aufsichtsbehörde zu unterrichten.

Informationen über Datenerhebungen und Mitteilungen bzw. Maßnahmen aufgrund von Anträgen, mit denen die betroffene Person ihre Rechte geltend macht, erfolgen grundsätzlich unentgeltlich (Artikel 12 Absatz 5 DSGVO).

### 9.2 Informationspflichten des Verantwortlichen nach den Artikeln 13 und 14 DSGVO

Ein wesentliches Anliegen der DSGVO ist die Stärkung des Transparenzgrundsatzes (Artikel 5 Absatz 1 Buchstabe a und Erwägungsgrund 39 DSGVO). Dass die betroffene Person die maßgeblichen Faktoren der Verarbeitung der Daten nachvollziehen kann, ist eine wesentliche Ausprägung einer fairen und transparenten Datenverarbeitung. Nur so kann die betroffene Person informiert über die Verarbeitung ihrer Daten entscheiden. Ferner muss die betroffene Person überhaupt Kenntnis von der Existenz der Datenverarbeitung erlangen, um die Betroffenenrechte effektiv wahrnehmen zu können. Zur Erfüllung der Grundsätze einer fairen und transparenten Verarbeitung von personenbezogenen Daten sehen Artikel 13 und 14 DSGVO daher einen umfangreichen Katalog proaktiver Benachrichtigungen bei der Erhebung personenbezogener Daten vor.
Während Artikel 13 DSGVO davon ausgeht, dass bei der Erhebung personenbezogener Daten unmittelbar bei der betroffenen Person, diese umgehend über relevante Fragen informiert werden kann, enthält Artikel 14 DSGVO Informationspflichten für die Konstellation, dass die Erhebung nicht unmittelbar bei der betroffenen Person erfolgt (sondern z.B. durch Ermittlung der Daten im Rahmen eines Verwaltungsverfahrens mittels Datenbankrecherche oder durch gezielte Befragung Dritter). In einem solchen Fall, in dem wegen Abwesenheit der betroffenen Person im Zeitpunkt der Erhebung keine zeitgleiche Information möglich ist, soll diese möglichst schnell im Anschluss an die Erhebung erfolgen.

In den Anlagen 5a und 5b finden sich Mustertexte mit Ausfüllhinweisen. Wesentliche Angaben zur Erfüllung der Informationspflichten nach Artikel 13 und 14 DSGVO decken sich mit den Angaben im Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 Absatz 1 DSGVO und können daher insoweit aus der jeweiligen Beschreibung der Verarbeitungstätigkeit übernommen werden.

Der Verantwortliche ist dazu verpflichtet, die betroffene Person zu informieren, wenn:

- personenbezogene Daten direkt bei der betroffenen Person erhoben werden (Artikel 13 DSGVO),
- personenbezogene Daten nicht direkt bei der betroffenen Person erhoben werden, (Artikel 14 DSGVO) oder
- beabsichtigt wird, bereits vorliegende personenbezogene Daten für einen anderen Zweck weiterzuverarbeiten als den, für den diese Daten erhoben oder erlangt wurden („Zweckänderung“, Artikel 13 Absatz 3 bzw. Artikel 14 Absatz 4 DSGVO).

Für alle zuvor genannten Fälle wird folgendes Prüfschema vorgeschlagen, zu dem nachfolgend unter den Ziffern 9.2.1 bis 9.2.3 weitere Ausführungen erfolgen:

a) Liegt ein Fall von Artikel 13 oder Artikel 14 DSGVO oder eine Zweckänderung vor?

b) Gibt es einschlägige Ausnahmen oder wurde die betroffene Person bereits anderweitig informiert?

c) Wann, in welcher Form und mit welchem Inhalt ist die betroffene Person zu informieren?

### 9.2.1 Informationspflichten bei einer Erhebung personenbezogener Daten bei der betroffenen Person

a) Liegt ein Fall des Artikels 13 Absatz 1 und 2 DSGVO vor?

Voraussetzung für die Informationspflicht nach Artikel 13 Absatz 1 und 2 DSGVO ist, dass der Verantwortliche die personenbezogenen Daten bei der betroffenen Person erhebt.

Eine Erhebung setzt voraus, dass der Verantwortliche die Daten selbst aktiv beschafft. Werden personenbezogene Daten von der betroffenen Person unaufgefordert selbst preisgegeben, liegt keine Erhebung vor.

***Beispiele*** *für eine Erhebung bei der betroffenen Person:*

- *Eine Person füllt ein von der öffentlichen Stelle vorgegebenes Formular aus und übermittelt es an die öffentliche Stelle.*
- *Eine Person gibt Daten auf einer Internetseite in vorgegebenen Datenfeldern ein (Kontaktformular, Online-Bewerbungssystem etc.).*
- *Eine Person sendet aufgrund einer Stellenausschreibung Bewerbungsunterlagen per Post oder E-Mail an eine öffentliche Stelle.*
- *Daten der betroffenen Person werden mittels E-Mail oder während eines Telefongesprächs erfragt.*
- *Daten einer Person werden in einem persönlichen Gespräch erfragt.*

***Beispiel*** *für nicht aktiv beschaffte Daten und damit keine Erhebung:*

- *Spam-E-Mails.*

Werden die personenbezogenen Daten nicht bei der betroffenen Person selbst erhoben, sondern z.B. von einer anderen öffentlichen Stelle auf Anfrage übermittelt, ist zu prüfen, ob ein Fall des Artikels 14 DSGVO vorliegt (dazu nachfolgend Ziffer 9.2.2).

b) Gibt es Ausnahmen von der Informationspflicht?

Ausnahmen finden sich in Artikel 13 Absatz 4 DSGVO und § 23 BlnDSG oder können sich aus bereichsspezifischen Gesetzen ergeben.

Verfügt die betroffene Person bereits über die Informationen, besteht keine Informationspflicht für den Verantwortlichen (Artikel 13 Absatz 4 DSGVO).

- In einem Verwaltungsverfahren ist es z.B. ausreichend, die betroffene Person zu Beginn des Verfahrens – in der Regel bei Antragseinreichung – zu informieren. Sollten sich im weiteren Verfahren Anfragen oder Rückfragen ergeben, die zu einer weiteren Datenerhebung bei der betroffenen Person führen, löst dies grundsätzlich keine neue

Informationspflicht aus, es sei denn, dass für die nachträglich erhobenen Daten andere Regelungen gelten, z.B. wenn diese einer längeren Speicherdauer unterliegen oder an andere Empfänger übermittelt werden sollen (Transparenzgebot, Artikel 5 Absatz 1 Buchstabe a DSGVO).

- Zudem ist eine besondere Information nicht erforderlich, wenn sich die mitzuteilenden Informationen eindeutig aus den Umständen der Erhebung ergeben. Hierbei ist allerdings zu beachten, ob sich alle erforderlichen Informationen tatsächlich aus dem Kontext ergeben (fraglich kann dies beispielsweise im Hinblick auf die Kontaktdaten des behördlichen Datenschutzbeauftragten [Artikel 13 Absatz 1 Buchstabe b DSGVO] sein).
- Auch bei wiederholten Erhebungen, die dem gleichen Zweck dienen, kann grundsätzlich davon ausgegangen werden, dass die betroffene Person bereits über die Information verfügt und eine Wiederholung der Information nicht erforderlich ist (Beispiel: wiederholte Lebensmittelkontrollen im gleichen Betrieb).

Die Pflicht zur Information der betroffenen Person besteht weiterhin nach § 23 Absatz 1 BlnDSG nicht, soweit und solange:

- die Information die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
- die Information die Verfolgung von Straftaten oder Ordnungswidrigkeiten gefährden würde oder
- Tatsachen aufgedeckt würden, die geheim zu halten sind:
    - nach einer öffentlichen Interessen dienenden Rechtsvorschrift oder
    - zum Schutz überwiegender Rechte und Freiheiten anderer Personen.

Unterbleibt die Information der betroffenen Person nach § 23 Absatz 1 BlnDSG, so hat der Verantwortliche gemäß § 23 Absatz 2 BlnDSG jedoch die Informationen nach Artikel 13 DSGVO in allgemeiner Form für die Öffentlichkeit zur Verfügung zu stellen. Da nicht steuerbar ist, in welchen Fällen die Voraussetzungen für die Ausnahmen von den Informationspflichten eintreten können, empfiehlt es sich, die allgemeine Information in jedem Fall vorzunehmen (z.B. auf der Internetseite der jeweiligen öffentlichen Stelle und/oder mittels eines Aushanges einer Stelle, die der Öffentlichkeit zugänglich ist), selbst wenn bisher noch kein Ausnahmefall eingetreten ist. Dies ist auch im Hinblick auf Artikel 14 Absatz 5 Buchstabe b DSGVO angezeigt, der ebenfalls eine allgemeine Information vorschreibt, wenn eine individuelle Information unmöglich ist oder mit einem unverhältnismäßigen Aufwand verbunden ist.

Unterbleibt eine vorgeschriebene Information aus einem der in § 23 BlnDSG genannten Gründen, hat der Verantwortliche die jeweiligen Gründe zu dokumentieren.

Im Falle vorübergehender Ausnahmegründe sollte regelmäßig überprüft werden, ob die Voraussetzungen des § 23 Absatz 1 BlnDSG weiterhin vorliegen. Ist dies nicht mehr der Fall, muss die betroffene Person über die Datenverarbeitung informiert werden.

c) Zeitpunkt, Form und Inhalt der Mitteilung der Informationen

Die Information hat zum Zeitpunkt der Erhebung gegenüber der betroffenen Person zu erfolgen. Sie muss in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden. Aus Artikel 12 Absatz 1 Satz 1

letzter Halbsatz DSGVO ergibt sich, dass die Informationspflicht und die Betroffenenrechte auch gegenüber Kindern bestehen können. Soweit sich Informationen speziell an Kinder richten, muss dies im Rahmen der Verständlichmachung berücksichtigt werden.

Die Informationen und Mitteilungen können schriftlich oder in einer anderen Form, gegebenenfalls auch elektronisch, erfolgen.

Bei Erhebung personenbezogener Daten mit Hilfe von Papierformularen können den betroffenen Personen die erforderlichen Informationen auf dem jeweiligen Formular oder durch ein separates Begleitdokument mitgeteilt werden. Werden Formulare auf der Internetseite zum Download zur Verfügung gestellt, können die Informationen auch in einem separaten Begleitdokument deutlich sichtbar auf der gleichen Seite zum Download zur Verfügung gestellt werden. In den Formularen wäre auf dieses Begleitdokument zudem hinzuweisen.

In den Fällen, in denen eine Person Daten auf einer Internetseite in vorgegebene Datenfelder eingibt, kann durch einen deutlich sichtbaren Link auf eine gesonderte Seite mit den Informationen nach Artikel 13 DSGVO hingewiesen werden. Des Weiteren besteht die Möglichkeit, zusätzlich begleitende Sofortinformationen zu den Datenfeldern durch Pop-Up-Fenster oder Mouseover-Effekte mitzuteilen.

Insbesondere für die Veröffentlichung von Informationen auf Internetseiten ist zu beachten, dass für jede Verarbeitungstätigkeit einer öffentlichen Stelle spezifische Informationen bereitzustellen sind. Im Ergebnis werden auf der Internetseite einer öffentlichen Stelle damit viele unterschiedliche Hinweise mit Informationen nach Artikel 13 DSGVO zum Abruf oder Download zur Verfügung stehen.

Auch bei der mündlichen Erhebung von personenbezogenen Daten (wie z.B. in persönlichen Gesprächen oder Telefonaten) besteht die Informationspflicht, wenn nicht eine der o.g. Ausnahmen greift. Gibt eine Person bspw. unaufgefordert personenbezogene Daten über sich preis und werden (ggf. im weiteren Verlauf des Gesprächs) auch keine personenbezogenen Daten selbst aktiv beschafft, handelt es sich grundsätzlich nicht um eine Erhebung bzw. es liegt eine Ausnahme von der Informationspflicht vor, weil die betroffene Person aufgrund der Umstände ggf. bereits über die Information verfügt (Artikel13 Absatz 2 DSGVO). In diesen Fällen besteht dem Grunde nach keine Informationspflicht nach Artikel 13 DSGVO.

Werden personenbezogene Daten mündlich erhoben (z.B. Kontaktdaten im Rahmen eines Telefonats erfragt) und kann kein Informationsblatt ausgehändigt werden, empfiehlt es sich, im Zusammenhang mit der Frage nach den Daten kurz darauf hinzuweisen, für welchen Zweck die Daten erfragt werden, dass die Daten nur für die zuvor genannten Zwecke bei der jeweiligen Behörde verarbeitet werden (bzw. an wen die Daten aus welchem Grund weitergeleitet werden) und ob die Daten anschließend gelöscht oder weiter aufbewahrt werden sollen. Abschließend sollte auf die Möglichkeit hingewiesen werden, sich erforderlichenfalls an den behördlichen Datenschutzbeauftragten wenden zu können, verbunden mit einem Hinweis auf weitergehende Datenschutzinformationen z.B. durch Aushänge vor Ort oder auf der Internetseite der jeweiligen öffentlichen Stelle.

Bereits bestehende Formulare für Datenerhebungen müssen an die neuen gesetzlichen Vorgaben angepasst und ggf. ergänzt werden.

Anlage 5a enthält einen Mustertext mit allen nach Artikel 13 DSGVO vorgeschriebenen Angaben und Ausfüllhinweisen. Bei Verwendung dieses Mustertextes sind die dort enthal-

tenen Angaben vollständig und auf die jeweilige Verarbeitungstätigkeit angepasst zur Verfügung zu stellen.

### 9.2.2 Informationspflichten bei der Erhebung personenbezogener Daten nicht bei der betroffenen Person

a) Liegt ein Fall des Artikels 14 DSGVO vor?

Voraussetzung für die Informationspflicht nach Artikel 14 DSGVO ist, dass die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden.

Damit eine Erhebung vorliegt, muss die öffentliche Stelle die Daten selbst aktiv beschaffen (vgl. oben Ziffer 9.2.1) und zwar ohne Mitwirkung der betroffenen Person. So liegt kein Fall des Artikels 14 DSGVO vor, wenn personenbezogene Daten von Dritten ohne Aufforderung an die öffentliche Stelle mitgeteilt werden.

***Beispiele** für eine Erhebung nicht bei der betroffenen Person:*

- *Die öffentliche Stelle beschafft aktiv Daten der betroffenen Person aus allgemein zugänglichen Quellen wie aus einer Zeitung, dem Internet oder durch Besichtigung allgemein zugänglicher Verkehrsflächen. Werden bei Lektüre der Zeitung, im Internet oder bei einer Besichtigung allgemein zugänglicher Verkehrsflächen personenbezogene Daten lediglich wahrgenommen, ohne dass eine gezielte Beschaffung bezweckt ist, liegt bereits keine Erhebung vor.*
- *Eine Behörde lässt sich personenbezogene Daten von einer anderen Behörde übermitteln.*
- *Die öffentliche Stelle verschafft sich personenbezogene Daten über einen Adresshändler.*

Werden personenbezogene Daten an eine andere öffentliche Stelle auf deren Anfrage übermittelt, löst diese Übermittlung seitens der anfragenden Behörde die Informationspflicht nach Artikel 14 DSGVO aus. Die übermittelnde Behörde muss die betroffene Person über die Übermittlung nur informieren, wenn die Übermittlung vom ursprünglichen Verarbeitungszweck nicht umfasst ist und somit eine Zweckänderung darstellt (Artikel 13 Absatz 3, siehe dazu nachfolgend Ziffer 9.2.3).

In diesem Fall hat also grundsätzlich die empfangende Stelle entsprechend dem Mustertext der Anlage 5b eine umfassende Information der betroffenen Person sicherzustellen und dabei unter Nummer 5 „Angabe der Quelle“ darzulegen, von welcher anderen Stelle die Daten übermittelt wurden.

b) Gibt es Ausnahmen von der Informationspflicht?

Ausnahmen finden sich in Artikel 14 Absatz 5 DSGVO und § 23 BlnDSG oder können sich aus bereichsspezifischen Gesetzen ergeben.

Eine Information der betroffenen Person kann nach Artikel 14 Absatz 5 DSGVO unterleiben, wenn und soweit:

- die betroffene Person bereits über die Informationen verfügt,
- sich die Erteilung einer Information als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, insbesondere bei Verarbeitungen für:
  - im öffentlichen Interesse liegende Archivzwecke,

- wissenschaftliche oder historische Forschungszwecke oder
- Statistikzwecke,

- wenn die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen vorsehen, ausdrücklich geregelt ist oder
- wenn die personenbezogenen Daten einem Berufsgeheimnis unterliegen und daher vertraulich behandelt werden müssen (z.B. bei einem Rechtsanwalt, der von seinem Mandanten personenbezogene Daten über den Prozessgegner erhält).

Die Pflicht zur Information der betroffenen Person besteht zudem nach § 23 Absatz 1 BlnDSG nicht, soweit und solange:

- die Information die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
- die Information die Verfolgung von Straftaten oder Ordnungswidrigkeiten gefährden würde oder
- Tatsachen aufgedeckt würden, die geheim zu halten sind:
  - nach einer öffentlichen Interessen dienenden Rechtsvorschrift oder
  - zum Schutz überwiegender Rechte und Freiheiten anderer Personen.

Unterbleibt die Information der betroffenen Person nach § 23 Absatz 1 BlnDSG, so hat der Verantwortliche gemäß § 23 Absatz 2 BlnDSG jedoch die Informationen nach Artikel 13 DSGVO in allgemeiner Form für die Öffentlichkeit zur Verfügung zu stellen. Da nicht steuerbar ist, in welchen Fällen die Voraussetzungen für die Ausnahmen von den Informationspflichten eintreten können, empfiehlt es sich, die allgemeine Information in jedem Fall vorzunehmen (z.B. auf der Internetseite der jeweiligen öffentlichen Stelle und/oder mittels eines Aushanges einer Stelle, die der Öffentlichkeit zugänglich ist), selbst wenn bisher noch kein Ausnahmefall eingetreten ist. Dies ist auch im Hinblick auf Artikel 14 Absatz 5 Buchstabe b DSGVO angezeigt, der ebenfalls eine allgemeine Information vorschreibt, wenn eine individuelle Information unmöglich ist oder mit einem unverhältnismäßigen Aufwand verbunden ist.

Unterbleibt eine vorgeschriebene Information aus einem der in § 23 BlnDSG genannten Gründen, hat der Verantwortliche die jeweiligen Gründe zu dokumentieren.

Im Falle vorübergehender Ausnahmegründe sollte regelmäßig überprüft werden, ob die Voraussetzungen des § 23 Absatz 1 BlnDSG weiterhin vorliegen. Ist dies nicht mehr der Fall, muss die betroffene Person über die Datenverarbeitung informiert werden.

c) Zeitpunkt, Form und Inhalt der Information

Werden personenbezogene Daten nicht direkt bei der betroffenen Person erhoben, weiß diese im Regelfall nichts von der Datenerhebung. Zur Information der betroffenen Person wird daher in aller Regel eine aktive Kontaktaufnahme erforderlich sein. Die notwendigen Informationen müssen nicht zwingend in Schriftform bereitgestellt werden, auch eine Information per E-Mail ist denkbar, soweit durch entsprechende Sicherheitsmaßnahmen gewährleistet ist, dass im Rahmen der Information mitgeteilte personenbezogene Daten nicht von unberechtigten Personen mitgelesen werden können. Außerdem ist bei der Kontaktaufnahme zu beachten, dass auch durch eine Kontaktaufnahme zur betroffenen Person schützenswerte Daten an Dritte offenbart werden können (z.B. durch ein Schreiben

mit der Absenderangabe: „Sozialpsychiatrischer Dienst“ auf dem Briefumschlag). Die Informationen über eine Erhebung im Sinne von Artikel 14 DSGVO sind der betroffenen Person innerhalb einer angemessenen Frist, spätestens jedoch innerhalb eines Monats nach Erlangung der Daten mitzuteilen (Artikel 14 Absatz 3 Buchst. a DSGVO).

Diese Frist verkürzt sich ggf., wenn die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen (z.B. in einem Anschreiben). In diesem Fall ist die Information spätestens zu erteilen, wenn mit der Person das erste Mal in Kontakt getreten wird (Artikel 14 Absatz 3 Buchstabe b DSGVO). Erfolgt diese erste Kommunikation daher vor der Einmonatsfrist, muss der Informationspflicht spätestens bei der ersten Kontaktaufnahme nachgekommen werden, auch wenn die Einmonatsfrist bisher nicht abgelaufen ist. Im umgekehrten Fall, wenn die erste Kommunikation später als einen Monat nach Erlangung der Daten erfolgt, gilt Artikel 14 Absatz 3 Buchstabe a DSGVO, sodass die betroffene Person spätestens innerhalb eines Monats informiert werden muss.

Falls eine Offenlegung an andere Empfänger beabsichtigt wird, ist die Information spätestens zum Zeitpunkt der ersten Offenlegung zu erteilen (Artikel 14 Absatz 3 Buchstabe c DSGVO). Auch in diesem Fall verkürzt sich die Einmonatsfrist des Artikels 14 Absatz 3 Buchstabe b DSGVO, wenn die erste Offenlegung vor Ablauf von einem Monat nach Erlangung der Daten erfolgt. Werden die Daten später als einen Monat nach Erlangung der Daten zum ersten Mal gegenüber einem anderen Empfänger offengelegt, gilt Artikel 14 Absatz 3 Buchstabe a DSGVO, sodass die betroffene Person spätestens innerhalb eines Monats informiert werden muss.

Bereits bestehende Formulare für Datenerhebungen müssen an die neuen gesetzlichen Vorgaben angepasst und ergänzt werden.

Anlage 5b enthält einen Mustertext mit allen nach Artikel 14 DSGVO vorgeschriebenen Angaben und Ausfüllhinweisen. Bei Verwendung dieses Mustertextes sind die dort enthaltenen Angaben vollständig und auf die jeweilige Verarbeitungstätigkeit angepasst zur Verfügung zu stellen.

### 9.2.3 Informationspflichten bei einer Verwendung personenbezogener Daten zu einem anderen Zweck

Beabsichtigt der Verantwortliche, bereits vorhandene personenbezogene Daten für einen anderen Zweck weiterzuverarbeiten als für denjenigen, für den die personenbezogenen Daten erhoben wurden, so hat er der betroffenen Person vor dieser Weiterverarbeitung Informationen über den anderen Zweck und weitere maßgebliche Informationen zur Verfügung zu stellen (Artikel 13 Absatz 3 DSGVO bzw. Artikel 14 Absatz 4 DSGVO).

a) Liegt eine Zweckänderung vor?

Artikel 5 Absatz 1 Buchstabe b DSGVO legt als Grundsatz fest, dass die Verarbeitung personenbezogener Daten immer zu einem oder mehreren festgelegten Zwecken erfolgen muss. Die Zwecke der Datenverarbeitung sollen zum Zeitpunkt der Datenverarbeitung bereits feststehen (Erwägungsgrund 39 DSGVO). Eine anlasslose Datensammlung ist somit unzulässig.

Bei öffentlichen Stellen werden die Zwecke durch den Verantwortlichen im Rahmen der gesetzlich zugewiesen Aufgaben festgelegt. Sobald eine Verarbeitung erfolgen soll, die

nicht mehr von den vorher konkret festgelegten Zwecken umfasst ist, liegt eine Zweckänderung vor.

Von der Frage des Vorliegens einer Zweckänderung zu trennen ist die Frage, ob die Verarbeitung zu dem neuen Zweck auch zulässig ist.

Die Kriterien für die Zulässigkeit einer Zweckänderung ergeben sich entweder aus Rechtsvorschriften außerhalb der DSGVO oder aus der DSGVO selber. Außerhalb der DSGVO finden sich insbesondere in § 15 Absatz 1 BlnDSG Regelbeispiele für typische Zweckänderungsgründe, deren Zulässigkeit vom Gesetzgeber bei Vorliegen der jeweiligen Voraussetzungen vermutet wird. In der DSGVO findet sich eine solche Vermutung zur Zulässigkeit in Artikel 5 Absatz 1 Buchstabe b für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke. Fehlt es an einer konkreten gesetzlichen Regelung für die Zulässigkeit der Zweckänderung, richtet sich diese nach Artikel 6 Absatz 4 DSGVO.

b) Gibt es Ausnahmen von der Informationspflicht?

Für die Informationspflichten im Falle einer Zweckänderung gelten ebenfalls die Ausnahmen der Artikel 13 Absatz 4 und Artikel 14 Absatz 5 DSGVO, insbesondere Artikel 14 Absatz 5 Buchstabe c DSGVO, wonach keine Informationspflicht besteht, wenn eine gesetzliche Vorschrift die Erlangung oder Offenlegung ausdrücklich regelt.

Zusätzliche Ausnahmen können sich aus § 15 Absatz 3 BlnDSG ergeben, wenn:

- es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist,
- sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden erforderlich erscheint oder
- der Zugriff auf die personenbezogenen Daten erforderlich ist und der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der internen Revision, der Rechnungsprüfung oder der Durchführung von Organisationsmaßnahmen dient

und ohne Absehen von der Information der jeweilige Zweck der Verarbeitung gefährdet wäre. Wie auch in den Ausnahmefällen des § 23 BlnDSG besteht eine Dokumentationspflicht über den jeweiligen Hinderungsgrund und die Verpflichtung, die Information nach Wegfall des Hindernisses, spätestens jedoch zwei Wochen, nachzuholen.

c) Zeitpunkt, Form und Inhalt der Information

Bei einer beabsichtigten Weiterverarbeitung von Daten zu einem anderen Zweck als dem, der bei der Erhebung zugrunde lag, ist die betroffene Person vor dieser Weiterverarbeitung zu informieren. Dies gilt unabhängig davon, ob die Daten durch eine Erhebung direkt bei der betroffenen Person (Artikel 13 Absatz 3 DSGVO) oder durch eine Erhebung auf andere Weise (Artikel 14 Absatz 4 DSGVO) erlangt worden sind.

Die betroffene Person ist über den neuen Zweck und alle anderen maßgeblichen Informationen gemäß Artikel 13 Absatz 2 bzw. Artikel 14 Absatz 2 DSGVO zu informieren.

Anlage 5a enthält unter dem Punkt *Sonderfall* einen Mustertext und Ausfüllhinweise für Zweckänderungen, wenn die Daten direkt bei der betroffenen Person erhoben wurden (Artikel 13 Absatz 3 DSGVO). Anlage 5b enthält unter dem Punkt *Sonderfall* einen Mus-

tertext und Ausfüllhinweise für Zweckänderungen, wenn die Daten nicht bei der betroffenen Person erhoben wurden (Artikel 14 Absatz 4 DSGVO). Bei Verwendung dieser Mustertexte sind die dort enthaltenen Angaben vollständig und auf die jeweilige Verarbeitungstätigkeit angepasst zur Verfügung zu stellen.

### 9.2.4 Informationspflicht bei einer Videoüberwachung öffentlich zugänglicher Räume

§ 20 BlnDSG enthält Vorschriften zur Videoüberwachung öffentlich zugänglicher Räume.

***Exkurs:***

*Die Videoüberwachung von für die Öffentlichkeit nicht zugänglichen Räumen (z.B. Innenbereiche gefährdeter Liegenschaften) richtet sich nach der DSGVO. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten von Beschäftigten in diesem Zusammenhang kommt § 18 BlnDSG i.V.m. § 26 BDSG in Betracht. Soweit Dritte betroffen sind (z.B. Lieferanten, Handwerker) kann Artikel 6 Absatz 1 Satz 1 Buchstabe b DSGVO als Rechtsgrundlage dienen, dessen Voraussetzungen im Einzelfall zu prüfen sind. Sowohl gegenüber Beschäftigten als auch gegenüber Vertragspartnern gelten die Informationspflichten der Artikel 13 und 14 DSGVO, einschließlich der Ausnahmen, insbesondere wenn die betroffenen Personen bereits über die mitzuteilenden Informationen verfügen.*

Für die Videoüberwachung öffentlich zugänglicher Räume ordnet § 20 Absatz 2 BlnDSG an, dass videoüberwachte Bereiche so zu kennzeichnen sind, dass Personen vor dem Betreten über den Umstand der Videoüberwachung sowie über den Namen und die Kontaktdaten des Verantwortlichen informiert werden. Damit sind bereits bestimmte Informationen mitzuteilen, bevor eine Erhebung personenbezogener Daten erfolgt und somit bevor die Informationspflichten der Artikel 13 und 14 DSGVO ausgelöst werden.

Daraus folgt, dass bei videoüberwachten Bereichen eine Kennzeichnung, beispielsweise durch ein standardisiertes Bildsymbol (vgl. Artikel 12 Absatz 7 DSGVO) einer Kamera, verbunden mit Namen und Kontaktdaten des Verantwortlichen so angebracht werden muss, dass betroffene Personen selber entscheiden können, ob sie sich in den überwachten Bereich begeben. Der Hinweis muss nicht vor dem Eingang des überwachten Bereiches angebracht werden, sondern er kann beispielsweise auch im überwachten Bereich angebracht werden, wenn er von außerhalb deutlich wahrgenommen werden kann.

Begibt sich eine Person in Kenntnis der Videoüberwachung in den überwachten Bereich, stellt diese Person selber personenbezogene Daten zur Verfügung, so dass die Informationspflichten des Artikels 13 Absatz 1 und 2 DSGVO (Erhebung personenbezogener Daten bei der betroffenen Person) ausgelöst werden. Sofern nicht bereits im Zusammenhang mit dem Hinweis nach § 20 Absatz 2 BlnDSG auch alle anderen Informationen gemäß Artikel 13 DSGVO mitgeteilt worden sind (eine weitere Information wäre dann gemäß Artikel 13 Absatz 4 DSGVO nicht mehr erforderlich), empfiehlt es sich, die weiteren Hinweise beispielsweise durch einen Aushang im überwachten Bereich mitzuteilen. Ob die Informationspflichten auch erfüllt werden können, indem auf der Kennzeichnung des überwachten Bereiches neben dem Verantwortlichen und dessen Kontaktdaten auf die Internetseite mit allen weiteren Informationen hingewiesen wird, ist noch nicht geklärt. Für eine rechtssichere Gestaltung empfiehlt sich jedoch bereits deshalb ein vollständiger Aushang, um auch Personen ohne Internetzugang die Kenntnisnahme zu ermöglichen.

Sofern durch die Videoüberwachung keine personenbezogenen Daten erhoben werden, z.B. weil bei Weitwinkelaufnahmen eine Identifizierung einzelner Personen nicht möglich ist, un-

terfällt eine solche Verarbeitung weder der DSGVO noch dem BlnDSG. In diesen Fällen können sich jedoch aus bereichsspezifischen Gesetzen besondere Regelungen ergeben. Solche Fälle dürften allerdings angesichts der Auflösungsmöglichkeiten moderner Kameras, bereits im Niedrigpreissegment, seltene Ausnahmefälle darstellen.

### 9.3 Auskunftsrecht und Akteneinsichtsrecht der betroffenen Person

#### 9.3.1 Auskunftsrecht

Das Auskunftsrecht nach Artikel 15 DSGVO in Verbindung mit § 24 BlnDSG ersetzt den bisherigen § 16 BlnDSG-alt. Das Auskunftsrecht besteht nunmehr bezüglich aller personenbezogenen Daten und ist nicht mehr auf automatisiert verarbeitete Daten beschränkt. Neu ist zudem der ausdrückliche Anspruch auf Auskunft darüber, *ob* personenbezogene Daten über eine Person gespeichert werden. Ist dies der Fall, besteht ein Anspruch auf Auskunft über die Umstände der Datenverarbeitung.

Die Einzelheiten des Auskunftsrechts ergeben sich aus Artikel 15 DSGVO. Besonders soll auf Folgendes hingewiesen werden:

- Anders als bisher kann die Auskunft über die Empfänger personenbezogener Daten auch durch eine Auskunft über Kategorien von Empfängern ersetzt werden. Eine Auskunft über Kategorien von Empfängern kann sich insbesondere empfehlen, wenn die Identität der Empfänger nicht gespeichert wird, aus rechtlichen Gründen nicht mitgeteilt werden darf oder wenn eine große Anzahl von Empfängern vorliegt, die nach sinnvollen Kriterien gegliedert werden können.
- Im Rahmen der Auskunftserteilung ist auch mitzuteilen, dass ein Anspruch auf Berichtigung oder Löschung der personenbezogenen Daten oder auf Einschränkung der Verarbeitung und ein Beschwerderecht bei der Aufsichtsbehörde besteht.

Das Auskunftsrecht des Artikels 15 umfasst nach dessen Absatz 3 Satz 1 auch die Zur-Verfügung-Stellung einer Kopie der personenbezogenen Daten. Hintergrund der Regelung ist, dass die betroffene Person die Möglichkeit haben soll, sich einen unmittelbaren Eindruck über die Verarbeitung ihrer personenbezogenen Daten beim Verantwortlichen zu verschaffen. Die Kopie darf deshalb nicht besonders aufbereitet werden. Zulässig sind lediglich Schwärzungen zu Daten, die nach Artikel 15 Absatz 4 DSGVO nicht mitgeteilt werden dürfen (z.B. personenbezogene Daten Dritter oder Betriebs- und Geschäftsgeheimnisse). Der Begriff „zur Verfügung stellen“ bedeutet das Bereithalten einer Kopie und das Angebot zur Aushändigung. Eine unaufgeforderte Aushändigung der Kopie ohne ausdrückliche oder zumindest konkludente Aufforderung durch die betroffene Person ist nicht erforderlich.

Wird eine große Menge an Informationen über die betroffene Person verarbeitet, kann eine Präzisierung verlangt werden, auf welche Informationen oder Verarbeitungsvorgänge sich das Auskunftsersuchen bezieht (Erwägungsgrund 63 DSGVO).

Im Rahmen der Auskunft werden personenbezogene Daten übermittelt. Deshalb muss der Verantwortliche sicherstellen, dass diese Daten tatsächlich an die betroffene Person und nicht an Dritte (z.B. bei Namensgleichheit) mitgeteilt werden. Eine eindeutige Identifizierung ist dafür zwingend erforderlich. Sofern eine Identifizierung anhand des Antrages allein nicht möglich ist, sollen weitere Informationen zur Identifizierung angefordert werden (Artikel 12 Absatz 6 DSGVO). Kann auch trotz Nutzung aller vertretbaren Mittel (Erwägungsgrund 64

DSGVO) keine sichere Identifizierung erfolgen, muss das Auskunftsersuchen abgelehnt werden (vgl. Artikel 11 Absatz 2 DSGVO).

***Beispiel:***

*Eine Person stellt per E-Mail einen Antrag auf Auskunft und teilt dazu ihren Namen mit. In der Behörde existiert eine Akte zu diesem Namen. Eine Auskunftserteilung an die E-Mail-Adresse des Antragstellers kommt regelmäßig nicht in Betracht, weil nicht gewährleistet werden kann, dass die E-Mail-Adresse tatsächlich der betroffenen Person zugeordnet ist (auch wenn Artikel 15 Absatz 3 Satz 3 DSGVO einen anderen Eindruck vermittelt). Ausnahmen können sich ergeben, wenn sichergestellt werden kann, dass ausschließlich die betroffene Person auf das E-Mailpostfach zugreifen kann. Dann müssen zusätzlich aber technisch-organisatorische Maßnahmen ergriffen werden, um das Mitlesen durch Dritte zu verhindern (z.B. durch Verschlüsselung). Scheidet eine Antwort per E-Mail aus, muss geprüft werden, ob die Auskunft durch Zusendung der Daten an die aus den Akten bekannte Anschrift erfolgen kann. Durch postalische Übersendung kann durch das strafrechtlich abgesicherte Postgeheimnis sichergestellt werden, dass keine anderen Personen, als der Adressat, an die Daten gelangen können. Geht aus der Akte keine (aktuelle) Anschrift hervor, muss dies dem Antragsteller (per E-Mail) mitgeteilt werden und dieser muss darauf hingewiesen werden, dass eine Auskunft nur erfolgen kann, wenn dieser seine Identität nachweist (Artikel 11 Absatz 2 DSGVO in Verbindung mit Artikel 12 Absatz 2 DSGVO).*

### 9.3.2 Akteneinsichtsrecht

In § 24 Absatz 6 BlnDSG wurde das bereits vorher in § 16 Absatz 4 BlnDSG-alt enthaltene Akteneinsichtsrecht übernommen. Die Akteneinsicht stellt eine spezielle Form der Auskunft dar, sie kann eine aktive Zusammenstellung und Mitteilung der vorhandenen personenbezogenen Daten, wie sie der betroffenen Person nach Artikel 15 Absatz 1 DSGVO zusteht, jedoch nicht ersetzen. Die Akteneinsicht ist daher immer zusätzlich zu gewähren, wenn ein entsprechender Wunsch geäußert wird. Äußert die betroffene Person in Kenntnis ihres weitergehenden Auskunftsrechts ausdrücklich, dass ausschließlich eine Akteneinsicht gewünscht wird, kann von einer weitergehenden Auskunft abgesehen werden. Wünscht die Person im Rahmen der Akteneinsicht die Aushändigung einer Kopie, ist diese nach Artikel 15 Absatz 3 DSGVO unentgeltlich auszuhändigen.

Das Akteneinsichtsrecht gilt nicht nur für die personenbezogenen Daten, sondern auch für die Informationen, die mit den personenbezogenen Daten im Zusammenhang stehen. Dies folgt aus der Regelung in § 24 Absatz 6 Satz 3 BlnDSG. Danach ist eine Einsichtnahme grundsätzlich unzulässig, wenn die personenbezogenen Daten untrennbar mit geheimhaltungsbedürftigen nicht personenbezogenen Daten verbunden sind. Eine solche Regelung wäre nicht erforderlich, wenn das Akteneinsichtsrecht ohnehin nur auf die personenbezogenen Daten beschränkt wäre. Aus der Regelung folgt stattdessen, dass die Einsichtnahme in nicht-personenbezogene und nicht geheimhaltungsbedürftige Daten grundsätzlich zulässig ist, wenn diese Daten mit personenbezogenen Daten verbunden sind. Für die Frage, welche nicht-personenbezogenen Daten geheimhaltungsbedürftig sind, können die Regelungen der §§ 6 ff. IFG entsprechend herangezogen werden.

Für die Einsichtnahme in nicht-automatisiert geführte Akten können Hinweise zum Auffinden gefordert werden, wenn die Suche ansonsten einen unverhältnismäßigen Aufwand erfordern würde. Dies kann z.B. bei umfangreichen Aktensammlungen der Fall sein, die komplett auf

das Vorhandensein personenbezogener Daten der betroffenen Person geprüft werden müssen. In einem solchen Fall können beispielsweise Angaben dazu gefordert werden, zu welchem Zeitpunkt oder auch aus welchem Anlass die betroffene Person mit dem Verantwortlichen in Kontakt stand, um die Suche zeitlich oder thematisch eingrenzen zu können.

Für automatisiert geführte Akten sollte eine Recherche über die Suchfunktion mit geringerem Aufwand möglich sein. Sollte aufgrund von Besonderheiten der verwendeten Software keine automatisierte Suche möglich sein, kann nach dem Erwägungsgrund 63 DSGVO eine Konkretisierung gefordert werden.

### 9.4 Recht auf Löschung („Recht auf Vergessenwerden“)

Die Verpflichtung zur Löschung ergibt sich nunmehr aus Artikel 17 DSGVO. Die wichtigsten Fallgruppen, in denen die Löschung von Daten verlangt werden kann, bleiben erhalten.

Anders als der Wortlaut von Artikel 17 Absatz 1 Buchst. a DSGVO zunächst vermuten lässt, besteht eine Löschpflicht - wie bisher - nicht nur, wenn die betroffene Person dies verlangt, sondern immer dann, wenn die personenbezogenen Daten für die Zwecke, für die sie verarbeitet wurden, nicht mehr erforderlich sind.

Nach Artikel 17 Absatz 3 Buchstabe b DSGVO scheidet eine Löschung z.B. auch weiterhin aus, wenn gesetzliche Aufbewahrungsfristen bestehen.

Das Zusammenspiel zwischen Löschpflichten und der Pflicht, abgeschlossene Akten dem Landesarchiv anzubieten, ist in § 25 BlnDSG geregelt. Danach gilt Folgendes:

- Zunächst ist zu prüfen, ob eine Verpflichtung zur Löschung personenbezogener Daten besteht, weil der Verarbeitungszweck erfüllt und die weitere Aufbewahrung für die Verarbeitungszwecke nicht mehr erforderlich ist (Artikel17 Absatz 1 Buchstabe a DSGVO).
- Ergibt die Prüfung, dass die personenbezogenen Daten gelöscht werden müssen, greift § 25 BlnDSG ein und schiebt die Löschungspflicht bis zu einer Entscheidung des Landesarchivs, längstens aber bis zu einer im Archivgesetz geregelten Frist (aktuell: 12 Monate) hinaus. Zugleich wird die Löschungsverpflichtung durch § 25 Satz 2 BlnDSG in eine Pflicht umgewandelt, die Akten dem Archiv auch tatsächlich anzubieten.
- Bei Ablehnung der Übernahme ins Archiv oder nach Ablauf der Entscheidungsfrist sind die Daten zu löschen.

Keine Ausnahme von der Verpflichtung zur Löschung besteht mehr in den Fällen, in denen personenbezogene Daten in Akten gespeichert waren (§ 17 Absatz 6 BlnDSG-alt). Anders als bisher ist bei einer Verarbeitung (im Rahmen der Speicherung von Vorgängen) in Akten zu prüfen, ob ein Vorgang weiterhin gespeichert werden muss, weil er für die Aufgabenerfüllung erforderlich ist oder ob er und die dabei verarbeiteten Daten gelöscht werden können. Begrifflich ist dabei die „Akte“ vom „Vorgang“ zu unterscheiden. Ein Vorgang umfasst in der Regel ein in sich abgeschlossenes (Verwaltungs-)Verfahren, beispielsweise die Bearbeitung eines Antrags von der Antragstellung bis zur Bescheidung, einschließlich eines etwaigen Rechtsbehelfsverfahrens oder die Bearbeitung einer Anfrage/Beschwerde. Vorgänge werden in Akten geführt. Enthält eine Akte mehrere Vorgänge mit personenbezogenen Daten, ist zu prüfen, ob der konkrete Vorgang weiterhin für die Aufgabenerfüllung (Zweck der Verarbei-

tung) erforderlich ist. Dementsprechend ist es möglich, dass Vorgänge aus Akten gelöscht werden müssen, bevor die Gesamtakte gelöscht wird.

Nicht vom Löschungsgebot umfasst ist die Aussonderung personenbezogener Daten aus Vorgängen, wenn der Verwaltungsvorgang insgesamt weiterhin gespeichert werden muss. Unter Umständen kann sich jedoch bei der Bearbeitung bestimmter Verfahren ergeben, dass nur ein Teil der Unterlagen dauerhaft zu speichern ist, andere, abtrennbare Teile, jedoch nicht dauerhaft benötigt werden und daher zu löschen sind. In diesen Fällen ist zu prüfen, in welcher Weise dem für diese Teile bestehenden Löschungsgebot Rechnung getragen werden kann.

In Artikel 17 Absatz 2 DSGVO ist mit dem „Recht auf Vergessenwerden“ eine Erweiterung des Löschungsanspruchs normiert: Ein Verantwortlicher, der zur Löschung personenbezogener Daten verpflichtet ist, diese aber zuvor öffentlich gemacht hat, muss Maßnahmen treffen, um andere Verantwortliche, die diese Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt hat. Für den Verantwortlichen bedeutet das konkret, dass er andere Verantwortliche ermitteln und informieren muss. Allerdings müssen die zu treffenden Maßnahmen angemessen sein. Insbesondere sind die verfügbaren Technologien und die Implementierungskosten zu berücksichtigen.

### 9.5 Recht auf Einschränkung der Verarbeitung

Das Recht auf Einschränkung der Verarbeitung findet sich in Artikel 18, die Begriffserklärung in Artikel 4 Nummer 3 DSGVO. Eine nähere Erläuterung zu dem Begriff *Einschränkung der Verarbeitung* findet sich im Erwägungsgrund 67 DSGVO. Demnach zählen dazu Methoden zur Beschränkung der Verarbeitung personenbezogener Daten, z.B. dass ausgewählte personenbezogene Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzer gesperrt werden oder dass veröffentlichte Daten vorübergehend von einer Webseite entfernt werden. Damit entspricht dieses Recht im weitesten Sinne dem bisherigen Recht auf Sperrung nach § 4 Absatz 2 Nummer 5 BlnDSG-alt.

Im Falle der Einschränkung der Verarbeitung ist der Verantwortliche gemäß Artikel 19 DSGVO (wie bisher nach § 17 Absatz 5 BlnDSG-alt) verpflichtet, Dritte, an welche die Daten übermittelt wurden, zu informieren, damit diese ihre Verarbeitungsprozesse selbst einschränken können. Diese Pflicht greift nur insoweit, wie die Unterrichtung möglich und dem Verantwortlichen nicht unzumutbar ist.

### 9.6 Sonstige Rechte der betroffenen Person

#### 9.6.1 Recht auf Berichtigung

Das Recht auf Berichtigung folgt aus Artikel 16 DSGVO. Eine ähnliche Regelung bestand bereits in § 17 Absatz 1 BlnDSG-alt. Die betroffene Person hat nach Artikel 16 DSGVO auch weiterhin das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten verlangen zu können. Zudem hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten verlangen zu können. Bei der Frage, ob Daten unvollständig sind, ist der Zweck der Verarbeitung zu berücksichtigen. Personenbezogene Daten sind dann unvollständig, wenn sie für sich genommen zwar richtig sind, aber bezogen auf den Verarbeitungszweck ein unzutreffendes

Bild der betroffenen Person ergeben, dass durch die fehlenden Daten korrigiert werden kann.

***Beispiel:***

*Bei einem Gewerbetreibenden wird seine Zuverlässigkeit überprüft. Aus den Akten geht hervor, dass er Steuerschulden hat, was gegen seine Zuverlässigkeit sprechen kann. Diese Information ist dann unvollständig, wenn in der Sache ein finanzgerichtliches Verfahren anhängig ist und darauf nicht hingewiesen wird.*

### 9.6.2 Recht auf Datenübertragbarkeit

Nach Artikel 20 DSGVO haben betroffene Personen das Recht, die sie betreffenden personenbezogenen Daten, die sie einem für die Verarbeitung Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie haben das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die Daten bereitgestellt wurden, zu übermitteln. Dieses Recht soll dann bestehen, wenn eine automatisierte Datenverarbeitung zur Durchführung eines Vertrags erfolgte oder auf einer Einwilligung basierte. Es gilt dagegen nicht, soweit die Verarbeitung zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, erforderlich ist (Artikel 20 Absatz 3 Satz 2 DSGVO). Der Anwendungsbereich wird somit für öffentliche Stellen sehr gering sein.

### 9.6.3 Widerspruchsrecht

Gemäß Artikel 21 DSGVO hat die betroffene Person (wie bisher gemäß § 17 Absatz 7 BlnDSG-alt) ein allgemeines Widerspruchsrecht gegen eine an sich rechtmäßige Verarbeitung von personenbezogenen Daten, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt oder aufgrund des berechtigten Interesses des Verantwortlichen oder eines Dritten erfolgt. Dabei ist Voraussetzung, dass die betroffene Person Gründe geltend macht, die sich aus ihrer besonderen Situation ergeben. Denkbar sind beispielsweise rechtliche, wirtschaftliche, ethische, soziale, gesellschaftliche oder familiäre Zwangssituationen. Ist bereits eine Datenschutzverletzung durch den Verantwortlichen eingetreten und ist zu befürchten, dass weitere Verletzungen folgen, kann auch dies zu einem Widerspruchsrecht führen.

Die betroffene Person hat den Widerspruch mit Tatsachen zu begründen, die vom Verantwortlichen zu prüfen sind. Es wird empfohlen, diese Prüfung zu dokumentieren. Der Verantwortliche darf bei einem rechtmäßig eingelegten Widerspruch die Daten nur noch verarbeiten, wenn er zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.

## 9.7 Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten

Verletzungen des Schutzes personenbezogener Daten (Datenpannen), die voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen, sind künftig der Berliner Beauftragten für Datenschutz und Informationsfreiheit zu melden (Artikel 33 DSGVO).

Geht von der Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen aus, sind auch die betroffenen Personen zu benachrichtigen (Artikel 34 DSGVO).

## 10. Auftragsverarbeitung

Vergleichbar zu § 3 BlnDSG-alt enthält die DSGVO in den Artikeln 28 und 29 Regelungen darüber, wann eine Auftragsverarbeitung vorliegt und welche spezifischen Anforderungen an die Ausgestaltung zu stellen sind, also das „wie“ der Auftragsverarbeitung. Davon zu trennen ist die Frage, „ob“ eine Auftragsverarbeitung zulässig ist. Hierzu können im bereichsspezifischen Bundes- oder Landesrecht besondere Regelungen enthalten sein (vgl. z.B. § 80 SGB X).

### 10.1 Neue Regelungen

Gegenüber der bisherigen Rechtslage ergeben sich auch über Artikel 28 und 29 DSGVO hinaus folgende Änderungen:

- Der Mindestinhalt eines Vertrages zur Auftragsverarbeitung ist umfassender.
- Der Vertrag zur Auftragsverarbeitung kann nicht nur schriftlich sondern auch in einem elektronischen Format geschlossen werden.
- Weisungen des Verantwortlichen an den Auftragsverarbeiter sind zu dokumentieren.
- Der Auftragsverarbeiter hat ein eigenes Verzeichnis von Verarbeitungstätigkeiten zu erstellen (Artikel 30 Absatz 2 DSGVO).
- Will der Auftragsverarbeiter Subunternehmen als weitere Auftragsverarbeiter bei der Erbringung der vereinbarten Dienstleistung einsetzen, so bedarf dies der vorherigen (schriftlichen oder elektronischen) Genehmigung durch den Verantwortlichen. Später beabsichtigte Änderungen bei den eingesetzten Subunternehmen muss der Auftragsverarbeiter vorher mitteilen, wobei der Verantwortliche dann bei Bedarf Einspruch gegen die geplante Einbeziehung des neuen Subunternehmens erheben kann.
- Der Spielraum bei der Kontrolle des Auftragsverarbeiters durch den Verantwortlichen vergrößert sich. Es ist z.B. nicht mehr zwingend eine Vorortkontrolle erforderlich, sondern es kann auch auf Zertifizierungen zurückgegriffen werden.
- Auftragsverarbeiter haben künftig Dokumentationspflichten und gegenüber dem Verantwortlichen eine Unterstützungsfunktion.
- Die Verpflichtung, für die Sicherheit der Verarbeitung zu sorgen trifft auch den Auftragsverarbeiter (Artikel 32 Absatz 1 DSGVO).
- Aufsichtsbehörden können Sanktionen direkt gegenüber dem Auftragsverarbeiter verhängen.
- Verantwortlicher und Auftragsverarbeiter haften gegenüber betroffenen Personen gesamtschuldnerisch auf Schadenersatz bei Datenschutzverstößen. Der Auftragsverarbeiter kann daher von betroffenen Personen direkt in Anspruch genommen werden (Artikel 82 DSGVO).

### 10.2 Zwingender Vertragsinhalt bei der Auftragsverarbeitung

Artikel 28 Absatz 3 DSGVO legt detailliert fest, welcher Mindestinhalt in den Vertrag aufgenommen werden muss. Die dortigen Festlegungen gehen über die bisherigen Regelungen in § 3 BlnDSG-alt hinaus. Im Vertrag sind Festlegungen zu treffen:

- zum Gegenstand der Verarbeitung (z.B. Verweis auf die Leistungsvereinbarung des Vertrags; Darstellung der konkreten Aufgaben),
- zur Dauer der Verarbeitung (Beispiele: Laufzeit des Vertrages, Befristung, einmalige Ausführung),
- zum Zweck der Verarbeitung (z.B. Verweis auf die Leistungsvereinbarung, Beschreibung des Zwecks),
- zur Art der Verarbeitung (z.B. automatisierte Verarbeitung, Erheben, Erfassen, Ordnen),
- zur Art der verarbeiteten personenbezogenen Daten (z.B. Adressdaten, Personenstammdaten, Telekommunikationsdaten, Daten aus öffentlichen Verzeichnissen)
- zu den Kategorien betroffener Personen (z.B. Antragsteller, Beschäftigte, Ansprechpartner etc.),
- zu den Pflichten und Rechten des Verantwortlichen (z.B. Ausgestaltung des Weisungsrechts oder der Kontrollmöglichkeiten, vgl. auch die nachfolgenden Regelungen).

Darüber hinaus hat der Vertrag dahingehend Regelungen zu enthalten, dass der Auftragsverarbeiter:

- die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten darf, es sei denn, er ist durch andere Vorschriften zur Verarbeitung verpflichtet,
- gewährleistet, dass sich die Mitarbeiter, die die Daten verarbeiten, zur Vertraulichkeit verpflichten oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen,
- technische und organisatorische Maßnahmen für die Sicherheit der Verarbeitung ergreift,
- die Bedingungen für die Inanspruchnahme eines weiteren Auftragsverarbeiters eingehalten werden,
- den Verantwortlichen bei der Erfüllung der diesem obliegenden Beantwortung von Anträgen zur Wahrnehmung von Betroffenenrechten unterstützt,
- den Verantwortlichen bei der Gewährleistung der Sicherheit der Verarbeitung sowie den Melde- und Benachrichtigungspflichten bei Datenschutzverstößen unterstützt,
- nach Erbringung der Verarbeitungsleistungen die personenbezogenen Daten löscht oder zurückgibt,
- dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellt und Überprüfungen zulässt.

Für den Anpassungsprozess bedeutet dies insbesondere, dass bestehende Verträge zu überprüfen und ggf. durch ergänzende Vereinbarungen an die neue Rechtslage anzupassen

sind. Als Grundlage des Überprüfungsprozesses kann der Mustervertragsentwurf der Anlage 6 genutzt werden. Auf welche Weise eine ggf. erforderliche Anpassung erfolgt, z.B. durch eine einvernehmliche Vertragsänderung/ -ergänzung, aufgrund von § 313 BGB wegen einer Änderung der Geschäftsgrundlage oder im Wege einer außerordentlichen Kündigung aus wichtigem Grund, ist im Einzelfall zu bewerten und zu entscheiden.

Soweit den Verantwortlichen aufgrund des neunen Datenschutzrechts neue Verpflichtungen treffen, zu deren Erfüllung er der Unterstützung durch den Auftragsverarbeiter bedarf, kann auch eine Unterstützungspflicht aufgrund von § 241 Absatz 2 BGB in Betracht kommen. Unabhängig davon sollten die jeweiligen Rechte und Pflichten möglichst umfassend im jeweiligen Vertrag geregelt werden.

## 11. Technischer und organisatorischer Datenschutz

Die DSGVO enthält vor allem in Artikel 5 und Artikel 32 Vorgaben zur Sicherheit der Verarbeitung, die in § 26 BlnDSG näher konkretisiert werden. Beibehalten wird das grundsätzliche Prinzip, dass geeignete technische und organisatorische Maßnahmen zu treffen sind, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten (bisher § 5 Absatz 1 BlnDSG-alt). Die Angemessenheit orientiert sich dabei an dem Stand der Technik, den Implementierungskosten, der Art und dem Umfang der Umstände, dem Zweck der Verarbeitung sowie an den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Ausdrücklich aufgeführt werden als Maßnahmen in Artikel 32 Absatz 1 Buchstabe a DSGVO lediglich Pseudonymisierung und Verschlüsselung der Daten.

Die bisherigen sechs Schutzziele des BlnDSG (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz) werden in Artikel 32 Absatz 1 Buchst. b DSGVO zusammengefasst. Auch wenn lediglich Vertraulichkeit, Integrität und Verfügbarkeit sowie das neu hinzugekommene Schutzziel der Belastbarkeit in der DSGVO ausdrücklich genannt werden, sind auch die weiteren bereits bekannten Schutzziele von Artikel 32 Absatz 1 DSGVO umfasst. Während die ersten drei Schutzziele aus der ISO 27001 und dem IT-Grundschutz des BSI bekannt sind, bedarf das Schutzziel der Belastbarkeit mangels konkreter Vorgaben in der DSGVO einer Interpretation. Am naheliegendsten erscheint es, die Belastbarkeit von Diensten und Systemen hinsichtlich ihrer Widerstandsfähigkeit auszulegen, so dass diese also auch noch „unter Last / starker Beanspruchung“ ihre datenschutzrelevanten Eigenschaften beibehalten sollen, was ggf. in einem entsprechenden Notfallmanagement zu berücksichtigen wäre. Außerdem besteht gemäß Artikel 32 Absatz 1 Buchstabe c DSGVO die Forderung, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall schnell wiederhergestellt werden sollen. Dies war grundsätzlich auch schon bisher im Rahmen der Verfügbarkeit der Daten sicherzustellen. Die Wiederherstellung der Daten muss somit regelmäßig wiederkehrend getestet werden.

Weitere Vorgaben in Bezug auf den technischen und organisatorischen Datenschutz sind in Artikel 24, 25 sowie 32 DSGVO normiert. Hieraus ergeben sich folgende neue bzw. spezifizierte Anforderungen bei der Entwicklung und Umsetzung technischer und organisatorischer Maßnahmen:

- Vor Festlegung der technischen und organisatorischen Maßnahmen hat eine risikobasierte Abwägung zu erfolgen. Diese beinhaltet, dass alle möglichen Bedrohungen und Schwachstellen mit ihrer jeweiligen Eintrittswahrscheinlichkeit und der potentiel-

len Schwere des Schadens für die Rechte und Freiheiten betroffener Personen identifiziert werden.

- Die bisher bekannten Prinzipien der Datenvermeidung und -sparsamkeit werden durch Artikel 25 Absatz 1 und 2 DSGVO konkretisiert und fordern künftig Datenschutz durch Technikgestaltung und durch datenschutzrechtliche Voreinstellungen (Privacy by design und Privacy by default).
- Der Verantwortliche muss die technischen und organisatorischen Maßnahmen, die er getroffen hat, nachweisen und aktuell halten. Gemäß Artikel 32 Absatz 1 Buchst. d DSGVO muss nun auch die Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen regelmäßig wiederkehrend getestet und ggf. nachgesteuert werden.

## 12. Datengeheimnis, Dienstanweisungen

Die in § 8 BlnDSG-alt enthaltene Regelung, wonach Dienstkräften die unbefugte Verarbeitung personenbezogener Daten untersagt war, folgt nunmehr aus Artikel 29 DSGVO in Verbindung mit dem Grundsatz der Rechtmäßigkeit der Datenverarbeitung (Artikel 5 Absatz 1 DSGVO) und dem aus Artikel 6 Absatz 1 DSGVO folgenden Verbot zur Verarbeitung personenbezogener Daten, soweit nicht ein Erlaubnistatbestand des Artikels 6 Absatz 1 DSGVO erfüllt ist.
Die in § 8 BlnDSG-alt ebenfalls enthaltene Regelung, wonach Dienstkräfte ausdrücklich entsprechend zu verpflichten sind, ist in der DSGVO nicht enthalten. Aus Artikel 32 Absatz 4 DSGVO folgt jedoch, dass der Verantwortliche und der Auftragsverarbeiter Schritte zu unternehmen haben, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen oder aufgrund einer rechtlichen Verpflichtung verarbeiten. Die ausdrückliche Verpflichtung auf das Datengeheimnis kann ein geeigneter Schritt sein, um die Anforderungen des Artikels 32 Absatz 4 DSGVO zu erfüllen. Die Verpflichtung auf das Datengeheimnis kann zudem auch eine geeignete organisatorische Maßnahme im Sinne von Artikel 24 DSGVO sein, der dem Verantwortlichen ebenfalls Pflichten auferlegt.

Im Anwendungsbereich der JI-Richtlinie wurde eine Regelung zum Datengeheimnis in § 38 BlnDSG aufgenommen.

Zudem kommen insbesondere konkrete Verhaltensvorgaben in Dienstanweisungen, die Einweisung der Mitarbeiter zum Umgang mit personenbezogenen Daten an ihrem konkreten Arbeitsplatz oder Weisungen bezogen auf einen Einzelfall in Betracht, um die Pflichten des Verantwortlichen zur Sicherstellung einer rechtmäßigen Verarbeitung zu erfüllen.

Anlage 7 enthält ein Muster für eine schriftliche Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DSGVO.

Sofern in der Vergangenheit eine formelle Verpflichtung auf das Datengeheimnis erfolgt ist, ist eine „Nachverpflichtung“ der Mitarbeiter aufgrund der Geltung der DSGVO nicht erforderlich. Die verwendeten Formulare und Merkblätter sind jedoch für die künftige Verwendung entsprechend der DSGVO inhaltlich anzupassen.

## 13. Dokumentationspflichten und Datenschutzmanagement

Die DSGVO enthält eine Vielzahl von Dokumentationspflichten. Mit der Erfüllung dieser Pflichten wird der Nachweis erbracht, dass die Verarbeitung personenbezogener Daten im Einklang mit der DSGVO erfolgt. Insbesondere sind hervorzuheben:

- Nachweis der Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (Artikel 5 Absatz 1 u. 2 DSGVO),
- Nachweis der erteilten Einwilligungen (Artikel 7 Absatz 1 DSGVO),
- Nachweis der Einhaltung der Betroffenenrechte (gemäß Artikel 12 ff. DSGVO),
- Nachweis der technischen und organisatorische Maßnahmen (Artikel 24 Absatz 1, Artikel 25 und 32 DSGVO),
- Führung des Verzeichnisses der Verarbeitungstätigkeiten (Artikel 30 DSGVO),
- Dokumentation von Verletzungen des Schutzes personenbezogener Daten (Artikel 33 Absatz 5 DSGVO),
- Durchführung der Datenschutz-Folgenabschätzung (gemäß Artikel 35 DSGVO),
- Verträge über Auftragsverarbeitungen (gemäß Artikel 28 DSGVO).

Zudem folgen auch aus § 26 BlnDSG weitere Dokumentationspflichten, wenn die Verarbeitung personenbezogener Daten automatisiert erfolgt.

Zur Erfüllung der Aufgaben des Verantwortlichen im Hinblick auf den technischen und organisatorischen Datenschutz und den damit verbundenen Dokumentationspflichten empfiehlt es sich, ein strukturiertes Datenschutzkonzept zu entwickeln. Im Falle einer automatisierten Verarbeitung ist die Erstellung eines Datenschutzkonzepts zudem vor erstmaliger Inbetriebnahme und dann bei wesentlichen Änderungen gesetzlich vorgeschrieben (§ 26 Absatz 2 BlnDSG).

Wesentliche Bausteine eines solchen Konzepts sind Regelungen zu:

- Ziel und Gültigkeitsbereich,
- übergreifenden Leitlinien zum Datenschutz / Grundsätze der Verarbeitung personenbezogener Daten,
- Festlegungen zu Zuständigkeiten innerhalb der öffentlichen Stelle betreffend den Datenschutz (übergreifend und in Spezialfragen),
    - z.B. Festlegung der Abteilung, des Sachgebietes etc., welche oder welches für die Verarbeitung der Daten zuständig ist,
    - Zuständigkeit für die Bearbeitung von Beschwerden oder Auskunftsersuchen,
    - evtl. Festlegungen zur Auftragsverarbeitung,
    - frühzeitige Einbeziehung des Datenschutzbeauftragten in die Verfahrenseinführung bzw. bereits zum Zeitpunkt der Verfahrensausschreibung,
- Inventarisierung und Klassifizierung von Daten und Verarbeitungsvorgängen einschließlich ihrer Zuordnung zu Verarbeitungszwecken,
- zu durchlaufende Prozesse bei der Einführung neuer Verfahren,

- Vorgehen zur Erstellung von Datenschutzkonzepten für neue Verfahren,
- Maßnahmen zur Feststellung von Datenschutzpannen (z.B. durch regelmäßige Prüfung der Protokolldateien, Schulungen), Meldewegen, Zuständigkeiten und zum weiteren Umgang,
- Datenschutzbeauftragten (insbesondere Aufgaben und Stellung),
- Verzeichnissen von Verarbeitungstätigkeiten (einschließlich Vorfeldmaßnahmen wie Inventarisierung und Klassifizierung),
- Datenschutz-Folgenabschätzungen, einschließlich der Beteiligung von Betroffenen (Artikel 35 Absatz 9 DSGVO),
- Verfahren der Risikobestimmung und Bewertung, Feststellung des Schutzbedarfs,
- Regelmaßnahmen zur Durchsetzung der Datenschutzgrundsätze, zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen,
- Regelmaßnahmen zur Sicherheit, insbesondere zu infrastrukturellen und anderen behördenweit eingesetzten Verfahren und zu speziellen Verarbeitungen bzw. Datenkategorien, einschließlich physischer Sicherheit,
- organisatorische Richtlinien, insbesondere zum Nachweis der Einhaltung der DSGVO und zur Überwachung der technischen und organisatorischen Maßnahmen (z.B. Backup, Virenschutz, Protokollierung),
- Management von Einwilligungen,
- Gewährleistung der Betroffenenrechte (einschließlich Meldewege, Zuständigkeiten, Überwachung der Fristen, Muster für die Informationen),
- Regelungen für die Auftragsverarbeitung, einschließlich Musterverträgen, akzeptablen Garantien im Sinne von Artikel 28 Absatz 1 DSGVO und Überwachung der Auftragsverarbeiter,
- Datenschutz-Unterweisungen,
- regelmäßigen Datenschutz-Kontrollen und Audits,

## 14. Empfehlungen für den Anpassungsprozess

| Empfehlungen | Anmerkungen |
|---|---|
| Prüfung der Zulässigkeit der Datenverarbeitungen | • Prüfen, ob das neue Recht für alle Prozesse eine Rechtsgrundlage bereitstellt.<br>• Vorhandene Einwilligungen prüfen, um sicherzustellen, dass sie nach Wirksamwerden der DSGVO fortgelten.<br>• Überprüfung von Dienstvereinbarungen, Satzungsrecht, Verwaltungsvorschriften und Geschäftsordnungen im Hinblick auf die Vereinbarkeit mit der DSGVO. |

| | |
|---|---|
| Einführung eines Datenschutzmanagements<br><br>Insbesondere zur Erfüllung der Dokumentationspflichten | • Festlegung von Zuständigkeiten.<br>• Entwicklung eines Datenschutzkonzepts.<br>• Anpassung der technischen und organisatorischen Maßnahmen:<br>- technische und organisatorischen Maßnahmen im Rahmen des Datenschutzkonzepts dokumentieren,<br>- Etablierung eines Verfahrens, das regelmäßig die Wirksamkeit der technischen und organisatorischen Maßnahmen bewertet und evaluiert,<br>- Berücksichtigung der Prinzipien Privacy bei design und Privacy by default künftig bereits im Zuge der vergaberechtskonformen Ausschreibung von IT-Produkten. |
| Organisatorische Maßnahmen zu Betroffenenrechten festlegen | • Wer ist innerhalb der öffentlichen Stelle zuständig, wenn ein Betroffener seine Rechte geltend macht?<br>• In welcher Frist soll das Anliegen des Betroffenen weitergeleitet und bearbeitet werden (beachte: Monatsfrist nach DSGVO für die Antwort)?<br>• In welcher Form soll das Anliegen weitergeleitet werden (Stichwort: Geheimhaltung, Vertraulichkeit)?<br>• Wer sind die Ansprechpartner für verschiedene Datenverarbeitungssysteme (um beispielsweise den Auskunftsanspruch überall in der öffentlichen Stelle gewährleisten zu können)?Es sind Verfahren zu definieren, wie die Informationspflichten nach Artikel 13 und 14 DSGVO erfüllt werden sollen. Für Standardverarbeitungen empfiehlt sich die Verwendung von Mustern (dazu oben Ziffer 9.2). |
| Einführung oder Anpassung von Verfahren zur:<br>➢ Führung von Verarbeitungsverzeichnissen,<br>➢ Durchführung des Freigabeverfahrens,<br>➢ Durchführung der Datenschutz-Folgenabschätzung, | • Anpassung der bestehenden Verfahrensverzeichnisse an Artikel 30 DSGVO.<br>• Prüfen, ob für alle Verarbeitungen ein Verarbeitungsverzeichnis vorliegt.<br>• Berücksichtigung der an die DSGVO angepassten Inhalte des Freigabeverfahrens und der Freigabeerklärung.<br>• Die Vorabkontrolle gemäß § 19a BlnDSG-alt wird durch die Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO abgelöst und erfordert eine umfangreiche Dokumentation. |

| | |
|---|---|
| | • Für Verarbeitungen, von denen hohe Risiken ausgehen, muss keine Folgenabschätzung vorgenommen werden, wenn sie der Vorabkontrolle durch den Datenschutzbeauftragten unterlegen haben und ohne wesentliche Änderung fortgeführt werden. Einer Überprüfung der Verarbeitungen innerhalb der nächsten 2-3 Jahre sind die Anforderungen von Artikel 35 DSGVO zugrunde zu legen. |
| Bestellung eines behördlichen Datenschutzbeauftragten und Anpassungen des Aufgabenbereichs des behördlichen Datenschutzbeauftragten | • Bereits bestellte Datenschutzbeauftragte bleiben in ihrer Funktion.<br>• Ggf. Überprüfung der Qualifikation und Unabhängigkeit.<br>• Neue Aufgaben und Verantwortlichkeiten beachten.<br>• Sollen weitere Aufgaben übertragen werden, ist dies durch den Verantwortlichen zu regeln.<br>• Prüfen, ob angesichts der geänderten bzw. erweiterten Aufgaben die Ressourcen des Datenschutzbeauftragten ausreichend sind.<br>• Veröffentlichung der Kontaktdaten und Mitteilung an die Berliner Beauftragte für Datenschutz und Informationsfreiheit (Artikel 37 Absatz 7 DSGVO). |
| Beschäftigte ggf. zur Geheimhaltung verpflichten | • Im Rahmen organisatorischer Maßnahmen ist zu entscheiden, ob und in welcher Weise die Beschäftigten zur Einhaltung der datenschutzrechtlichen Erfordernisse verpflichtet und entsprechend belehrt werden.<br>• Ggf. bereits verwendete Vordrucke und Merkblätter sind an die DSGVO anzupassen. |
| Anpassung von Verträgen über Auftragsverarbeitungen | • Überprüfung der bestehenden Verträge, ob diese die Vorgaben von Artikel 28 DSGVO einhalten. |
| Prüfung, ob Datenschutz-Folgenabschätzungen erforderlich sind | • Wurde eine Vorabkontrolle durchgeführt?<br>• Lag der Vorabkontrolle eine Risikoanalyse und Sicherheitskonzept zugrunde?<br>• War eine Beteiligung der Aufsichtsbehörde erforderlich und ist diese erfolgt?<br>• Gab es zwischenzeitlich relevante Änderungen?<br>• Ist eine Wiederholung der Prüfung aufgrund eines längeren Zeitraumes erforderlich (empfohlen: alle 3 Jahre)? |