Anwendungshinweise des Ministeriums des Innern und für Kommunales des Landes Brandenburg zur Umsetzung der Anforderungen der EU-Datenschutz-Grundverordnung und des Brandenburgischen Datenschutzgesetzes in den öffentlichen Stellen des Landes Brandenburg

Version 2, Stand: April 2021

Inhaltsverzeichnis

Anlagenverzeichnis

1 Vorwort

Seit dem 25. Mai 2018 ist die von der Europäischen Union erlassene Datenschutz-Grundverordnung (DSGVO) für die öffentlichen Stellen des Landes Brandenburg unmittelbar anzuwenden. Der aktuelle Text der DSGVO kann auf EUR-Lex, dem Online-Portal zum EU-Recht, aufgerufen werden: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:02016R0679-20160504.

Nahezu zum gleichen Zeitpunkt wie die DSGVO (6. Mai 2018) war auch die Richtlinie (EU) 2016/680 der Europäischen Union (Richtlinie zum Datenschutz bei Polizei und Justiz) in das Recht der Mitgliedstaaten umzusetzen. Das Datenschutzrecht sowohl des Bundes als auch Brandenburgs war an die beiden Rechtakte der EU anzupassen. Der Bund hat ein neues Bundesdatenschutzgesetz (BDSG) erlassen, in Brandenburg hat der Landtag die Gesetze zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (BbgDSG) sowie das Gesetz zur Anpassung des bereichsspezifischen Rechts an die Verordnung (EU) 2016/679 am 25. April 2018 verabschiedet. Sie wurden am 8. Mai 2018 im Gesetz- und Verordnungsblatt für das Land Brandenburg verkündet (GVBl. I - 2018, Nr. 7 und GVBI. I - 2018, Nr. 8). Die Verkündungen können unter den folgenden Links aufgerufen werden:

- https://www.landesrecht.brandenburg.de/dislservice/public/gvbldetail.jsp?id=7633,
- https://www.landesrecht.brandenburg.de/dislservice/public/gvbldetail.jsp?id=7634.

Beide Gesetze traten gemeinsam mit dem Wirksamwerden der DSGVO am 25. Mai 2018 in Kraft. Dies führt seit dem 25. Mai 2018 zu einer neuen Struktur des Datenschutzrechts. Die DSGVO ist als europäische Verordnung unmittelbar geltendes Recht. Damit kommt ihr ein Anwendungsvorrang vor jedem nationalen Recht zu. Ergänzend zur DSGVO als direkt anwendbares Recht haben die öffentlichen Stellen Brandenburgs das BbgDSG und – je nach Verwaltungsbereich – weiterhin auch bereichsspezifische datenschutzrechtliche Vorschriften zu beachten. Wie bisher gilt, dass diese bereichsspezifischen Datenschutzvorschriften den Vorschriften des BbgDSG vorgehen.

Wegen der Strukturveränderungen bleiben im BbgDSG nur wenige materielle Kernelemente wie zum Beispiel die Zulässigkeit der Datenverarbeitung zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgaben (§ 5 BbgDSG) oder zur Zweckbindung (§ 6 BbgDSG) sowie die meisten der besondere Verarbeitungen betreffenden Regelungen erhalten. Anderes, insbesondere in Bezug auf den technischen und organisatorischen Datenschutz oder im Hinblick auf die Auftragsverarbeitung, ergibt sich aus der DSGVO unmittelbar. Daneben bringt die DSGVO Verfahrensänderungen mit sich, die in die Organisationsstrukturen und Verwaltungsabläufe öffentlicher Stellen einzupassen sind. Die DSGVO erfordert ein umfassendes Zusammenspiel von Organisationsverantwortlichen, IT-Beauftragten und Fachabteilungen, in dessen Rahmen der oder dem behördlichen Datenschutzbeauftragten (bDSB) eine beratende und überwachende Funktion zukommt.

Die vorliegenden Anwendungshinweise sollen einen Überblick über die wesentlichen Änderungen geben und die öffentlichen Stellen als Verantwortliche im Sinne der DSGVO bei der Anpassung der Prozesse und Verfahren an die Anforderungen der DSGVO unterstützen. Dabei sollen sie den Anpassungsaufwand

der Datenschutzpraxis unter Ausschöpfung der Interpretationsspielräume des neuen europäischen Datenschutzrechts begrenzen und dazu nach Möglichkeit, insbesondere soweit nicht technische oder gesetzliche Änderungen eintreten, auf einmalige Maßnahmen beschränken.

Die **Version 2 der Anwendungshinweise** enthält gegenüber der ersten Fassung vom 9. Mai 2018 im Wesentlichen inhaltliche Änderungen zu den Abschnitten 1, 4 bis 8, 10, 14 und 15 sowie den Anlagen 4b, 4c, 5, 7a und 7b, 8 und 9.

Des Weiteren wurden folgende Abschnitte und Anlagen neu hinzugefügt:
- Bereitstellung von Informationen auf der Internetseite (Ziffer 8.1.5),
- Verwendung von Cookies und ähnlichen technischen Komponenten (Ziffer 8.1.6),
- Bereitstellung von Informationen in E-Mail-Signaturen und Anschreiben (Ziffer 8.1.7),
- Gemeinsam Verantwortliche (Ziffer 9),
- Abgrenzung zu (gemeinsam) Verantwortlichen (Ziffer 10.3),
- Umgang mit Verletzungen des Schutzes personenbezogener Daten (Ziffer 12),
- Weitere Informationen und weiterführende Links (Ziffer 16),
- Anlage 5: Muster für die Freigabeerklärung gemäß § 4 Absatz 1 BbgDSG,
- Anlage 7c: Beispiele für Datenschutzerklärungen auf einer Internetseite,
- Anlage 10: Muster für eine Handreichung zum Datenschutz für Beschäftigte.

2 Einführung

2.1 Die Datenschutzreform der Europäischen Union

Seit dem 25. Mai 2018 ist die DSGVO in den brandenburgischen Behörden und sonstigen öffentlichen Stellen anzuwenden. Als europäische Verordnung ist die DSGVO unmittelbar geltendes Recht. Entgegenstehende Regelungen der Mitgliedstaaten sind seit diesem Zeitpunkt nicht mehr anzuwenden. Trotz ihrer unmittelbaren Geltung als EU-Verordnung lässt die DSGVO für die nationalen Gesetzgeber besonders im öffentlichen Bereich über sogenannte „Öffnungsklauseln“ bzw. Regelungsermächtigungen noch Spielräume für Konkretisierungen der DSGVO. Des Weiteren enthält die DSGVO konkrete Regelungsaufträge.

Unter diesen Prämissen ist das Datenschutzrecht im Bund und in den Ländern an die DSGVO anzupassen. Der Bund hat ein neues BDSG und weitere Änderungen datenschutzrechtlicher Vorschriften verabschiedet, zum Beispiel durch Einfügung von Datenschutzvorschriften in die Abgabenordnung und Neufassung der Datenschutzvorschriften im Ersten und Zehnten Buch Sozialgesetzbuch. Weitere Rechtsänderungen des bereichsspezifischen Datenschutzrechts des Bundes sind mit Beschluss des Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetzes EU im November 2019 verabschiedet worden. In Brandenburg sind die zuvor bereits angesprochenen Anpassungsgesetze am 25. Mai 2018 in Kraft getreten. Im bereichsspezifischen Recht werden weitere Rechtsänderungen auf Gesetz- und Verordnungsebene folgen.

2.2 Der Anwendungsbereich der DSGVO

Der sachliche Anwendungsbereich der DSGVO ist in Artikel 2 geregelt. Danach gilt die Verordnung 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 zugänglich ist. In der Kommentarliteratur werden dabei überwiegend zwei Zuordnungskriterien wie zum Beispiel Aktenzeichen, Jahreszahl oder Name als ausreichend erachtet. Dabei wird der Anwendungsbereich der DSGVO technikneutral sehr groß 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 Verordnung (siehe Erwägungsgrund 15 DSGVO).

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

- Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen (zum Beispiel Tätigkeit der Abgeordneten im Landtag, 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 Anwendungsbereich der Richtlinie zum Datenschutz bei Polizei und Justiz.

Unabhängig davon ist zu beachten, dass öffentliche Stellen in Brandenburg auch bei Verarbeitungen, die nicht in den sachlichen Anwendungsbereich der DSGVO im Sinne des Artikel 2 DSGVO fallen, gemäß § 2 Absatz 6 BbgDSG die Vorschriften der DSGVO anzuwenden haben, soweit in Spezialvorschriften nichts anderes geregelt ist (siehe auch Ziffer 2.4).

2.3 Der Anwendungsvorrang der DSGVO

Da - wie bereits dargelegt - die DSGVO unmittelbar, also ohne weiteren Umsetzungsakt gilt, ist sie innerhalb ihres Anwendungsbereiches das zentrale, maßgebliche Datenschutzrecht. Allerdings gibt es wie auch bisher weitere bundes- oder landesrechtliche Vorschriften über den Datenschutz. In Brandenburg ergänzt insbesondere das BbgDSG die DSGVO um allgemeine datenschutzrechtliche Regelungen. Andere spezielle datenschutzrechtliche Regelungen wie zum Beispiel die Vorschriften zur Verarbeitung personenbezogener Daten im Landesbeamtengesetz oder im Schulgesetz bleiben grundsätzlich erhalten, wurden aber soweit notwendig an die Vorgaben der DSGVO angepasst.

Für die künftige Rechtsanwendung bedeutet das unter anderem konkret:

- Das Verständnis datenschutzrechtlicher Begriffe ergibt sich ausschließlich aus den Definitionen der DSGVO (siehe Artikel 4 DSGVO und Erwägungsgründe 26 bis 37 DSGVO).
- Die Pflichten, die den öffentlichen Stellen als Verantwortliche für die Verarbeitung personenbezogener Daten obliegen (Näheres unter Ziffer 3), sind in der DSGVO verankert (siehe insbesondere Artikel 5, 24 ff. und 32 ff. DSGVO).

- Gleichzeitig sind auch die Rechte der betroffenen Personen unmittelbar in der DSGVO normiert. Ausnahmen von diesen Rechten enthält entweder die DSGVO selbst oder können in engen Grenzen durch nationale Gesetze, Rechtsverordnungen oder Satzungen zugelassen sein.
- Ausgangspunkt der Prüfung, ob eine Verarbeitung personenbezogener Daten rechtmäßig erfolgt, sind Artikel 6 Absatz 1 und Artikel 9 Absatz 2 DSGVO. Wie sich die Prüfungsreihenfolge im Zusammenspiel mit nationalen spezialgesetzlichen Regelungen gestaltet, wird unter Ziffer 4 dargestellt.
- Soweit die Verarbeitung auf einer Einwilligung der betroffenen Person beruht, ergeben sich die Bedingungen für die Einwilligung aus der DSGVO (siehe Artikel 7 und 8 DSGVO). Als Rechtsgrundlage für die Verarbeitung durch eine Behörde kommt die Einwilligung in aller Regel nicht in Betracht (siehe Erwägungsgründe 43 und 45 der DSGVO).
- Die DSGVO schreibt für öffentliche Stellen zwingend vor, dass eine oder ein bDSB zu benennen ist und welche Aufgaben diese oder dieser hat (siehe Artikel 37 ff. DSGVO).
- Aufgaben und Befugnisse der Aufsichtsbehörde ergeben sich unmittelbar aus der DSGVO (siehe Artikel 57 und 58 DSGVO).

Die DSGVO beinhaltet neben ihren 99 Artikeln auch insgesamt 173 Erwägungsgründe, die den Artikeln voranstehen. 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**.

2.4 Das neue Brandenburgische Datenschutzgesetz

Das neue BbgDSG dient der Anpassung des allgemeinen Datenschutzrechts an die DSGVO und enthält in erster Linie ergänzende Regelungen. Des Weiteren trifft es auch für Bereiche, die nicht dem sachlichen Anwendungsbereich der DSGVO unterfallen, die erforderlichen datenschutzrechtlichen Regelungen: Soweit nicht im jeweiligen Fachrecht abweichende Regelungen getroffen werden, unterfallen auch solche Datenverarbeitungen der DSGVO (§ 2 Absatz 6 BbgDSG). Dies betrifft beispielsweise die Datenverarbeitung in unstrukturierten Akten der DSGVO. Ausgenommen sind jedoch die Artikel 30, 35 und 36 DSGVO, die nur gelten, soweit die Verarbeitung automatisiert erfolgt oder die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Durch die entsprechende Anwendbarkeit der DSGVO für diese Bereiche wird sichergestellt, dass jegliche Verarbeitungen personenbezogener Daten einem vom Grundsatz her einheitlichen Regelungsrahmen unterfallen, der neben dem Recht auf den Schutz personenbezogener Daten gemäß Artikel 8 der EU-Grundrechte-Charta auch das vom Bundesverfassungsgericht entwickelte Recht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG gewährleistet.

Inhaltlich enthält das BbgDSG folgende Regelungsschwerpunkte:
- Beibehaltung des Freigabeverfahrens für automatisierte Datenverarbeitungen (§ 4 BbgDSG),
- Beibehaltung einer Auffangnorm, die die Verarbeitung personenbezogener Daten zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgaben erlaubt (§ 5 BbgDSG),
- Definition der Voraussetzungen, unter denen personenbezogene Daten zu anderen als den ursprünglichen Erhebungszwecken verarbeitet werden dürfen (§ 6 BbgDSG),

- Definition der Voraussetzungen für die Beschränkung von den Rechten der betroffenen Personen auf Auskunft und Löschung sowie den Pflichten der verantwortlichen Stelle zur Information der betroffenen Person (§§ 10 bis 13 BbgDSG),
- Umsetzung der Anforderungen der DSGVO an die Tätigkeit und Unabhängigkeit der Aufsichtsbehörden (Abschnitt 4 des BbgDSG),
- Beibehaltung von Regelungen zu besonderen Verarbeitungssituationen (Abschnitt 5 des BbgDSG).

Als →**Anlage 2** ist eine Übersicht beigefügt, die die bisherigen Regelungen des BbgDSG-alt den neuen Rechtsvorschriften gegenüberstellt

2.5 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 (siehe Ziffer 2.6) 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 BbgDSG. Die DSGVO enthält teilweise neue bzw. gegenüber dem bisherigen Stand modifizierende verfahrensrechtliche Vorgaben und Dokumentationspflichten. Der oder dem (behördlichen) Datenschutzbeauftragten werden konkrete Aufgaben zugewiesen und ihre oder seine Rolle als Beraterin oder Berater des Verantwortlichen klargestellt. Hinsichtlich des technischen Datenschutzes 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. Des Weiteren werden der Aufsichtsbehörde neue Befugnisse übertragen, die bis hin zur Untersagung von Verarbeitungen reichen können.

2.6 Begriffsbestimmungen

Die Begriffsbestimmungen ergeben sich zukünftig unmittelbar aus Artikel 4 DSGVO. Lediglich in Bezug auf das Anonymisieren enthält § 3 BbgDSG eine ergänzende Begriffsbestimmung. Gegenüber den bisher im BbgDSG verwendeten Begriffen ergeben sich unter anderem aus Artikel 4 DSGVO folgende Änderungen:

- „Betroffener“ = „betroffene Person“,
- „Sperrung“ = „Einschränkung der Verarbeitung“,
- „verantwortliche Stelle“ = „Verantwortlicher“,
- „besondere Arten personenbezogener Daten“ = „besondere Kategorien personenbezogener Daten“,
- „Auftragsdatenverarbeiter“ = „Auftragsverarbeiter“,
- „Datei“ = „Dateisystem“.

3 Rolle des Verantwortlichen nach der DSGVO

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“. Im öffentlichen Bereich ist Verantwortlicher die jeweilige Daten verarbeitende öffentliche Stelle im Sinne von § 2 Absatz 1 BbgDSG, also wie bisher zum Beispiel die Gemeinde, der Landkreis oder das Ministerium.

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 §§ 5 und 6 BbgDSG und in fachgesetzlichen Datenschutzvorschriften geregelt.
- die Verfahrensvorschriften der DSGVO beachtet werden. Dies gilt zum Beispiel für die Führung des Verzeichnisses von Verarbeitungstätigkeiten nach Artikel 30 DSGVO, die Melde- und Benachrichtigungspflichten nach Artikel 33 und 34 DSGVO und die Durchführung von Datenschutz-Folgenabschätzungen nach Artikel 35 DSGVO.
- die datenschutzrechtlichen Informationspflichten nach Artikel 13 und 14 DSGVO in Verbindung mit § 6 Absatz 2 und § 10 BbgDSG und die sonstigen Rechte der Betroffenen beachtet werden (zum Beispiel das Auskunftsrecht nach Artikel 15 DSGVO in Verbindung mit § 11 BbgDSG, 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 Absatz 1, 25 und 32 DSGVO).
- geeignete sonstige Datenschutzvorkehrungen getroffen werden (zum Beispiel Datenschutzrichtlinien oder sonstige Datenschutzanweisungen nach Artikel 24 Absatz 2 DSGVO).

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 dabei 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. Die Letztverantwortlichkeit verbleibt bei der Behördenleitung bzw. der Leitung der öffentlichen Stelle.

➔ **Handlungserfordernis:**
Zuständigkeiten sind festzulegen und erforderliche Maßnahmen umzusetzen (siehe Ziffern 14 und 15).

4 Zulässigkeit der Verarbeitung personenbezogener Daten

Wie bisher gilt hinsichtlich der Zulässigkeit der Verarbeitung personenbezogener Daten das Prinzip des Verbots mit Erlaubnisvorbehalt. Zentrale Vorschrift ist Artikel 6 DSGVO. Die einzelnen in Artikel 6 Absatz 1 DSGVO definierten Erlaubnistatbestände sind:

- die Einwilligung, Artikel 6 Absatz 1 Buchstabe a DSGVO (siehe auch Artikel 7 und 8 DSGVO),
- die Erforderlichkeit zur Erfüllung von Verträgen oder vorvertraglicher Verpflichtungen, Artikel 6 Absatz 1 Buchstabe b DSGVO,

- die Erforderlichkeit zur Erfüllung einer rechtlichen Verpflichtung, Artikel 6 Absatz 1 Buchstabe c DSGVO (in Verbindung mit Artikel 6 Absatz 2 und 3 DSGVO, der eine EU-Norm oder nationale Rechtsvorschrift fordert),
- die Erforderlichkeit zum Schutz lebenswichtiger Interessen, Artikel 6 Absatz 1 Buchstabe d DSGVO,
- die Erforderlichkeit zur Wahrnehmung öffentlicher Aufgaben oder in Ausübung hoheitlicher Gewalt, Artikel 6 Absatz 1 Buchstabe e DSGVO (in Verbindung mit Artikel 6 Absatz 2 und 3 DSGVO, der eine EU-Norm oder nationale Rechtsvorschrift fordert),
- die Erforderlichkeit zur Wahrung berechtigter Interessen des Verantwortlichen, Artikel 6 Absatz 1 Buchstabe f DSGVO (Buchstabe f gilt nicht für die von öffentlichen Stellen in Erfüllung ihrer durch Rechtsvorschriften zugewiesenen Aufgaben vorgenommene Verarbeitung).

Dabei gelten die Erlaubnistatbestände von Artikel 6 Absatz 1 Buchstabe a, b, d und f DSGVO unmittelbar. Eine Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung (Buchstabe c) oder zur Wahrnehmung einer öffentlichen Aufgabe (Buchstabe e) kann nicht auf die die DSGVO unmittelbar gestützt werden, sondern es bedarf einer Rechtsvorschrift der EU oder des Mitgliedstaates. Solche Rechtsvorschriften sind insbesondere das bereichsspezifische nationale Recht und – als Auffangnorm – das BbgDSG. Neben den per Gesetz oder Verordnung erlassenen Rechtsvorschriften kann die Verarbeitung personenbezogener Daten auch durch untergesetzliche Vorschriften (Satzungen, Dienstvereinbarungen, Verwaltungsvorschriften, Geschäftsordnungen) geregelt sein. Im Rahmen des Anpassungsprozesses ist es erforderlich, auch diese Vorschriften daraufhin zu überprüfen, ob sie im Einklang mit der DSGVO stehen, und sind gegebenenfalls anzupassen. Entsprechende Hinweise finden sich in →**Anlage 3**. Soweit bereichsspezifische Regelungen keine konkrete Befugnis enthalten, die für die Wahrnehmung einer öffentlichen Aufsicht erforderlichen personenbezogenen Daten zu verarbeiten, können öffentliche Stellen die Datenverarbeitung auf § 5 Absatz 2 Satz 1 und 2 BbgDSG (unter dessen Voraussetzungen) stützen.

Erteilte Einwilligungen wirken nach Erwägungsgrund 171 DSGVO fort. Sofern sie die Grundlage für eine Verarbeitung personenbezogener Daten nach Artikel 6 Absatz 1 Buchstabe a DSGVO sein sollen, gilt dies jedoch nur, sofern sie auch der Art nach und inhaltlich den in Artikel 4 Nummer 11, Artikel 7 und Artikel 8 DSGVO geregelten Bedingungen entsprechen. Demnach ist eine Einwilligung nur wirksam, wenn sie freiwillig und bezogen auf die bestimmte Verarbeitung informiert abgegeben wird. Freiwillig ist eine Einwilligung nur, wenn die betroffene Person eine echte und freie Wahl hat, also die Einwilligung auch verweigern oder zurückziehen kann, ohne dass ihr dabei Nachteile entstehen (siehe Erwägungsgrund 42 DSGVO). In der Regel besteht jedoch ein klares Ungleichgewicht zwischen öffentlichen Stellen als Verantwortlichen und der betroffenen Person, sodass hier nach Erwägungsgrund 43 DSGVO eine Einwilligung als Rechtsgrundlage oft ausscheidet. Im Ausnahmefall (zum Beispiel bei Presseverteilern und Newslettern oder im Zusammenhang mit § 26 BbgDSG) kann eine Einwilligung aber als Rechtsgrundlage dienen, sofern die Verarbeitung grundsätzlich im Zusammenhang mit den Aufgaben der öffentlichen Stelle steht und einer Verweigerung der Einwilligung keine nachteiligen Auswirkungen für die betroffenen Personen hat. Sofern diese Voraussetzungen nicht erfüllt sind, kann sich die öffentliche Stelle nicht auf eine Einwilligung im Sinne des Artikel 6 Absatz 1 Buchstabe a DSGVO stützen.

Artikel 6 Absatz 4 DSGVO enthält Vorschriften über zulässige Zweckänderungen, die durch § 6 BbgDSG umgesetzt bzw. ergänzt werden. Gemäß § 6 Absatz 1 BbgDSG ist eine Verarbeitung personenbezogener

Daten zu einem anderen Zweck, als zu demjenigen, zu dem die Daten erhoben wurden, im Rahmen der Aufgabenerfüllung des Verantwortlichen zulässig, unter anderem wenn

- es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist (§ 6 Absatz 1 Nummer 1 BbgDSG),
- es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist (§ 6 Absatz 1 Nummer 2 BbgDSG),
- sich bei der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten erscheint (§ 6 Absatz 1 Nummer 3 BbgDSG),
- es erforderlich ist, Angaben der betroffenen Person zu überprüfen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen (§ 6 Absatz 1 Nummer 4 BbgDSG).

Da Zweckänderungen eine erneute Informationspflicht auslösen (siehe Ziffer 8.1.3), sollten alle Zwecke einer Verarbeitung, einschließlich bestimmbarer zukünftiger Zwecke, von Beginn an festgelegt sein.

Hinsichtlich der Verarbeitung besonderer Datenkategorien enthält Artikel 9 DSGVO spezifische Anforderungen. Zu den in Artikel 9 Absatz 1 DSGVO genannten Daten gehören solche über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Auch bei diesen sogenannten „sensiblen Daten“ gilt hinsichtlich der Zulässigkeit der Verarbeitung das Prinzip des Verbots mit Erlaubnisvorbehalt. Artikel 9 Absatz 2 DSGVO regelt hierbei die Erlaubnistatbestände.

Mit Blick darauf, dass öffentliche Stellen in der Regel zum Zweck der Erfüllung der ihnen gesetzlich oder aufgrund Gesetz 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 BbgDSG (§§ 5, 6 oder 25 bis 31 BbgDSG) eine Erlaubnisnorm zur Verfügung?
3. Kann die Datenverarbeitung auf Artikel 6 Absatz 1 Buchstabe 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 in der Regel nicht auf Artikel 6 Absatz 1 Buchstabe f DSGVO stützen können.

In jedem Fall ist zu beachten, dass sowohl das allgemeine als auch das fachspezifische 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- oder im Bundesrecht) im Zusammenhang zu lesen und anzuwenden sein.

Handlungserfordernisse:

- Es ist zu prüfen, ob das neue Recht für alle Prozesse eine Rechtsgrundlage bereitstellt.

- Vorhandene Einwilligungen sind zu prüfen, um sicherzustellen, dass sie mit der DSGVO vereinbar sind.
- Dienstvereinbarungen, Satzungsrecht, Verwaltungsvorschriften und Geschäftsordnungen sind im Hinblick auf die Vereinbarkeit mit der DSGVO zu überprüfen.

5 Verfahrensänderungen

Schwerpunkt der anstehenden Anpassungsaufgaben an die DSGVO und das neue BbgDSG sind die umfangreichen Verfahrensänderungen im Datenschutz hinsichtlich des Verzeichnisses von Verarbeitungstätigkeiten, der Freigabe automatisierter Verfahren und der Datenschutz-Folgenabschätzung.

5.1 Verzeichnis von Verarbeitungstätigkeiten

Das Verfahrensverzeichnis nach § 8 BbgDSG-alt wurde durch das Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 DSGVO abgelöst. Anders als nach altem Recht ist ein Verzeichnis von Verarbeitungstätigkeiten unabhängig davon zu führen, ob Verarbeitungen automatisiert erfolgen oder nicht. Das heißt, auch soweit personenbezogene Daten in (strukturierten) Papierakten verarbeitet werden (siehe Ziffer 2.2), ist ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Darüber hinaus gelten die in § 8 Absatz 5 BbgDSG-alt geregelten Ausnahmen für das Verfahrensverzeichnis nicht mehr.

Das Verzeichnis von Verarbeitungstätigkeiten ist als ein Verzeichnis aller Verarbeitungstätigkeiten zu verstehen. Es enthält Beschreibungen zu allen Verarbeitungstätigkeiten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) hat zur Erstellung des Verzeichnisses Arbeitshilfen entwickelt, die als →**Anlage 4a** beigefügt sind. Des Weiteren finden sich in den →**Anlagen 4b und 4c** Muster für das Verzeichnis von Verarbeitungstätigkeiten von Verantwortlichen und von Auftragsverarbeitern.

Das Verzeichnis ist vom Verantwortlichen zu führen. Die Führung des Verzeichnisses hat zentral an einer Stelle zu erfolgen. Es ist empfehlenswert, dass die oder der bDSB zumindest eine Kopie des Verzeichnisses vorhält, um ihre oder seine Aufgaben wahrnehmen zu können. Für jede Verarbeitungstätigkeit ist eine Beschreibung (als ein Eintrag im Verzeichnis) nach Maßgabe des Artikel 30 DSGVO zu erstellen. Als Verarbeitungstätigkeit in diesem Sinne wird im Allgemeinen ein Prozess auf geeignetem Abstraktionsniveau verstanden. So können Verarbeitungen, die den gleichen Zwecken dienen, die gleiche oder ähnliche Datenarten umfassen und auf der gleichen Rechtsgrundlage beruhen, in der Regel in einer Beschreibung bzw. einem Eintrag zusammengefasst werden.

Beispiele:
Geburtstagslisten und An-/Abwesenheitslisten: Werden Listen mit personenbezogenen Daten privat geführt, so ist eine Beschreibung für das Verzeichnis von Verarbeitungstätigkeiten nicht erforderlich. In der Regel ist dies bei Geburtstagslisten der Fall. Werden Listen aus dienstlichen Gründen geführt, ist eine Beschreibung für das Verzeichnis von Verarbeitungstätigkeiten erforderlich, was regelmäßig bei An- und Abwesenheitslisten der Fall sein wird.

Verarbeitungen zu Zwecken des „Arbeitsschutzes“: Eine zusammengefasste Beschreibung verschiedener Verarbeitungen mit dem übergeordneten Zweck „Arbeitsschutz“ ist zwar möglich. Einzelne Angaben

(zum Beispiel konkrete Löschfristen gemäß Artikel 30 Absatz 1 Buchstabe f DSGVO) sollten jedoch zu den jeweiligen Verarbeitungen beispielsweise durch fortlaufende Nummerierungen zuordenbar sein (siehe Muster in →**Anlage 4b**). Dies ist gegebenenfalls aber unübersichtlich und nicht praktikabel. In solchen Fällen empfiehlt sich statt einer zusammengefassten Beschreibung von verschiedenen Verarbeitungen mit einem übergeordneten Zweck die Erstellung mehrerer Beschreibungen bzw. Eintragungen für das Verzeichnis von Verarbeitungstätigkeiten.

Nutzung von Bürokommunikationssoftware wie Outlook: Es ist ein eigenständiger Eintrag zu Outlook im Verzeichnis von Verarbeitungstätigkeiten erforderlich. Zusätzlich dazu wird empfohlen, soweit Outlook im Rahmen einer bestimmten Verarbeitungstätigkeit verwendet wird, Outlook in der Beschreibung dieser Verarbeitungstätigkeit in der Zeile „Name des eingesetzten Verfahrens“ (siehe Muster in →**Anlage 4b**) einzutragen.

Entsprechend des Musters in →**Anlage 4b** wird empfohlen, innerhalb der jeweiligen Beschreibungen laufende Nummern hinsichtlich der Kategorien betroffener Personen zu vergeben, um so eine Zuordnung zu den weiteren Angaben, wie zum Beispiel konkreten Löschfristen, zu ermöglichen. Auch sind tabellarische Darstellungen für eine bessere Übersichtlichkeit und Zuordenbarkeit denkbar.

Beispiel für eine tabellarische Darstellung:
In einem Verfahren X werden personenbezogene Daten von Antragsstellenden verarbeitet. Die Verarbeitung erfolgt mittels Software Y. Der Zugriff durch Mitarbeitende der öffentlichen Stelle auf Software Y und auf die darin gespeicherten personenbezogenen Daten der Antragsstellenden wird protokolliert. Entsprechend könnte in der Beschreibung der Verarbeitungstätigkeit folgende laufende Nummerierung gewählt werden:

<table>
<tr><th>Ldf. Nr.</th><th>Kategorien von personenbezogenen Daten</th><th>Kategorien betroffener Personen</th><th>Löschfristen</th></tr>
<tr><td>1</td><td>Kontaktdaten</td><td rowspan="4">Antragsstellende</td><td rowspan="4">gemäß § … [Rechtsgrundlage] für 5 Jahre nach Abschluss des Verfahrens, Vorschriften des BbgArchivG bleiben unberührt</td></tr>
<tr><td>2</td><td>Geburtsdaten</td></tr>
<tr><td>3</td><td>Staatsangehörigkeit</td></tr>
<tr><td>4</td><td>Religionszugehörigkeit
(Datum nach Artikel 9 DSGVO)</td></tr>
<tr><td>4</td><td>Benutzerkennungen</td><td rowspan="2">Sachbearbeitende</td><td>1 Jahr nach Beendigung des Arbeitsverhältnisses</td></tr>
<tr><td>5</td><td>Zugriffs- und Protokolldaten</td><td>2 Jahre nach dem Zugriff auf die Daten</td></tr>
</table>

Der Verantwortliche hat im Rahmen seiner Organisationshoheit zu bestimmen, wer die jeweiligen Beschreibungen der Verarbeitungstätigkeiten für das Verzeichnis erstellt und wer für die Überarbeitung bzw.

Aktualisierung zuständig ist. Die Erstellung sollte zweckmäßiger Weise durch den für die jeweilige Fachaufgabe verantwortlichen Bereich, gegebenenfalls unter Beteiligung der IT-Stelle, erfolgen. Die oder der bDSB berät bei der Erstellung des Verzeichnisses.

Handlungserfordernisse:

- Noch nach altem Recht bestehenden Verfahrensverzeichnisse sind an Artikel 30 DSGVO anzupassen.
- Es ist zu prüfen, ob für alle Verarbeitungstätigkeiten eine Beschreibung für das Verarbeitungsverzeichnis vorliegt.

5.2 Freigabe

Die datenschutzrechtliche Freigabe automatisierter Verfahren durch den Verantwortlichen wurde beibehalten und ist in § 4 Absatz 1 BbgDSG geregelt. Danach ist in den Fällen, in denen die Verarbeitung personenbezogener Daten mittels automatisierter Verfahren erfolgen soll, vor Beginn dieser Verarbeitung oder vor einer wesentlichen Änderung ein Freigabeverfahren durchzuführen. Wesentlich ist eine Verfahrensänderung insbesondere dann, wenn Änderungen in Bezug auf die Zweckbestimmungen, die betroffenen Personengruppen und die zu verarbeitenden Daten, die Datenempfänger, die technischen und organisatorischen Maßnahmen sowie die eingesetzten Datenverarbeitungsanlagen oder Datenverarbeitungsprogramme erfolgen sollen.

Zu beachten ist, dass § 4 Absatz 2 BbgDSG bestimmte Verfahren von der Freigabepflicht ausnimmt. Das trifft beispielsweise auf den Einsatz von handelsüblichen Schreibprogrammen wie Microsoft Word oder auch auf Anschriftenverzeichnisse, die ausschließlich für die Versendung von Informationen an betroffene Personen genutzt werden, zu. Gleichwohl ist auch für diese Verfahren, anders als nach altem Recht, eine Beschreibung bzw. ein Eintrag für das Verzeichnis von Verarbeitungstätigkeiten gemäß Artikel 30 DSGVO zu erstellen.

Freigaben, die vor dem 25. Mai 2018 erteilt wurden, bleiben wirksam. Es empfiehlt sich, im Rahmen des Freigabeverfahrens der oder dem bDSB Gelegenheit zur Stellungnahme zu geben. Ein Mustertext für eine Freigabeerklärung gemäß § 4 Absatz 1 BbgDSG findet sich in →**Anlage 5**.

Handlungserfordernis:

Die Inhalte des an die DSGVO angepassten Freigabeverfahrens und der Freigabeerklärung sind zu berücksichtigen.

5.3 Datenschutz-Folgenabschätzung

Vor dem Einsatz „hochrisikoträchtiger“ und eingriffsintensiver Verarbeitungen ist eine Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO durchzuführen. Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg (LDA) hat hierzu auf ihrer Internetseite zwei Listen mit Verarbeitungsvorgängen veröffentlicht, für die ein solches Verfahren durchzuführen ist: https://www.lda.brandenburg.de/lda/de/datenschutz/auslegungshilfen-der-landesbeauftragten/.

Für Datenverarbeitungen, die vor dem 25. Mai 2018 bereits durchgeführt wurden und die in die Kategorie „hochrisikoträchtiger" Verarbeitungen im Sinne des Artikel 35 DSGVO einzustufen wären, ist keine Datenschutz-Folgenabschätzung erforderlich, wenn eine Vorabkontrolle nach altem Recht durch die oder den bDSB erfolgt ist und soweit die Verarbeitung ohne wesentliche Änderung fortgesetzt wird. 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 2-3 Jahren nach der Geltung der DSGVO, also spätestens bis zum 25. Mai 2021, durchgeführt werden sollte. Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie (Artikel-29-Gruppe) hatte bereits vor Geltung der DSGVO Leitlinien zur Datenschutz-Folgenabschätzung entwickelt (WP 248 Rev. 01, siehe →**Anlage 6**), die nähere Ausführungen zu diesem Verfahren enthalten. Diese Leitlinien wurden vom Europäischen Datenschutzausschuss (EDSA), der die Artikel-29-Gruppe mit Geltung der DSGVO ablöste, in dessen konstituierender Sitzung bestätigt.

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

Bei Verarbeitungen im öffentlichen Bereich, die auf einer Rechtsgrundlage im Unionsrecht oder im Recht der Mitgliedsstaaten gemäß Artikel 6 Absatz 1 Buchstabe c oder e DSGVO beruhen, ist die Durchführung einer Datenschutz-Folgenabschätzung gemäß Artikel 35 Absatz 10 DSGVO nicht erforderlich, sofern diese Rechtsvorschriften den konkreten Verarbeitungsvorgang regeln und bereits im Rahmen einer allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass der Rechtsvorschrift eine Datenschutz-Folgenabschätzung erfolgte. Eine Datenschutz-Folgenabschätzung wäre in diesen Fällen nur dann durchzuführen, wenn dies nach dem Ermessen des Gesetzgebers für erforderlich gehalten wird. Ob insbesondere nationale bereichsspezifische Rechtsvorschriften als Rechtsgrundlagen im Sinne von Artikel 35 Absatz 10 DSGVO angesehen werden können, richtet sich vor allem danach, ob der konkrete Verarbeitungsvorgang unter Beachtung der in Artikel 35 Absatz 7 DSGVO genannten Aspekte geregelt ist bzw. diese im Rahmen der Rechtsetzung berücksichtigt wurden. Insbesondere müssen folgende Aspekte betrachtet worden sein:

- systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen (Artikel 35 Absatz 7 Buchstabe a DSGVO),
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck (Artikel 35 Absatz 7 Buchstabe b DSGVO),
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Artikel 35 Absatz 1 DSGVO (Artikel 35 Absatz 7 Buchstabe c DSGVO) und
- zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die DSGVO eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird (Artikel 35 Absatz 7 Buchstabe d DSGVO).

Sofern nur einzelne der vorgenannten Aspekte betrachtet wurden, ist eine Datenschutz-Folgenabschätzung für die fehlenden Sachverhalte durchzuführen.

➔ **Handlungserfordernisse:**

- Die Vorabkontrolle durch die oder den bDSB gemäß § 10a BbgDSG-alt wird durch die Datenschutz-Folgenabschätzung, die der Verantwortliche durchzuführen hat, 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 die oder den bDSB unterlegen haben und ohne wesentliche Änderung fortgeführt werden. Bei der Überprüfung dieser Verarbeitungen bis spätestens Mai 2021 sind die Anforderungen von Artikel 35 DSGVO zugrunde zu legen.

6 Die oder der behördliche Datenschutzbeauftragte

Mit Anwendbarkeit der DSGVO am 25. Mai 2018 wurden auch die Stellung und die Aufgaben der Datenschutzbeauftragten neu geregelt (Artikel 37 bis 39 DSGVO). Nach Artikel 37 Absatz 1 Buchstabe a DSGVO hat jede öffentliche Stelle eine oder einen bDSB zu benennen. Hiervon ausgenommen sind Gerichte und unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit.

Die bDSB können mit ihrem Einverständnis auch für mehrere Behörden bestellt werden, wenn dadurch die Erfüllung der Aufgaben der bDSB nicht beeinträchtigt wird. Dabei sind nicht nur die verfügbaren Ressourcen und die Erreichbarkeit der bDSB insbesondere für Beschäftigte zu beachten, sondern gemäß Artikel 37 Absatz 3 DSGVO auch die Organisationsstrukturen und die Größe der jeweiligen Behörden zu berücksichtigen.

Die bDSB sind 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 Informations- und Kommunikationstechnik. Den bDSB sind die zur Erfüllung der Aufgaben zudem die erforderlichen Ressourcen zur Verfügung zu stellen (Artikel 38 Absatz 2 DSGVO). Dazu gehören abhängig von der Art der Verarbeitungstätigkeiten und der Größe der öffentlichen Stelle unter anderem:

- die Gewährung von genügend Zeit für die Erfüllung der Pflichten der oder des bDSB,
- eine angemessene Unterstützung durch Räumlichkeiten, Ausrüstung (zum Beispiel Fachliteratur und Nachschlagewerke sowie Zugang zu aktueller Rechtsprechung) und gegebenenfalls zusätzlichem Personal sowie
- die kontinuierliche Teilnahme an Schulungs- und Fortbildungsveranstaltungen einschließlich Übernahme der dafür anfallenden Kosten.

Zwar gehören die bDSB zur jeweiligen öffentlichen Stelle, die Funktion bDSB hat jedoch eine herausgehobene Stellung. Sie berichten der jeweiligen Leitung der öffentlichen Stelle unmittelbar. In der Ausübung ihrer Aufgaben sind die bDSB weisungsfrei: Gemäß Artikel 38 Absatz 4 DSGVO stellen die Verantwortlichen sicher, dass Datenschutzbeauftragte bei der Erfüllung der Aufgaben keine Anweisungen bezüglich der Ausübung erhalten. Dies betrifft jedoch nicht die Einhaltung der allgemeinen Dienstpflichten oder sich aus dem Arbeitsvertrag ergebenden Pflichten.

Darüber hinaus lässt es die DSGVO zu, dass die bDSB neben der Tätigkeit als bDSB auch andere Aufgaben wahrnehmen können. Soll die Funktion des bDSB Beschäftigten übertragen werden, die auch mit anderweitigen (Haupt-)Aufgaben betraut sind, muss sichergestellt werden, dass derartige Aufgaben nicht zu einem Interessenskonflikt führen (Artikel 39 Absatz 6 DSGVO). Der Verantwortliche sollte daher kritisch überprüfen, ob es zu einer Inkompatibilität kommen könnte und sicherstellen, dass die bDSB (und gegebenenfalls die Stellvertretung) in der Aufgabenwahrnehmung nicht eingeschränkt zur Verfügung stehen. Die bDSB dürfen sich aufgrund anderer Funktionen nicht selbst überwachen müssen. Grundsätzlich sollte daher niemand als bDSB bestellt werden, der Aufgaben übertragen bekommen hat, die nach der DSGVO dem Verantwortlichen obliegen. Zur Vermeidung von Interessenskonflikten können interne Richtlinien aufgestellt werden.

Beispiele für mögliche Interessenskonflikte:
In der Regel scheiden Personen, die mit der Leitung der IT-Abteilung oder der Leitung der Personalabteilung betraut sind, als bDSB aus. Bei einfachen Personalratsmitgliedern wird in der Regel keine Unvereinbarkeit im Sinne von Artikel 38 Absatz 6 Satz 2 DSGVO vorliegen, da sie in dem Gremium keine alleinigen Entscheidungen treffen. Bei Personalratsvorsitzenden können jedoch Interessenkonflikte auftreten, eine Benennung als bDSB ist daher nicht empfehlenswert.

Die bDSB sind frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden (Artikel 38 Absatz 1 DSGVO). Sie müssen Zugang zum Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 DSGVO haben, sofern ihnen nicht sowieso eine Kopie vorliegt oder die Aufgabe übertragen wurde, das Verzeichnis zentral vorzuhalten bzw. aufzubewahren.

Wesentliche Aufgaben der bDSB gemäß Artikel 39 Absatz 1 DSGVO sind insbesondere
- die Unterrichtung und Beratung des Verantwortlichen über dessen datenschutzrechtliche Pflichten,
- die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften,
- die Überwachung der Durchführung von Sensibilisierungs- und Schulungsmaßnahmen der Beschäftigten durch den Verantwortlichen,
- die Zusammenarbeit mit der Aufsichtsbehörde und
- die Beratung des Verantwortlichen bei Datenschutz-Folgenabschätzungen.

Die Führung des Verzeichnisses von Verarbeitungstätigkeiten und die Durchführung der Datenschutz-Folgenabschätzung sind nach der DSGVO keine Pflichtaufgaben der bDSB – anders als früher die Führung des Verfahrensverzeichnisses und die Durchführung der Vorabkontrolle. Der Verantwortliche kann den bDSB im Einklang mit der DSGVO weitere Aufgaben übertragen. Dies betrifft zum Beispiel die Übertragung der Aufgabe, das Verzeichnis von Verarbeitungstätigkeiten zu führen. In diesem Zusammenhang bedeutet die Führung die reine Verwaltung des Verzeichnisses und nicht die Erstellung der Beschreibungen bzw. Einträge für das Verzeichnis. Hierfür sowie für die Richtigkeit, Vollständigkeit und Aktualität des Verzeichnisses von Verarbeitungstätigkeiten ist der Verantwortliche (bzw. der jeweilige Fachbereich) zuständig. Auch kann vorgegeben werden, dass vor jedem beabsichtigten Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens mit dem personenbezogene Daten verarbeitet werden, die Stellungnahme der bDSB einzuholen ist. Aus Artikel 35 Absatz 1 Satz 1 und Absatz 2 DSGVO ergibt sich aber, dass die Durchführung der Datenschutz-Folgenabschätzung nicht auf die bDSB übertragen werden kann.

Handlungserfordernisse:

- Bereits bestellte bDSB bleiben in ihrer Funktion, gegebenenfalls ist aber eine Überprüfung der Qualifikation und Unabhängigkeit (zur Vermeidung von Interessenskonflikten) erforderlich. Zudem sind neue Aufgaben und Verantwortlichkeiten zu beachten.
- Sollen weitere Aufgaben übertragen werden, ist dies durch den Verantwortlichen zu regeln.
- Es ist zu prüfen, ob angesichts der geänderten bzw. erweiterten Aufgaben die Ressourcen der bDSB ausreichend sind.
- Die Kontaktdaten der bDSB sind gemäß Artikel 37 Absatz 7 DSGVO zu veröffentlichen.
- Die bDSB sind gemäß Artikel 37 Absatz 7 DSGVO an die LDA zu melden. Dies ist über das folgende Formular möglich: https://www.lda.brandenburg.de/lda/de/service/formulare-und-musterschreiben/meldung-des-datenschutzbeauftragten/.

7 Aufgaben und Befugnisse der Aufsichtsbehörde

Die Aufgaben und Befugnisse der LDA als datenschutzrechtliche Aufsichtsbehörde in Brandenburg ergeben sich aus den Artikeln 57 bis 59 DSGVO sowie § 18 BbgDSG. Insbesondere obliegt ihr im Land Brandenburg die Überwachung der Einhaltung und Durchsetzung der Anforderungen der DSGVO, des BbgDSG und anderer datenschutzrechtlicher Vorschriften. Zudem berät sie öffentliche und private Stellen im Umgang mit personenbezogenen Daten.

Die DSGVO stärkt die Befugnisse der LDA. Sie hat gemäß Artikel 58 Absatz 1 DSGVO umfassende Untersuchungsbefugnisse. Öffentliche Stellen sind gemäß § 21 BbgDSG verpflichtet, die LDA und ihre Mitarbeitenden bei der Erfüllung ihrer Aufgaben zu unterstützen. Die öffentlichen Stellen müssen insbesondere:

- Auskünfte erteilen,
- Einsicht in alle Vorgänge und Aufzeichnungen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, und
- jederzeit Zutritt zu allen Diensträumen, einschließlich aller Datenverarbeitungsanlagen und Geräte gewähren.

Neben diesen Untersuchungsbefugnissen verfügt die LDA gemäß Artikel 58 Absatz 3 DSGVO über Genehmigungs- und Beratungsbefugnisse sowie gemäß Artikel 58 Absatz 2 DSGVO auch gegenüber öffentlichen Stellen über Abhilfebefugnisse. Mit diesen Abhilfebefugnissen kann sie unter anderem:

- warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die DSGVO verstoßen,
- verwarnen, wenn gegen die DSGVO verstoßen wird,
- anweisen, den Anträgen von betroffenen Person auf Ausübung ihrer Rechte zu entsprechen,
- anweisen, Verarbeitungsvorgänge in Einklang mit der DSGVO zu bringen,
- eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, verhängen,
- die Berichtigung oder Löschung von personenbezogenen Daten anordnen oder
- die Übermittlung von Daten in Drittländer aussetzen.

Geldbußen kann die LDA gegen öffentliche Stellen im Sinne des § 2 Absatz 1 und 2 BbgDSG hingegen nicht verhängen (§ 32 Absatz 3 BbgDSG). Sofern jedoch Beschäftigte öffentlicher Stellen Verstöße im Sinne von § 32 Absatz 1 BbgDSG begehen, kann die LDA gegen diese ein Ordnungswidrigkeitenverfahren einleiten.

Anstelle des Beanstandungsverfahrens nach altem Recht vor Geltung der DSGVO teilt die LDA der zuständigen Fach- oder Rechtsaufsicht mit, wenn sie von ihren Befugnissen nach Artikel 58 Absatz 2 DSGVO Gebrauch gemacht hat (§ 22 Satz 1 BbgDSG). Der Verantwortliche ist verpflichtet, gegenüber der Aufsicht innerhalb eines Monats eine Stellungnahme abzugeben, in der auch darzustellen ist, in welcher Weise auf die Maßnahme der LDA reagiert wird (§ 22 Satz 2 BbgDSG).

Vor dem Erlass von Rechts- und Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten betreffen, ist die LDA gemäß § 18 Absatz 5 Satz 1 BbgDSG zu hören. Zudem ist sie über Planungen des Landes zum Aufbau oder zur wesentlichen Änderung von Systemen zur automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten, sofern in den Systemen personenbezogene Daten verarbeitet werden.

Verletzungen des Schutzes personenbezogener Daten, die voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen, sind der LDA gemäß Artikel 33 DSGVO zu melden (siehe Ziffer 12).

8 Betroffenenrechte (Artikel 12 bis 22 DSGVO)

Die Rechte der betroffenen Personen sind durch die DSGVO erheblich gestärkt worden. Dies gilt insbesondere für die Information der betroffenen Person bei einer Datenerhebung und das Recht auf Datenportabilität. Die §§ 10 bis 13 BbgDSG enthalten Regelungen, die die Rechte der betroffenen Personen unter Berücksichtigung der Spielräume der DSGVO beschränken und ergänzend anzuwenden sind. Ebenso können bereichsspezifische Regelungen des Bundes- oder Landesrechts Beschränkungen enthalten, die zu beachten sind (zum Beispiel § 32c Abgabenordnung, § 82 und 83 Zehntes Buch Sozialgesetzbuch).

Für Informationen und Mitteilungen an Betroffene enthält Artikel 12 DSGVO allgemeine Vorgaben. Informationen über Datenerhebungen und Mitteilungen zu geltend gemachten Rechten sind der betroffenen Person 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 nach Möglichkeit auf elektronischem Wege zu beantworten sind, wenn sie auf elektronischem Wege gestellt wurden.

Eine Neuerung enthält Artikel 12 Absatz 4 DSGVO. Nach dieser Norm muss der Verantwortliche der betroffenen Person antworten, wenn und soweit er nach einem Antrag auf Geltendmachung eines Betroffenenrechts untätig bleibt oder diesen ablehnt (siehe auch Erwägungsgrund 59 Satz 3 DSGVO). Neben einer Begründung für die Untätigkeit oder Ablehnung ist die betroffene Person in der Antwort auch über die Möglichkeit zur Beschwerde bei einer Aufsichtsbehörde zu unterrichten.

Informationen über Datenerhebungen und Mitteilungen bzw. Maßnahmen auf Anträge, mit denen die betroffene Person ihre Rechte geltend macht, erfolgen gemäß Artikel 12 Absatz 5 DSGVO unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen kann der Verantwortliche jedoch ein angemessenes Entgelt verlangen oder sich weigern, aufgrund eines Antrags tätig zu werden. In diesen Fällen muss der Verantwortliche jedoch den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen.

➔ **Handlungserfordernisse:**

- Zur Erfüllung von Rechten der betroffenen Personen und von entsprechenden Pflichten der öffentlichen Stelle sind organisatorische Maßnahmen zu folgenden Punkten festzulegen:
  - Wer ist innerhalb der öffentlichen Stelle zuständig, wenn eine betroffene Person Rechte geltend macht?
  - In welcher Frist (unter Beachtung der Monatsfrist nach DSGVO) soll das Anliegen der betroffenen Person weitergeleitet und bearbeitet werden?
  - In welcher Form soll das Anliegen weitergeleitet werden (Stichworte: Geheimhaltung und Vertraulichkeit)?
  - Wer sind die Ansprechpartner für verschiedene Datenverarbeitungssysteme (um beispielsweise den Auskunftsanspruch überall in der öffentlichen Stelle gewährleisten zu können)?
- Es sind insbesondere Verfahren zu definieren, wie die Informationspflichten nach Artikel 13 und 14 DSGVO erfüllt werden sollen. Für Standardverarbeitungen empfiehlt sich die Verwendung von Mustern.

8.1 Informationspflichten des Verantwortlichen (Artikel 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 einen Anlass zu haben, ihre 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.

Gerade mit Blick auf Artikel 12 Absatz 1 DSGVO, der fordert, dass datenschutzrechtliche Informationen und Mitteilungen leicht zugänglich sind sowie in verständlicher, klarer und einfacher Sprache verfasst sind, kann es in der Praxis insbesondere dann zu Problemen kommen, wenn die betroffene Person nicht

über ausreichend Deutschkenntnisse verfügt, um den Inhalt der Informationen nach Artikel 13 und 14 DSGVO zu verstehen. In ihrer Handreichung „Wie erfülle ich als Verantwortlicher meine Informationspflichten?“ (https://www.lda.brandenburg.de/lda/de/service/informationsmaterial/details/~30-12-2019-wie-erfuelle-ich-als-verantwortlicher-meine-informationspflichten) führt die LDA aus, dass es zwar empfehlenswert und zu begrüßen sei, wenn die Informationen auch in anderen Sprachen zur Verfügung gestellt werden. Eine Verpflichtung dazu besteht jedoch nicht, da bei öffentlichen Stellen der Grundsatz gilt, dass die Amtssprache im Inland deutsch ist. Die Bereitstellung der Informationen in deutscher Sprache ist daher dem Grunde nach ausreichend.

Zur Erfüllung der Informationspflichten finden sich in den →**Anlagen 7a und 7b** Mustertexte mit Hinweisen. Wesentliche Angaben nach Artikel 13 und 14 DSGVO decken sich mit den Angaben im Verzeichnis von 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, diese also zum Beispiel aus öffentlichen Quellen oder von Dritten stammen (Artikel 14 DSGVO)
- oder beabsichtigt wird, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den diese Daten erhoben oder erlangt wurden (sogenannte „Zweckänderung“, Artikel 13 Absatz 3 bzw. 14 Absatz 4 DSGVO).

Für die drei genannten Fälle wird folgendes Prüfschema vorgeschlagen:
1. Liegt ein Fall von Artikel 13 oder Artikel 14 DSGVO oder eine Zweckänderung vor?
2. Gibt es einschlägige Ausnahmen oder wurde die betroffene Person bereits anderweitig informiert?
3. Wann, in welcher Form und mit welchem Inhalt ist die betroffene Person zu informieren?

8.1.1 Informationspflicht bei einer Erhebung bei der betroffenen Person (Artikel 13 DSGVO)

1. Liegt ein Fall von Artikel 13 DSGVO vor?

Voraussetzung für die Informationspflicht nach Artikel 13 DSGVO ist, dass der Verantwortliche die personenbezogenen Daten bei der betroffenen Person erhebt. Eine Erhebung bei der betroffenen Person setzt voraus, dass der Verantwortliche die Daten mit Kenntnis der betroffenen Person selbst aktiv bei dieser beschafft. Werden personenbezogene Daten von der betroffenen Person selbst und ohne Vorgaben oder Aufforderung (preis)gegeben bzw. an den Verantwortlichen übersandt, liegt noch 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 (zum Beispiel über ein Kontaktformular oder ein Online-Bewerbungssystem).

- 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 persönlichen Gesprächs, zum Beispiel am Telefon, erfragt.

Beispiele für nicht aktiv beschaffte Daten:
- Eine Person wendet sich mit einer allgemeinen Anfrage an die Behörde.
- Eine Person reicht eine allgemeine Beschwerde ein.
- Eine Person sendet initiativ Bewerbungsunterlagen per Post oder E-Mail an die öffentliche Stelle.

Eine Erhebung findet bei nicht aktiv beschafften Daten jedoch möglicherweise im Anschluss dadurch statt, dass unaufgefordert übersandte personenbezogene Daten von dem Verantwortlichen nicht sofort gelöscht oder diese in einen eigenen Vorgang übernommen und verarbeitet werden.

Werden die personenbezogenen Daten nicht bei der betroffenen Person selbst erhoben, sondern zum Beispiel von einer anderen öffentlichen Stelle oder über eine Recherche im Internet erlangt, ist zu prüfen, ob ein Fall des Artikel 14 DSGVO vorliegt.

2. Gibt es einschlägige Ausnahmen oder wurde die betroffene Person bereits anderweitig informiert?

Ausnahmen finden sich in Artikel 13 Absatz 4 DSGVO und § 10 BbgDSG oder können sich aus Fachgesetzen ergeben. Verfügt die betroffene Person beispielsweise bereits über die Informationen, besteht keine Informationspflicht für den Verantwortlichen (Artikel 13 Absatz 4 DSGVO).

Beispiel für eine Ausnahme von der Informationspflicht:
In einem Verwaltungsverfahren ist es 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 erneuten Datenerhebung bei der betroffenen Person führen, löst dies grundsätzlich keine neue Informationspflicht aus.

Zudem ist es nicht erforderlich, eine Person zu informieren, wenn sich die Informationen eindeutig aus den Umständen der Erhebung ergeben (Beispiel: Fahrkartenkontrolle). Auch bei wiederholten Erhebungen, die dem gleichen Zweck dienen, kann grundsätzlich davon ausgegangen werden, dass die betroffene Person bereits über die Information verfügt (Beispiel: wiederholte Lebensmittelkontrollen im gleichen Betrieb). Eine Wiederholung der Information ist in diesen Fällen nicht erforderlich.

Die Pflicht zur Information der betroffenen Person besteht des Weiteren nach § 10 Absatz 1 BbgDSG 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,
- die Information die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen oder

– die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder wegen der überwiegenden Rechte und Freiheiten anderer Personen geheim zu halten ist.

Unterbleibt die Information der betroffenen Person nach § 10 Absatz 1 BbgDSG, so hat der Verantwortliche gemäß § 10 Absatz 2 BbgDSG jedoch die Informationen in allgemeiner Form für die Öffentlichkeit zur Verfügung zu stellen, zum Beispiel auf der Internetseite (zu Datenschutzerklärungen auf Internetseiten siehe Ziffer 8.1.5). Zudem hat der Verantwortliche festzuhalten, aus welchen Gründen von einer Information abgesehen wird.

Beispiel für eine Ausnahme nach § 10 Absatz 1 BbgDSG:
Eine Person gibt einen Notruf über eine allgemeine Notrufnummer ab. Müsste bei einem Notruf zunächst den Informationspflichten bei der Erhebung personenbezogener Daten nachgekommen werden, würde dies die Bearbeitung des Notrufs und in der Folge den (erforderlichen) Rettungseinsatz verzögern. Hierdurch wären die Rechte oder Rechtsgüter der betroffenen Person oder anderer und damit die öffentliche Sicherheit gefährdet. Die Pflicht zur Information besteht in diesem Fall grundsätzlich nicht, da die Information die öffentliche Sicherheit gefährden würde (§ 10 Absatz 1 Nummer 1 BbgDSG). Entfällt die individuelle Mitteilung der Informationen nach Artikel 13 DSGVO, sollten – aus Transparenzgründen und um dem Erfordernis des § 10 Absatz 2 BbgDSG nachzukommen – allgemeine Informationen, die die nach Artikel 13 DSGVO erforderlichen Angaben umfassen, für die Öffentlichkeit zum Beispiel auf der Internetseite des Verantwortlichen veröffentlicht werden.

Es sollte regelmäßig überprüft werden, ob die Voraussetzungen des § 10 Absatz 1 BbgDSG weiterhin vorliegen. Ist dies nicht (mehr) der Fall, so muss die betroffene Person gegebenenfalls über die Datenverarbeitung informiert werden.

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

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. Die Person kann schriftlich oder in einer anderen Form, gegebenenfalls auch elektronisch, informiert werden.

– Erhebung von personenbezogenen Daten durch Formulare (zum Beispiel Papier, Word oder PDF)

  Bei Erhebungen durch Papierformulare können den betroffenen Personen die erforderlichen Informationen nach Artikel 13 DSGVO auf dem jeweiligen Formular oder durch ein separates Begleitdokument mitgeteilt werden.

  Werden die Formulare auf der Internetseite zum Download zur Verfügung gestellt, können auch hier die Informationen nach Artikel 13 DSGVO in dem jeweiligen Formular gegeben oder in einem separaten Begleitdokument deutlich sichtbar auf der gleichen Seite zum Download zur Verfügung gestellt werden. Alternativ kann direkt auf der gleichen Seite, auf der das Formular zum Download angeboten wird, zum Beispiel unter dem Downloadlink, über die Verarbeitung informiert werden. In diesen Fällen sollte zusätzlich in den Formularen selbst auf dieses zum Download angebotene Begleitdokument bzw. diese Internetseite mittels eines Links hingewiesen werden.

Es besteht auch die Möglichkeit, in dem entsprechenden Papierformular oder in dem zum Download angebotenen Formular deutlich sichtbar einen Link zu verwenden, der zur Datenschutzerklärung der öffentlichen Stelle mit den entsprechenden Hinweisen nach Artikel 13 DSGVO sowie gegebenenfalls Artikel 14 DSGVO führt (zu Datenschutzerklärungen auf Internetseiten siehe Ziffer 8.1.5). Angesichts der hohen Internet-Zugangsquote in der EU vertritt der EDSA zwar die Ansicht, dass in Fällen, in denen Verantwortliche eine Internetseite betreiben, der Einsatz elektronischer Datenschutzerklärungen eine geeignete Maßnahme zur Übermittlung von Transparenzangaben sei. Je nach den Umständen müsse der Verantwortliche allerdings gegebenenfalls zusätzlich auch sonstige Möglichkeiten für die Informationsübermittlung nutzen (siehe Randnummer 40 der vom EDSA bestätigten Leitlinien für Transparenz der Artikel-29-Gruppe, WP 260 Rev. 01, aufrufbar unter: https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html). Zu beachten ist daher, dass bestimmten Personen der Zugang zum Internet in Brandenburg eventuell nicht oder nur eingeschränkt möglich ist. Zudem sind Fälle zu berücksichtigen, bei denen man davon ausgehen kann, dass die betroffene Person zum Beispiel alters- oder sozialbedingt nicht oder nur eingeschränkt mit der Nutzung des Internets vertraut ist. Sofern vorgesehen ist, (nur) einen Link zu einer Internetseite zu verwenden, sollte in einem Papierformular mindestens auf die wichtigsten Informationen und zusätzlich darauf hingewiesen werden, dass die Informationen nach Artikel 13 DSGVO auf Wunsch zum Beispiel telefonisch beim Sachbearbeiter erfragt, per Fax oder postalisch in Papierform zugesandt werden können. Hierzu wird empfohlen, verschiedene nach Bedarf und gegebenenfalls Fachbereich angepasste und standardisierte Hinweistexte in Brief-Vorlagen einzufügen und diese für die öffentliche Stelle einheitlich zu verwenden (siehe dazu auch Ziffer 8.1.7).

Beispiel für eine Formulierung in Formularen:
„Als für die Datenverarbeitung Verantwortlicher verarbeitet … *[die öffentliche Stelle]* Ihre Angaben in diesem Formular, um … *[Zwecke der Verarbeitung].* Unsere Datenschutzhinweise gemäß Artikel 13 Datenschutz-Grundverordnung können Sie unter … *[Link zur Internetseite mit den konkreten Datenschutzinformationen]* aufrufen. Bei Bedarf können wir Ihnen diese Datenschutzhinweise postalisch in Papierform zusenden."

– Erhebung von personenbezogenen Daten im Internet (zum Beispiel Online-Anträge oder E-Mails)

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

Werden Antragsformulare oder ähnliches per E-Mail an Personen verschickt oder personenbezogene Daten durch E-Mails abgefragt, können die erforderlichen Informationen als Anlage (zum Beispiel als PDF-Dokument) beigefügt und im E-Mail-Text deutlich auf die Datenschutzinformationen in der Anlage hingewiesen werden. Empfohlen wird jedoch, verschiedene nach Bedarf und gegebenenfalls Fachbereich angepasste Standard-Signaturen für E-Mails zu formulieren und zu verwenden (siehe dazu auch Ziffer 8.1.7).

– Erhebung von personenbezogenen Daten bei persönlichen Gesprächen (zum Beispiel Telefonate oder Vor-Ort-Gespräche)

  Auch bei der mündlichen Erhebung von personenbezogenen Daten besteht die Informationspflicht, wenn nicht eine der zuvor genannte Ausnahmen greift. Gibt eine Person beispielsweise unaufgefordert personenbezogene Daten über sich Preis und werden (gegebenenfalls im weiteren Verlauf des Gesprächs) auch keine personenbezogenen Daten selbst aktiv beschafft, handelt es sich grundsätzlich nicht um eine Erhebung bzw. verfügt die betroffene Person aufgrund der Umstände gegebenenfalls bereits über die erforderlichen Informationen. In diesen Fällen besteht dem Grunde nach keine Informationspflicht nach Artikel 13 DSGVO.

  Werden personenbezogene Daten mündlich erhoben, wird empfohlen, die betroffene Person auf die Erhebung der Daten hinzuweisen und anzugeben, wo und wie die Informationen nach Artikel 13 DSGVO zur Verfügung gestellt werden (zum Beispiel durch Aushänge vor Ort, auf der Internetseite, durch Übermittlung per E-Mail oder Post). Des Weiteren können Informationsblätter vorgehalten, auf diese hingewiesen und auf Anfrage der betroffenen Person an diese ausgegeben werden. Sofern den Umständen nach angemessen, besteht zum Beispiel bei der Erhebung von Daten im Rahmen von Telefongesprächen die Möglichkeit, der betroffenen Person während des Gesprächs kurz und bündig die Informationen nach Artikel 13 DSGVO mündlich mitzuteilen.

– Erhebung von personenbezogenen Daten durch Weiterverarbeitung von unaufgefordert übermittelten Daten

  Werden der öffentlichen Stelle ohne vorherige Aufforderung personenbezogene Daten von der betroffenen Person zum Beispiel per Brief oder E-Mail übermittelt und der Verantwortliche löscht die Daten nicht, sondern verarbeitet diese zum Beispiel dadurch, dass die Daten in einen Vorgang übernommen werden, ist die betroffene Person über die Datenverarbeitung zu informieren. Denkbar ist, der Person die notwendigen Informationen zusammen mit einer Eingangsbestätigung zukommen zu lassen.

  Erfolgt die Eingangsbestätigung per E-Mail kann auch hier durch eine beigefügte Anlage informiert und im E-Mail-Text deutlich auf die Datenschutzinformationen in der Anlage hingewiesen werden. Die Verwendung von nach Bedarf und gegebenenfalls Fachbereich angepassten Standard-Signaturen für E-Mails ist ebenfalls möglich (siehe auch Ziffer 8.1.7). Soll eine Eingangsbestätigung per Brief an die Person geschickt werden, besteht die Möglichkeit, in dem Anschreiben deutlich sichtbar einen Link zu verwenden, der zur Datenschutzerklärung der öffentlichen Stelle mit den entsprechenden Hinweisen nach Artikel 13 DSGVO führt (zu Datenschutzerklärungen auf Internetseiten siehe Ziffer 8.1.5). Auch hier wäre zu beachten, dass betroffenen Personen der Umgang mit dem Internet nicht vertraut oder Zugang zum Internet in Brandenburg eventuell nicht oder nur eingeschränkt möglich ist. Daher sollte neben einem Link zur Internetseite in dem Anschreiben mindestens auf die wichtigsten Informationen nach Artikel 13 DSGVO und zusätzlich darauf hingewiesen werden, dass die Informationen auf Wunsch zum Beispiel telefonisch beim Sachbearbeiter erfragt, per Fax oder postalisch in Papierform zugesandt werden können (zu standardisierten Hinweistexten für Brief-Vorlagen siehe auch Ziffer 8.1.7).

→**Anlage 7a** enthält einen Mustertext mit allen nach Artikel 13 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. Bereits vor Geltung der DSGVO bestehende Formulare für Datenerhebungen sind an die neuen gesetzlichen Vorgaben anzupassen und zu ergänzen.

8.1.2 Informationspflicht bei der Erhebung nicht bei der betroffenen Person (Artikel 14 DSGVO)

1. Liegt ein Fall von Artikel 14 DSGVO vor?

Voraussetzung für die Informationspflicht nach Artikel 14 DSGVO ist, dass die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden. Die betroffene Person dient also nicht selbst als unmittelbare Datenquelle. Eine Erhebung von Daten auf andere Weise als bei der betroffenen Person umfasst grundsätzlich auch das Erlangen von Daten, die von Dritten ohne Aufforderung oder Befragung übermittelt werden.

Beispiele für Erhebungen nicht bei der betroffenen Person:
- Die öffentliche Stelle erlangt Daten der betroffenen Person aus öffentlich verfügbaren Quellen wie aus der Zeitung, dem Internet oder durch eine Besichtigung allgemein zugänglicher Verkehrsflächen.
- Personenbezogene Daten werden von einer anderen öffentlichen Stelle oder einem anderen Dritten auf Anfrage oder aufgrund von Rechtsvorschriften übermittelt.
- Die öffentliche Stelle verschafft sich personenbezogene Daten über einen Adresshändler.

Werden personenbezogene Daten an eine andere öffentliche Stelle auf deren Anfrage übermittelt, löst diese Datenübermittlung, soweit keine Zweckänderung vorliegt, keine Informationspflicht der übermittelnden öffentlichen Stelle aus. Es liegt vielmehr aus Sicht der anfragenden öffentlichen Stelle eine Erhebung nach Artikel 14 DSGVO vor. In diesem Fall hat also grundsätzlich die empfangende Stelle entsprechend dem Mustertext der →**Anlage 7b** eine umfassende Information der betroffenen Person sicherzustellen und dabei unter Ziffer 4 („Quelle der Daten“) darzulegen, von welcher anderen Stelle die Daten übermittelt wurden.

Im Übrigen ist nach § 7 BbgDSG die dritte Person oder eine nicht-öffentliche Stelle, bei denen personenbezogene Daten über die betroffene Person erhoben werden, auf Verlangen über den Erhebungszweck zu unterrichten, soweit dadurch schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden. Durch diese Information gegenüber Dritten soll auch ihnen gegenüber ein größtmögliches Maß an Transparenz hergestellt werden. Werden die Daten aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, ist auf die Auskunftspflicht, sonst auf die Freiwilligkeit hinzuweisen.

2. Gibt es einschlägige Ausnahmen oder wurde die betroffene Person bereits anderweitig informiert?

Ausnahmen finden sich in Artikel 14 Absatz 5 DSGVO und § 10 BbgDSG (siehe Ausführungen zu § 10 BbgDSG unter Ziffer 8.1.1) oder können sich aus Fachgesetzen 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 (Artikel 14 Absatz 5 Buchstabe a DSGVO).

- 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 (Artikel 14 Absatz 5 Buchstabe b DSGVO). In der Praxis wird diese Ausnahme nur selten zur Anwendung kommen. Gegenüber Dritten, von denen anlässlich einer Erhebung von Daten zu einer Person ebenfalls personenbezogene Daten erhoben werden, besteht jedenfalls dann in der Regel keine Informationspflicht, wenn diese nicht selbst am Verfahren beteiligt, ihre Daten also als sogenannter „Beifang" verarbeitet werden, und eine Information einen unverhältnismäßigen Aufwand verursachen würde.

  Beispiel für einen unverhältnismäßigen Aufwand:
  Ein großes städtisches Krankenhaus verlangt bei Behandlungen, längerfristigen Aufenthalten und Terminen von allen Patienten das Ausfüllen eines Papierfragebogens, in dem Angaben zu zwei Angehörigen (=die hier nach Artikel 14 DSGVO betroffenen Personen) gemacht werden sollen. Angesichts des hohen täglichen Patientenaufkommens in dem Krankenhaus wäre es mit einem unverhältnismäßigen Aufwand verbunden, jeden Tag alle aufgeführten Angehörigen nach Artikel 14 DSGVO zu informieren.

- 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 (Artikel 14 Absatz 5 Buchstabe c DSGVO).

  Beispiel für eine Rechtsvorschrift nach Artikel 14 Absatz 5 Buchstabe c DSGVO:
  Nach § 22a Einkommenssteuergesetz in Verbindung mit § 93c Abgabenordnung erhält die zentrale Stelle für Altersvermögen unter anderem von den Trägern der gesetzlichen Rentenversicherung Angaben zu Rentenbezügen von Steuerpflichtigen (=die hier nach Artikel 14 DSGVO betroffenen Personen). Da die Erlangung der personenbezogenen Daten ausdrücklich rechtlich festgelegt ist, finden die Informationspflichten in diesem Fall keine Anwendung.

- wenn die personenbezogenen Daten dem Berufsgeheimnis unterliegen und daher vertraulich behandelt werden müssen (zum Beispiel ein Rechtsanwalt, der von seinem Mandanten personenbezogene Daten über den Prozessgegner erhält).

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

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. Die erforderlichen Informationen könnten auch in diesem Fall direkt im E-Mail-Text oder als Anlage (zum Beispiel als PDF) beigefügt werden, wobei im E-Mail-Text deutlich auf die Datenschutzinformationen in der Anlage hingewiesen werden sollte.

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 Buchstabe a DSGVO). Sollen die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden (zum Beispiel Verwendung der Kontaktdaten für ein Anschreiben), ist die Informationspflicht spätestens zum Zeitpunkt der ersten Mitteilung im Rahmen der Kontaktaufnahme mit der betroffenen Person zu erfüllen (Artikel 14 Absatz 3 Buchstabe b DSGVO), jedoch nicht später als einen Monat nach Erlangen der Daten (Artikel 14 Absatz 3 Buchstabe a DSGVO). Falls eine Offenlegung an einen anderen Empfänger beabsichtigt ist, ist die Information spätestens zum Zeitpunkt der ersten Offenlegung zu erteilen (Artikel 14 Absatz 3 Buchstabe c DSGVO), jedoch nicht später als einen Monat nach Erlangen der Daten (Artikel 14 Absatz 3 Buchstabe a DSGVO).

→**Anlage 7b** 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. Bereits vor Geltung der DSGVO bestehende Formulare sind an die neuen gesetzlichen Vorgaben anzupassen und zu ergänzen.

8.1.3 Informationspflicht bei einer Zweckänderung

1. Liegt eine Zweckänderung vor?

Beabsichtigt der Verantwortliche, personenbezogene Daten für einen anderen Zweck weiterzuverarbeiten als den, 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). Generell liegt keine Zweckänderung vor, wenn die Daten für die in § 5 Absatz 2 BbgDSG genannten Zwecke verarbeitet werden. Zu diesen Zwecken zählen die Wahrnehmung von Aufsichts- und Kontrollbefugnissen, die Rechnungsprüfung, die Durchführung von Organisationsuntersuchungen und, sofern dies unerlässlich ist und schutzwürdige Belange der betroffenen Person dem nicht entgegenstehen, die Verarbeitung zu Aus- und Fortbildungszwecken. Zulässige Zweckänderungen, die grundsätzlich eine Informationspflicht auslösen, sind in § 6 BbgDSG geregelt (siehe Ausführungen zu § 6 BbgDSG unter Ziffer 4), ergeben sich aus bereichsspezifischem Fachrecht oder aus Artikel 6 Absatz 4 DSGVO unmittelbar (Stichwort: Vereinbarkeit des neuen Zwecks mit den Erhebungszwecken).

2. Gibt es einschlägige Ausnahmen oder wurde die betroffene Person bereits anderweitig informiert?

Eine Information der betroffenen Person kann unter den Voraussetzungen des § 6 Absatz 2 in Verbindung mit Absatz 1 Nummer 1 bis 4 BbgDSG unterbleiben (siehe auch Ziffer 4). Die Pflicht zur Information der betroffenen Person kann zudem auch im Falle einer Zweckänderung gegebenenfalls gemäß § 10 BbgDSG unter bestimmten Voraussetzungen entfallen (siehe Ausführungen zu § 10 BbgDSG unter Ziffer 8.1.1).

Keine Informationspflicht lösen die Fälle aus, in denen personenbezogene Daten aufgrund einer speziellen gesetzlichen Übermittlungspflicht übermittelt oder weitergegeben werden. In diesen Fällen gilt grundsätzlich die Ausnahme von Artikel 14 Absatz 5 Buchstabe c DSGVO.

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

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 eine Erhebung nicht bei der betroffenen Person (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 7a** und →**Anlage 7b** enthalten unter dem Punkt „Sonderfall" entsprechende Mustertexte und Hinweise für Zweckänderungen. Bei Verwendung dieser Mustertexte sind die dort enthaltenen Angaben vollständig und auf die jeweilige Verarbeitungstätigkeit angepasst zur Verfügung zu stellen.

8.1.4 Informationspflicht bei einer Videoüberwachung öffentlich zugänglicher Räume

Für die Videoüberwachung öffentlich zugänglicher Räume enthalten § 28 Absatz 2 und 4 BbgDSG besondere Regelungen der Informationspflicht. Die Videoüberwachung und die Informationen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen (zum Beispiel durch Hinweisschilder, siehe auch Artikel 12 Absatz 7 DSGVO). Dabei sind der Verantwortliche, die Kontaktdaten der oder des Datenschutzbeauftragten und die Zwecke sowie die Rechtsgrundlage der Verarbeitung anzugeben. Weiterhin ist darauf hinzuweisen, dass alle weiteren Informationen nach Artikel 13 DSGVO beim Verantwortlichen eingeholt werden können. Können die Videoaufnahmen einer bestimmten Person zugeordnet werden oder werden die Videoaufnahmen zu einem anderen Zweck verarbeitet, so ist die betroffene Person gesondert darüber zu informieren. Eine Ausnahme hiervon besteht, wenn der Zweck der Verarbeitung durch die Information gefährdet wird.

8.1.5 Bereitstellung von Informationen auf der Internetseite

Auf der Internetseite einer öffentlichen Stelle nicht nur über Datenverarbeitungen im Zusammenhang mit der Nutzung der Internetseite zu informieren, sondern auch über weitere Verarbeitungstätigkeiten im Rahmen der Aufgabenerfüllung der öffentlichen Stelle, bietet zahlreiche Vorteile. Zum einen können sich interessierte Bürgerinnen und Bürger selbst ohne Umwege direkt auf der Internetseite über die Verarbeitung von Daten der öffentlichen Stelle informieren. Ihnen wird dadurch größtmögliche Transparenz geboten. Anfragen kann so gezielt vorgebeugt werden bzw. können Bürgerinnen und Bürger bei Anfragen zu Datenschutzinformationen auf die Datenschutzerklärung verwiesen werden. Zum anderen ist es in zahlreichen Fällen schnell und einfach durch Verlinkung auf die Datenschutzerklärung möglich, den Informationspflichten nach Artikel 13 und 14 DSGVO nachzukommen. Lange Texte in E-Mails, PDF-Anhänge oder seitenlange Beiblätter in Anschreiben können sich dadurch häufig erübrigen.

Entscheidet sich eine öffentliche Stelle, proaktiv auf ihrer Internetseite über Verarbeitungen im Rahmen ihrer Aufgabenerfüllung zu informieren, ist zu beachten, dass für die jeweiligen Verarbeitungstätigkeiten spezifische Informationen bereitzustellen sind. Im Ergebnis werden auf der Internetseite insofern viele unterschiedliche Hinweise mit Informationen nach Artikel 13 und 14 DSGVO zur Verfügung stehen.

Zwar könnten diese Informationen als PDF-Dateien zum Download angeboten werden. Im Sinne der Barrierefreiheit (PDF-Dokumente sind in der Regel nicht barrierefrei) sollten die Informationen aber in Textform direkt auf der Internetseite der öffentlichen Stelle veröffentlicht werden. Dabei ist zu beachten, dass

Bürgerinnen und Bürger bei der Vielzahl an Informationen nicht den Überblick verlieren. Die Informationen sollten strukturiert und übersichtlich bereitgestellt werden. Es empfiehlt sich daher eine Unterteilung in verschiedene Abschnitte. Aus Gründen der Übersichtlichkeit könnte die Datenschutzerklärung entweder mit Hilfe eines sogenannten Akkordeons (ein Navigationselement zum Ein- und Ausklappen von Texten) gestaltet oder zu Beginn eine Art Inhaltsverzeichnis mit Links zu den entsprechenden Abschnitten eingefügt werden (mit Hilfe von sogenannten „Ankern" bzw. „Sprungmarken"). So können sich Interessierte leichter durch die und zu den relevanten Informationen navigieren. Zwei konkrete Beispiele können der →**Anlage 7c** entnommen werden.

Neben einer besseren Navigation und Übersichtlichkeit ist ein weiterer Vorteil bei der Verwendung von Ankern und Akkordeon-Elementen, dass gezielt auf bestimmte Abschnitte der Datenschutzerklärung verlinkt werden kann. So kann zum Beispiel in Anschreiben auf entsprechende Abschnitte mit den notwendigen Informationen in der Datenschutzerklärung verlinkt werden (zur Bereitstellung von Informationen in Anschreiben und E-Mail-Signaturen siehe Ziffer 8.1.7).

8.1.6 Verwendung von Cookies und ähnlichen technischen Komponenten

Sowohl der Bundesgerichtshof (BGH) als auch der Europäische Gerichtshof (EuGH) befassten sich unlängst mit dem Thema Cookie-Einwilligungen. Aus den Urteilen des EuGH vom 1. Oktober 2019 (C-673/17) und des BGH vom 28. Mai 2020 (I ZR 7/16) folgt, dass eine Einwilligung in Cookies, sofern eine solche Einwilligung erforderlich ist, keine Wirksamkeit hat, wenn ein Kästchen zur Einwilligung bereits vorausgefüllt bzw. angekreuzt ist. Auch Stillschweigen oder Untätigkeit können keine Einwilligung darstellen.

Es wird jedoch darauf hingewiesen, dass der Einsatz von Cookies nicht immer einwilligungsbedürftig ist. Eine Einwilligung der Nutzerinnen und Nutzer in Cookies ist dem Grunde nach nicht erforderlich, sofern der Einsatz für den technischen Betrieb einer Webseite erforderlich ist und keinem anderen als diesem Zweck dient. Beispielsweise könnte der Einsatz bestimmter Cookies gegebenenfalls zum Zweck der Verhinderung und Abwehr von Angriffen auf die Informationstechnik oder zum Erkennen und zur Beseitigung technischer Störungen oder Fehler erforderlich sein. Hingegen wird der Einsatz einer Webanalyse-Software zur Erstellung von Nutzungsprofilen und dem damit im Zusammenhang stehenden Einsatz von Cookies oder andere Formen des Trackings von Nutzerinnen und Nutzern in der Regel nicht zum technischen Betrieb einer Webseite erforderlich sein. In diesen Fällen ist das Einholen einer wirksamen Einwilligung nötig.

Aus diesen Gründen ist es nicht nur erforderlich, in der Datenschutzerklärung auf der Internetseite der öffentlichen Stelle über den Einsatz von Cookies oder anderen technischen Komponenten, mit denen personenbezogene Daten verarbeitet werden, transparent und verständlich zu informieren. Zusätzlich müssen Einwilligungen, soweit diese erforderlich sind, wirksam eingeholt und dokumentiert werden.

Ausführliche Informationen und Hinweise, was zu berücksichtigen ist, um Einwilligungen für technische Komponenten wie Cookies wirksam einzuholen, finden sich in der Orientierungshilfe der DSK für Anbieter von Telemedien (siehe insbesondere Seiten 9 und 10). Diese Orientierungshilfe kann unter dem folgenden Link abgerufen werden:
https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

8.1.7 Bereitstellung von Informationen in E-Mail-Signaturen und Anschreiben

Häufig befasst sich eine öffentliche Stelle mit der Beantwortung von Anfragen und verarbeitet hierbei personenbezogene Daten der Anfragenden (zum Beispiel durch Absenderangaben in Anschreiben und E-Mails oder durch persönliche Informationen, die freiwillig von den Personen gegeben werden). Sofern es sich dabei nicht um Verwaltungsverfahren, sondern allgemeine Anfragen und deren Beantwortung handelt, empfiehlt sich für öffentliche Stellen ein standardisierter Text für E-Mails und gegebenenfalls auch für Anschreiben. Der Standard-Text kann in solchen Fällen einheitlich von allen Mitarbeitenden der öffentlichen Stelle, die allgemeine Anfragen beantworten, verwendet werden, um betroffene Personen zu informieren und somit die Informationspflichten gemäß DSGVO zu erfüllen.

Insbesondere könnte ein solcher Standard-Text als Hinweis in intern vorgegebenen Brief-Vorlagen sowie in vorgegebenen E-Mail-Signaturen verwendet werden. Mitarbeitende der öffentlichen Stelle könnten dann auf diese Brief-Vorlagen zurückgreifen bzw. müssten ihre E-Mail-Signaturen nur einmalig anpassen. Gesonderte Beiblätter zu Anschreiben oder der E-Mail beigefügte PDF-Dokumente mit Informationen nach Artikel 13 und 14 DSGVO würden sich damit für zahlreiche Fälle erübrigen, da bereits durch den Hinweis in der Brief-Vorlage oder der E-Mail-Signatur die Informationspflichten in der Regel erfüllt wären.

Beispiel für eine allgemeine Datenschutzinformation in E-Mail-Signaturen:
Der telefonische, schriftliche oder elektronische Kontakt mit … [*Nennung der öffentlichen Stelle*] ist mit der Verarbeitung der von Ihnen gegebenenfalls mitgeteilten persönlichen Daten verbunden. Diese personenbezogenen Daten werden von uns verarbeitet, um Ihr Anliegen bearbeiten und um Sie im Rahmen der Beantwortung Ihres Anliegens gegebenenfalls kontaktieren zu können. Rechtsgrundlage hierfür ist Artikel 6 Absatz 1 Buchstabe e, Absatz 3 Datenschutz-Grundverordnung in Verbindung mit § 5 Absatz 1 Brandenburgisches Datenschutzgesetz.

Weitere Informationen finden Sie in unseren Datenschutzhinweisen unter dem folgenden Link: … [*Link zum speziellen Abschnitt/Akkordeon-Element der Datenschutzerklärung mit Informationen über Datenverarbeitungen bei Kontaktaufnahme mit der öffentlichen Stelle*]
Bei Bedarf können wir Ihnen diese Datenschutzhinweise postalisch in Papierform zusenden.

Darüber hinaus ist es möglich, auch für bestimmte Verwaltungsverfahren und damit zusammenhängende Verarbeitungen personenbezogener Daten spezifisch auf den betroffenen Fachbereich zugeschnittene Standard-Texte zu entwerfen, die dann ebenfalls in E-Mail-Signaturen und Brief-Vorlagen verwendet werden können. Voraussetzung wäre hierbei, dass in der Datenschutzerklärung auf der Internetseite der öffentlichen Stelle umfassende Informationen nach Artikel 13 und 14 DSGVO für den Fachbereich bzw. die Verarbeitung personenbezogener Daten im Rahmen des jeweiligen konkreten Verwaltungsverfahrens veröffentlicht sind, auf die verlinkt werden kann.

Beispiel für eine fachbereichsspezifische Datenschutzinformation in E-Mail-Signaturen:
Datenschutzinformationen für die Datenverarbeitung im Rahmen von Anträgen auf … (*zum Beispiel Wohngeld*):
Ihr Antrag ist mit der Verarbeitung der von Ihnen gegebenenfalls mitgeteilten persönlichen Daten durch … [*Nennung der öffentlichen Stelle*] verbunden. Diese personenbezogenen Daten werden von uns verarbeitet, um Ihren Antrag bearbeiten und Sie kontaktieren zu können. Rechtsgrundlage hierfür ist … [*Nennung der Rechtsgrundlage*].

Weitere Informationen finden Sie in unseren Datenschutzhinweisen unter dem folgenden Link: … [*Link zum speziellen Abschnitt/Akkordeon-Element der Datenschutzerklärung mit Informationen über die konkreten Datenverarbeitungen bei Anträgen auf …*]
Bei Bedarf können wir Ihnen diese Datenschutzhinweise postalisch in Papierform zusenden.

8.2 Recht auf Auskunft (Artikel 15 DSGVO)

Das Auskunftsrecht nach Artikel 15 DSGVO in Verbindung mit § 11 BbgDSG entspricht im Wesentlichen dem zuvor geltenden Recht auf Auskunft nach § 18 BbgDSG-alt. Anders als nach altem Recht ist in Artikel 15 DSGVO explizit geregelt, dass die betroffene Person auch einen Anspruch auf Information darüber hat, ob Daten über sie gespeichert sind. Ist dies der Fall, besteht ein Anspruch auf Auskunft über diese Daten und die Umstände der Datenverarbeitung.

Die Auskunft über die Empfänger oder Kategorien von Empfängern ist – ebenfalls anders als nach altem Recht – zu erteilen, unabhängig davon, ob diese gespeichert sind. Sind einzelne Empfänger nicht mehr gespeichert, sind in diesen Fällen die Kategorien von Empfängern anzugeben. Gegenüber der Auskunftspflicht nach dem BbgDSG-alt erweitert Artikel 15 DSGVO den Anspruchsumfang auf die geplante Dauer der Speicherung und das Vorliegen einer automatisierten Entscheidungsfindung. Zusätzlich umfasst das Auskunftsrecht nun auch einen Anspruch auf Informationen über das Bestehen eines Rechts auf Berichtigung oder Löschung der personenbezogenen Daten oder auf Einschränkung der Verarbeitung und einen Anspruch auf Informationen über das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde.

Bestehen Zweifel an der Identität der betroffenen Person, kann der Verantwortliche zusätzliche Informationen zum Nachweis der Identität anfordern (Artikel 12 Absatz 6 DSGVO). Gemäß Erwägungsgrund 63 Satz 6 DSGVO kann der Verantwortliche zudem verlangen, dass die betroffene Person präzisiert, auf welche Informationen oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht.

§ 11 Absatz 2 BbgDSG enthält eine spezifische Regelung zur Gewährung des Auskunftsanspruchs, wenn die Daten in Akten (in Papierform oder elektronisch) enthalten sind. In diesen Fällen kann der betroffenen Person, wie bisher, anstelle der Auskunft auch Akteneinsicht gewährt werden. Die Entscheidung hierüber steht im pflichtgemäßen Ermessen der Behörde. Zu berücksichtigen ist dabei, dass die Gewährung von Akteneinsicht den schutzwürdigen Interessen der betroffenen Person dienen kann und ob die Erteilung einer Auskunft einen unverhältnismäßigen Aufwand verursachen würden (siehe Begründung zu § 11 Absatz 2 BbgDSG, Landtags-Drucksache 6/7365).

Das Recht auf Auskunft der betroffenen Person umfasst künftig auch das Recht auf die Bereitstellung einer kostenlosen Kopie (Artikel 15 Absatz 3 DSGVO). Hierdurch dürfen jedoch nicht die Rechte anderer Personen beeinträchtigt werden (Artikel 15 Absatz 4 DSGVO).

8.3 Recht auf Berichtigung (Artikel 16 DSGVO)

Eine ähnliche Regelung zum Recht auf Berechtigung gab es bereits in § 19 Absatz 1 BbgDSG-alt. Die betroffene Person hat nach Artikel 16 DSGVO auch weiterhin das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Zudem hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten

zu verlangen. 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 für unvollständige Informationen:
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.

8.4 Recht auf Löschung (Artikel 17 DSGVO)

Der Verantwortliche hat personenbezogene Daten grundsätzlich zu löschen, wenn

- die Daten für den Zweck, zu dem sie erhoben wurden, nicht mehr erforderlich sind (Artikel 17 Absatz 1 Buchstabe a DSGVO)
- oder sie unrechtmäßig verarbeitet wurden (Artikel 17 Absatz 1 Buchstabe d DSGVO).

Des Weiteren besteht dem Grunde nach auch in den folgenden Fällen eine Löschpflicht:

- Die betroffene Person hat ihre Einwilligung widerrufen und es besteht keine anderweitige Rechtsgrundlage für die Verarbeitung (Artikel 17 Absatz 1 Buchstabe b DSGVO).
- Die betroffene Person hat Widerspruch gegen die Verarbeitung eingelegt und es liegen keine schützenswerten Gründe für die Verarbeitung vor (Artikel 17 Absatz 1 Buchstabe c DSGVO).
- Die Löschung ist aufgrund einer anderen Rechtsgrundlage erforderlich (Artikel 17 Absatz 1 Buchstabe e DSGVO).
- Ein Kind hat sich gemäß Artikel 8 Absatz 1 DSGVO eigenständig bei einem angebotenen Dienst der Informationsgesellschaft angemeldet (Artikel 17 Absatz 1 Buchstabe f DSGVO).

Die Löschpflicht besteht im Übrigen - wie auch nach altem Recht - nicht nur, wenn die betroffene Person dies verlangt. Vielmehr ist der Verantwortliche von sich aus verpflichtet, personenbezogene Daten zu löschen, wenn eine der Fallgruppen des Artikel 17 Absatz 1 DSGVO eintrifft und keine Ausnahmen von der Löschung bestehen.

So scheidet eine Löschung insbesondere nach Artikel 17 Absatz 3 Buchstabe b DSGVO (in Korrespondenz zu den Rechtsgrundlagen nach Artikel 6 Absatz 1 Buchstaben b und c DSGVO) aus, wenn die Verarbeitung der Daten zur Erfüllung einer Rechtspflicht oder einer öffentlichen Aufgabe erforderlich ist. Das ist insbesondere der Fall, wenn gesetzliche Aufbewahrungsfristen bestehen. Bestehen keine gesetzlichen Fristen, sind vom Verantwortlichen Aufbewahrungsfristen festzulegen. Dabei ist zu berücksichtigen, für wie lange die Daten zur Aufgabenerfüllung erforderlich sind; dies schließt die Aufgaben des Nachweises seines ordnungsgemäßen Verwaltungshandelns ein. Außerdem geht gemäß § 9 BbgDSG auch weiterhin die archivrechtliche Anbietungspflicht einer Löschung vor. Bei individuellen Begehren auf Löschung sind daher insbesondere die Rechtmäßigkeit der Verarbeitung und die Archivwürdigkeit der verarbeiteten Daten zu prüfen.

Keine Ausnahme besteht mehr in den Fällen, in denen personenbezogene Daten in Akten gespeichert waren. Anders als nach altem Recht 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 oder 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 Verarbeitung) 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. Besteht ein Anspruch auf Löschung, bezieht sich dieser nicht generell auf die Vernichtung einer gesamten Akte oder eines gesamten Vorgangs, sondern nur auf die Löschung der darin enthaltenen personenbezogenen Daten. In diesen Fällen ist zu prüfen, in welcher Weise dem bestehenden Löschungsgebot für diese abtrennbaren Teile oder in Bezug auf die enthaltenen personenbezogenen Daten Rechnung getragen werden kann (zum Beispiel durch Vernichtung von Aktenteilen oder Schwärzung).

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.

8.5 Recht auf Einschränkung der Verarbeitung (Artikel 18 DSGVO)

Unter der Einschränkung der Verarbeitung sind nach den Erwägungsgründen der DSGVO Methoden zur Beschränkung der Verarbeitung personenbezogener Daten zu verstehen, zum Beispiel dass ausgewählte personenbezogene Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzerinnen und Nutzer gesperrt werden oder dass veröffentlichte Daten vorübergehend von einer Webseite entfernt werden. Damit entspricht dieses Recht im weitesten Sinne dem alten Recht auf Sperrung nach § 19 Absatz 3 BbgDSG-alt.

Unter Geltendmachung des Rechts auf Einschränkung der Verarbeitung kann die betroffene Person verlangen, dass sämtliche erhobene personenbezogene Daten fortan nur mit individueller Einwilligung (und zur Geltendmachung und Durchsetzung von Rechtsansprüchen) verarbeitet werden dürfen. Die Berechtigung des Verantwortlichen zur Speicherung wird dadurch allerdings nicht berührt. Ist eine Einschränkung der Verarbeitung erfolgt, soll er die gespeicherten Daten nur nicht wie bisher verwenden können.

Soll die Einschränkung der Verarbeitung aufgehoben werden, hat der Verantwortliche die Pflicht, die betroffene Person vor der Aufhebung der Einschränkung zu unterrichten.

Im Falle der Einschränkung der Verarbeitung ist der Verantwortliche gemäß Artikel 19 DSGVO (wie auch gemäß § 19 Absatz 5 BbgDSG-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.

8.6 Recht auf Datenübertragbarkeit (Artikel 20 DSGVO)

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. Sie haben außerdem das Recht, diese Daten einem anderen für die Verarbeitung Verantwortlichen ohne Behinderung durch den für die Verarbeitung 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.

8.7 Widerspruchsrecht (Artikel 21 DSGVO)

Gemäß Artikel 21 DSGVO hat die betroffene Person – wie zuvor gemäß § 4b BbgDSG-alt - ein allgemeines Widerspruchsrecht gegen eine an sich rechtmäßige Verarbeitung von personenbezogenen Daten, die im öffentlichen Interesse liegt, in Ausübung öffentlicher Gewalt oder aufgrund des berechtigten Interesses des Verantwortlichen oder eines Dritten erfolgt (Artikel 6 Absatz 1 Buchstabe e oder f DSGVO). Dabei ist Voraussetzung, dass die 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, berechtigt auch dies zu einem Widerspruch. 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, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.

Einschränkungen für das Recht auf Widerspruch bestehen nach § 13 BbgDSG. Demnach besteht ein Widerspruchsrecht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet. Darüber hinaus enthält § 25 Absatz 5 BbgDSG spezifische Einschränkungen des Widerspruchsrechts für die Datenverarbeitung zu wissenschaftlichen und historischen Forschungszwecken.

9 Gemeinsam Verantwortliche

Nach Artikel 4 Nummer 7 in Verbindung mit 26 Absatz 1 DSGVO handeln zwei oder mehr Verantwortliche als gemeinsam Verantwortliche, wenn sie gemeinsam die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegen. Das bedeutet, dass bei gemeinsam Verantwortlichen alle Beteiligten bewusst zusammenarbeiten und wesentlich über die Zwecke und Mittel der Verarbeitung (mit)entscheiden, wobei abgestufte Einflussmöglichkeiten auf Zwecke und/oder Mittel und daher unterschiedliche Ausprägungen der jeweiligen Verantwortungsbereiche möglich sind. Die Beteiligung an den Entscheidungen über Zwecke und Mittel der Verarbeitung muss nicht gleichmäßig verteilt sein. „Gemeinsam" kann auch bedeuten, dass die Zwecke und Mittel vollständig oder aber nur teilweise übereinstimmen, indem die Verantwortlichen jeweils nur über Zwecke, nur über die Mittel oder nur Teile davon entscheiden. Aufgrund der weiten Formulierung von Artikel 4 Nummer 7 DSGVO können auch Kooperationen, in denen mehrere Verantwortliche bei der Entwicklung von einem Programm bzw. einer Software zur Erfüllung ihrer Aufgaben zusammenarbeiten und dabei einem Beteiligten die Verantwortung für die DSGVO-Konformität des Programms oder der Software übertragen, als gemeinsam Verantwortliche gelten.

Beispiele für gemeinsam Verantwortliche:
PTravel: Für die Reisekostenabrechnung wird in der Landesverwaltung einheitlich PTravel eingesetzt. Die Staatskanzlei, die Landesministerien und die ihnen nachgeordneten Behörden, Einrichtungen und Landesbetriebe verarbeiten personenbezogene Daten zu eigenen (wenn auch gleichlautenden) Zwecken und nutzen PTravel gemeinsam als Mittel zur Verarbeitung, wobei jeder Verantwortliche die personenbezogenen Daten in getrennten Datenbeständen in PTravel verarbeitet. Darüber hinaus sind bestimmte Zuständigkeiten der einzelnen Verantwortlichen im Rahmen der Reisekostenabrechnungen durch Verordnungen auf die Zentrale Bezügestelle des Landes Brandenburg (ZBB) übertragen. Bei der Verarbeitung wird der Datenbestand der ZBB gemeinsam genutzt, wobei jeder Verantwortliche nur Zugriff auf die seinen Zuständigkeitsbereich betreffenden personenbezogenen Daten hat.

HKR-Verfahren: Im Rahmen des Neuen Finanzmanagements der Landesverwaltung wird zu Zwecken des Haushalts-, Kassen- und Rechnungswesens (HKR) die Software SAP eingesetzt. Die Verantwortlichen verarbeiten personenbezogene Daten sowohl zu eigenen als auch gemeinsamen Zwecken in bzw. aus einem gemeinsamen Datenbestand mit Hilfe von SAP als gemeinsam eingesetztes Mittel der Datenverarbeitung. Für die Weiterentwicklung des HKR-Verfahrens und die entsprechende Beauftragung von Dienstleistern ist das für Finanzen zuständige Ministerium verantwortlich.

EL.DOK: EL.DOK wird zur elektronischen Aktenhaltung und Vorgangsbearbeitung in der Landesverwaltung eingesetzt. Die Entscheidung über die Entwicklung und den Einsatz einer einheitlichen Software zu diesen Zwecken erfolgte dabei von den Ressorts gemeinsam, wobei die Verantwortung für die DSGVO-Konformität der Software und die damit verbundenen Verpflichtungen dem Ministerium des Innern und für Kommunales übertragen wurde. Die Verantwortung für die konkret erfolgenden Datenverarbeitungen bei der Vorgangsbearbeitung liegt bei den jeweiligen Dienststellen als Verantwortlicher.

Gemeinsame Verantwortung bedeutet jedoch nicht, dass alle Verantwortlichen auch für alle Verarbeitungsschritte und die Einhaltung aller datenschutzrechtlichen Anforderungen (im gleichen Maße) verantwortlich sind. Vor diesem Hintergrund bestimmt Artikel 26 Absatz 1 Satz 2 DSGVO, dass in einer Vereinbarung festzulegen ist, wer von den Verantwortlichen welche Verpflichtungen nach der DSGVO erfüllt,

sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht bereits durch nationale Rechtsvorschriften oder Rechtsvorschriften der Union geregelt sind. Zu beachten ist, dass die Verteilung von Zuständigkeiten für die Erfüllung bestimmter Aufgaben zwar durch Rechtsvorschriften geregelt sein kann. Wurde dabei die Verantwortung für die Erfüllung weiterer Aufgaben oder Verpflichtungen insbesondere aus der DSGVO nicht oder nicht ausreichend festgelegt, ist gleichwohl eine Vereinbarung bezüglich dieser Pflichten erforderlich, die die Rechtsvorschriften insoweit ergänzt.

Beispiel für eine nationale Rechtsvorschrift:
§ 11 Brandenburgisches E-Government-Gesetz und § 2 eID- und IT-Basiskomponentenverordnung regeln datenschutzrechtliche Einzelheiten zu den Befugnissen und Verpflichtungen des Brandenburgischen IT-Dienstleisters und den Pflichten der Behörden, soweit im Rahmen der Einrichtung und des Betriebs sowie der Nutzung von IT-Basiskomponenten personenbezogene Daten verarbeitet werden.

Gemäß Artikel 26 DSGVO ist, soweit nicht durch Rechtsvorschrift geregelt, in einer solchen Vereinbarung transparent festzulegen, wer unter den Verantwortlichen insbesondere für die Gewährleistung der Rechte der betroffenen Personen zuständig ist und wer welchen Informationspflichten nach Artikel 13 und 14 DSGVO nachkommt. Neben der Einhaltung der Betroffenenrechte (Artikel 12 ff. DSGVO) sind weitere Pflichten, die sich aus der DSGVO ergeben, insbesondere die Umsetzung von technischen und organisatorischen Maßnahmen (Artikel 24 Absatz 1 und Artikel 32 DSGVO), die Erstellung der Beschreibung für das Verzeichnis von Verarbeitungstätigkeiten der Verantwortlichen (Artikel 30 DSGVO), die Meldung und Dokumentation von Datenschutzverletzungen (Artikel 33 und 34 DSGVO) oder auch die Durchführung einer Datenschutz-Folgenabschätzung (Artikel 35 DSGVO). Auch diese Regelungspunkte sollten in der Vereinbarung nach Artikel 26 DSGVO festgeschrieben werden, um die Verteilung der datenschutzrechtlichen Verpflichtungen zwischen den Verantwortlichen in transparenter Weise festzulegen. Ebenso sollte in der Vereinbarung die Zuständigkeit für die Freigabe gemäß § 4 Absatz 1 BbgDSG geregelt werden.

Ist in den Fällen, in denen gemeinsam ein Programm oder eine Software entwickelt wird und einem beteiligten Verantwortlichen die Aufgabe der Umsetzung und Einhaltung der DSGVO übertragen werden soll, vorgesehen, einen Auftragsverarbeiter einzusetzen (zum Beispiel zur technischen Umsetzung oder zum Betrieb des Programms oder der Software), kann in der Vereinbarung nach Artikel 26 DSGVO ebenso die Zuständigkeit für den Abschluss eines Vertrags über die Auftragsverarbeitung geregelt und auf diesen beteiligten Verantwortlichen übertragen werden. Die anderen Verantwortlichen müssen dann in der Regel nicht alle einzeln Verträge mit dem Auftragsverarbeiter abschließen.

Artikel 26 DSGVO und auch eine Vereinbarung nach Artikel 26 DSGVO stellen im Übrigen keine eigene Rechtsgrundlage für die Datenverarbeitung dar. Die Verarbeitung durch jeden einzelnen Verantwortlichen muss (unabhängig vom Bestehen einer gemeinsamen Verantwortlichkeit) auf einer ausreichenden rechtlichen Grundlage nach Artikel 6 Absatz 1 oder Artikel 9 Absatz 2 DSGVO gegebenenfalls in Verbindung mit bundes- oder landesrechtlichen Vorschriften beruhen.

Ergänzend zu diesen Hinweisen wird auf die folgenden Veröffentlichungen und Entscheidungen hingewiesen:

- Leitlinie 7/2020 des EDSA zu Verantwortlichen und Auftragsverarbeitern:

https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de (nach Abschluss der öffentlichen Konsultation steht die Veröffentlichung der finalen Fassung zu Redaktionsschluss dieser Anwendungshinweise noch aus),
- EuGH-Urteil vom 05. Juni 2018 – C-2010/16 („Gemeinsame Verantwortlichkeit eines Fanpage-Betreibers und des dazugehörigen sozialen Netzwerks“),
- EuGH-Urteil vom 10. Juli 2018 – C-25/17 („Verarbeitung personenbezogener Daten bei Religionsgemeinschaften – Zeugen Jehovas“) und
- EuGH-Urteil vom 29. Juli 2019 – C-40/17 (Fashion ID gegen Verbraucherzentrale NRW).

Auch wenn sich die Entscheidungen des EuGH auf die Anwendung der am 25. Mai 2018 durch die DSGVO abgelösten Richtlinie 95/46/EG beziehen, sind die darin enthaltenen Erläuterungen weiterhin zur Heranziehung bei der Auslegung der DSGVO geeignet.

➔ **Handlungserfordernisse:**
- Bestehende Kooperationen sind im Hinblick auf eine gemeinsame Verantwortung zu überprüfen und gegebenenfalls ist eine Vereinbarung nach Artikel 26 DSGVO abzuschließen.
- Bei Bestehen einer gemeinsamen Verantwortung sind die entsprechenden Rechtsgrundlagen und die Vereinbarungen im Hinblick auf die Anforderungen gemäß Artikel 26 DSGVO zu überprüfen.

10 Auftragsverarbeitung

Auftragsverarbeiter ist, wer gemäß Artikel 4 Nummer 8 DSGVO personenbezogene Daten im Auftrag eines Verantwortlichen verarbeiten. Der Verantwortliche als Auftraggeber lagert dabei eine Datenverarbeitung an eine andere Stelle – den Auftragsverarbeiter – aus, behält aber die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung. Der Auftragsverarbeiter handelt dabei im Interesse des Verantwortlichen und unterliegt bei der Verarbeitung der Daten dessen Weisungen. Der Auftragsverarbeiter entscheidet nicht über Zwecke und Mittel der Verarbeitung, wobei ihm vom Verantwortlichen jedoch im Bereich der eingesetzten Mittel gewisse Entscheidungsspielräume (zum Beispiel bei der Wahl der technischen Mittel) zugestanden werden können, mit denen der Auftragsverarbeiter die Interessen des Verantwortlichen am besten wahrnehmen kann.

Die DSGVO regelt die Auftragsverarbeitung insbesondere in den Artikeln 28 und 29. Das bereichsspezifische Bundes- oder Landesrecht kann Regelungen enthalten, die das „Ob“ der Auftragsverarbeitung bestimmen, also die Frage betreffen, ob in bestimmten Fällen eine Auftragsverarbeitung zulässig ist (siehe zum Beispiel § 80 Zehntes Sozialgesetzbuch). Im Hinblick auf die Frage, wann von einer Auftragsverarbeitung ausgegangen werden muss und das „Wie“ der Auftragsverarbeitung, also die spezifischen Anforderungen an die Ausgestaltung der Auftragsverarbeitung, sind die Artikel 28 und 29 DSGVO dagegen abschließend und gelten unmittelbar.

Beispiele für eine Auftragsverarbeitung:
Die Auslagerung des Betriebs von Webservern oder eines Rechenzentrums, die Entsorgung von Datenträgern oder auch die Wartung von IT-Systemen, soweit dabei auf personenbezogene Daten zugegriffen

werden kann, sind in der Regel Auftragsverarbeitungen, wenn sich die öffentliche Stelle als Verantwortlicher zur Erfüllung solcher Tätigkeiten eines Dritten bedient.

10.1 Änderungen gegenüber der alten Rechtslage

Gegenüber der alten 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, siehe auch →**Anlage 4c**).
- 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 einlegen kann.
- Auftragsverarbeiter haben künftig Dokumentationspflichten und gegenüber dem Verantwortlichen eine Unterstützungsfunktion.
- 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 Regelungen in § 11 BbgDSG-alt hinaus. Im Vertrag sind Festlegungen zu treffen

- zum Gegenstand der Verarbeitung (zum Beispiel: Verweis auf die Leistungsvereinbarung des Vertrags, Darstellung der konkreten Aufgaben),
- zur Dauer der Verarbeitung (zum Beispiel: Laufzeit des Vertrages, Befristung, einmalige Ausführung),
- zum Zweck der Verarbeitung (zum Beispiel: Verweis auf die Leistungsvereinbarung, Beschreibung des Zwecks),
- zur Art der Verarbeitung (zum Beispiel: automatisierte Verarbeitung, Erheben, Erfassen, Ordnen),
- zur Art der verarbeiteten personenbezogenen Daten (zum Beispiel: Adressdaten, Personenstammdaten, Telekommunikationsdaten, Daten aus öffentlichen Verzeichnissen),
- zu den Kategorien betroffener Personen (zum Beispiel: Antragstellende, Beschäftigte, Ansprechpartner),
- zu den Pflichten und Rechten des Verantwortlichen (zum Beispiel Ausgestaltung des Weisungsrechts oder der Kontrollmöglichkeiten, siehe 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 Mitarbeitenden, 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 gegebenenfalls durch ergänzende Vereinbarungen an die neue Rechtslage anzupassen sind. Als Grundlage des Überprüfungsprozesses kann der als →**Anlage 8** beigefügte Mustervertragsentwurf genutzt werden. Auf welche Weise eine gegebenenfalls erforderliche Anpassung erfolgt, ob mit einer einvernehmlichen Vertragsänderung oder -ergänzung oder etwa im Wege einer außerordentlichen Kündigung aus wichtigem Grund, ist im Einzelfall zu bewerten und zu entscheiden.

10.3 Abgrenzung zu (gemeinsam) Verantwortlichen

Ob es sich abhängig vom Einzelfall um eine Auftragsverarbeitung im Sinne von Artikel 4 Nummer 8 DSGVO handelt oder die beteiligte Partei nicht als Auftragsverarbeiter, sondern selbst als (gegebenenfalls gemeinsam) Verantwortlicher im Sinne von Artikel 4 Nummer 7 DSGVO tätig ist, richtet sich danach, wer über Zwecke und Mittel der Datenverarbeitung entscheidet. Die Einstufung als Verantwortlicher oder als Auftragsverarbeiter muss jeweils im Hinblick auf den Einzelfall und die spezifische Datenverarbeitung anhand der faktischen tatsächlichen Verhältnisse und der Einflussmöglichkeiten auf die Zwecke und Mittel der Verarbeitung bewertet werden

Gemäß Artikel 4 Nummer 8 in Verbindung mit Artikel 28 DSGVO werden bei der Auftragsverarbeitung unter den Beteiligten die Zwecke und Mittel der Verarbeitung nicht gemeinsam festgelegt. Der Auftragsverarbeiter hat hierbei keine Entscheidungsmöglichkeit, wobei ihm vom Auftraggeber jedoch in der Wahl der technischen und organisatorischen Mittel gewisse Entscheidungsspielräume zugestanden werden können. Der Auftragsverarbeiter handelt im Auftrag und Interesse des Auftraggebers und ist an seine Weisungen zumindest hinsichtlich des Zwecks der Verarbeitung und der wesentlichen Elemente der Mittel gebunden. Zur Abgrenzung zwischen einem Auftragsverarbeiter und einem Verantwortlichen im Sinne von Artikel 4 Nummer 7 DSGVO können unter anderem folgende Kriterien herangezogen werden:

- die Zuständigkeit für die Aufgabenerfüllung,
- die Ausführlichkeit der vom Verantwortlichen erteilten Weisungen,
- die Beaufsichtigung bzw. Kontrolle durch den Verantwortlichen,
- die Außenwirkung gegenüber betroffenen Personen.

Ein Beteiligter, der einen rechtlichen oder tatsächlichen Einfluss auf die Entscheidung hat, wie personenbezogene Daten verarbeitet werden, ist hingegen als (gegebenenfalls gemeinsam) für die Verarbeitung Verantwortlicher tätig. Wenn die an der Datenverarbeitung beteiligte Partei daher personenbezogene Daten zu eigenen Zwecken (weiter)verarbeitet oder sie über Zwecke und Mittel der Datenverarbeitung selbst (mit)entscheiden kann, ist sie insofern nicht als Auftragsverarbeiter einzustufen.

Ergänzend wird zudem auf die folgenden Veröffentlichungen hingewiesen:

- Leitlinie 7/2020 des EDSA zu Verantwortlichen und Auftragsverarbeitern: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de (nach Abschluss der öffentlichen Konsultation steht die Veröffentlichung der finalen Fassung zu Redaktionsschluss noch aus),
- Kurzpapiere der DSK - Nummer 13 (Auftragsverarbeitung) und Nummer 16 (gemeinsam für die Verarbeitung Verantwortliche): https://www.datenschutzkonferenz-online.de/kurzpapiere.html

➔ **Handlungserfordernisse:**

- Bestehende Verträge sind darauf zu überprüfen, ob sie die Vorgaben von Artikel 28 DSGVO einhalten.
- Die Verträge zur Auftragsverarbeitung sind zu dokumentieren.

11 Technischer und organisatorischer Datenschutz

Die DSGVO enthält vor allem in den Artikeln 5, 24, 25 und 32 Vorgaben zur „Sicherheit der Verarbeitung". Es gilt das grundsätzliche Prinzip, dass geeignete technische und organisatorische Maßnahmen zu treffen sind, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten (zuvor § 10 Absatz 1 BbgDSG-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 die Pseudonymisierung und Verschlüsselung der Daten.

Die bisherigen sechs Schutzziele des BbgDSG-alt (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz) werden in Artikel 32 Absatz 1 Buchstabe b DSGVO zusammengefasst, wobei lediglich Vertraulichkeit, Integrität und Verfügbarkeit sowie das neu hinzugekommene Schutzziel der Belastbarkeit in der DSGVO ausdrücklich genannt werden. Während die ersten drei Schutzziele aus der ISO 27001 und dem vom Bundesamt für Sicherheit in der Informationstechnik entwickelten Grundschutz bekannt sind, bedarf das Schutzziel der Belastbarkeit mangels konkreter Vorgaben in der DSGVO der Interpretation. Am naheliegendsten erscheint, die Belastbarkeit von Diensten und Systemen hinsichtlich ihrer Widerstandsfähigkeit auszulegen, so dass diese also auch noch „unter Last oder starker Beanspruchung" funktionieren sollen, was gegebenenfalls 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 nach altem Recht im Rahmen

der Verfügbarkeit der Daten sicherzustellen. Die Wiederherstellung der Daten muss somit regelmäßig getestet werden.

Aus den Artikeln 24, 25 sowie 32 DSGVO ergeben sich darüber hinaus folgende 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 potentiellen 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 (auch genannt „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 Buchstabe d DSGVO muss nun auch die Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen regelmäßig geprüft und gegebenenfalls nachgesteuert werden.

➔ **Handlungserfordernisse:**

- Der Verantwortliche hat die technischen und organisatorischen Maßnahmen zu dokumentieren. Dies sollte insbesondere im Rahmen eines Sicherheitskonzeptes nach § 4 BbgDSG, das gegebenenfalls Teil des Datenschutzkonzeptes (siehe Ziffer 14) sein kann, erfolgen.
- Es ist ein Verfahren zu etablieren, das regelmäßig die Wirksamkeit der technischen und organisatorischen Maßnahmen bewertet und evaluiert. Hierfür empfiehlt sich die Einführung eines Datenschutz-Managementsystems.
- Die Prinzipien privacy by design und privacy by default sollten künftig bereits im Zuge der vergaberechtskonformen Ausschreibung von IT-Produkten berücksichtigt werden.

12 Umgang mit Verletzungen des Schutzes personenbezogener Daten

12.1 Begriffsbestimmung und mögliche Folgen von Datenschutzverletzungen

Artikel 4 Nummer 12 DSGVO definiert eine Verletzung des Schutzes personenbezogener Daten (auch als Datenschutzverletzung bezeichnet) als eine Verletzung der Sicherheit der Verarbeitung, die zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von personenbezogenen Daten bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Dies gilt unabhängig davon, ob es unbeabsichtigt oder unrechtmäßig zu einer Datenschutzverletzung kommt. Zudem bezieht sich dies nicht nur auf besonders schutzbedürftige Daten im Sinne von Artikel 9 DSGVO, sondern auf alle personenbezogenen Daten.

Datenschutzverletzungen lassen sich nach den drei bekannten Grundsätzen der Informationssicherheit in folgende Formen unterteilen:

- Verletzung der Vertraulichkeit: die unbefugte oder unbeabsichtigte Preisgabe von oder Einsichtnahme in personenbezogene Daten,

- Verletzung der Integrität: die unbefugte oder unbeabsichtigte Änderung personenbezogener Daten,
- Verletzung der Verfügbarkeit: der unbefugte oder unbeabsichtigte Verlust des Zugangs zu personenbezogenen Daten oder die unbeabsichtigte oder unrechtmäßige Vernichtung personenbezogener Daten.

Beispiele für die Formen von Datenschutzverletzungen:
Verletzung der Vertraulichkeit: E-Mails an mehrere Empfänger werden mittels eines offenen Verteilers verschickt, die Empfänger werden also nicht in die Empfangszeile „BCC“, sondern in die Zeile „CC“ gesetzt. Personenbezogenen Daten werden durch eine fehlende Kontrolle der E-Mail-Adressaten an die E-Mail-Adresse eines unbefugten Dritten geschickt.

Verletzung der Integrität: Für eine Software, in denen Datenbestände geführt werden, werden für jede einzelne Nutzerin und jeden einzelnen Nutzer Kennungen mit Passwörtern vergeben. Eine Nutzerin oder ein Nutzer gibt die Kennungen und das Passwort an eine andere Person weiter, die im Datenbestand unbefugt personenbezogene Daten ändert.

Verletzung der Verfügbarkeit: Es werden Daten unbeabsichtigt oder durch eine unbefugte Person gelöscht, oder im Falle sicher verschlüsselter Daten geht der Entschlüsselungsschlüssel verloren. Kann der Verantwortliche den Zugang zu den Daten etwa mit Hilfe einer Sicherungskopie nicht wiederherstellen, wird man in der Regel von einem Verlust des Zugangs und damit von einer Verletzung der Verfügbarkeit ausgehen müssen.

Eine Datenschutzverletzung kann sowohl alle drei oder zwei gleichzeitig, als auch nur einzelne dieser Formen betreffen. Es liegt im Übrigen auch dann eine Form der Datenschutzverletzung vor, wenn diese nur vorübergehend und nicht dauerhaft ist. Bei einer vorübergehenden Datenschutzverletzung ist eine Meldung an die Aufsichtsbehörde oder Benachrichtigung der betroffenen Personen nicht erforderlich, soweit durch diese vorübergehende Datenschutzverletzung keine weiteren Rechte und Freiheiten der betroffenen Personen gefährdet werden oder werden könnten.

Beispiel für eine nicht dauerhafte Datenschutzverletzung:
Ein kurzfristiger Stromausfall führt dazu, dass personenbezogene Daten für einen kurzen Zeitraum nicht zur Verfügung stehen.

12.2 Meldung an die Aufsichtsbehörde (Artikel 33 DSGVO)

Verletzungen des Schutzes personenbezogener Daten müssen gemäß Artikel 33 Absatz 1 DSGVO unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden des Vorfalls an die zuständige Aufsichtsbehörde gemeldet werden. Die Meldung hat auch dann zu erfolgen, wenn der Verantwortliche die Verletzung nicht selbst verschuldet hat. Ausschlaggebend für die Meldung und den Beginn der Frist von 72 Stunden ist das Bekanntwerden des Vorfalls. Die DSGVO verpflichtet den Verantwortlichen zur Meldung, nicht hingegen die oder den bDSB.

Wenn die Datenschutzverletzung voraussichtlich kein Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person zur Folge hat, muss die Verletzung jedoch nicht an die Aufsichtsbehörde gemeldet werden. Hingegen begründet jedes nicht auszuschließende Risiko eine Meldepflicht. Der Verantwortliche

hat daher nach Kenntnis der Datenschutzverletzung diese nicht nur zu beheben oder einzudämmen, sondern innerhalb der zeitlichen Meldefrist von 72 Stunden eine Risikobewertung anhand der spezifischen Umstände der Datenschutzverletzung vorzunehmen (siehe Ziffer 12.4). Möglicherweise wurde im Rahmen einer bereits durchgeführten Datenschutz-Folgenabschätzung eine erste allgemeine Einschätzung möglicher Risiken vorgenommen, die gegebenenfalls als erste Grundlage dienen kann.

Beispiel für eine Datenschutzverletzung, die in der Regel keine Meldung erfordert:
Eine öffentliche Stelle wird Opfer eines Ransomware-Angriffs, bei dem sämtliche Daten verschlüsselt werden. Es ist jedoch eine Sicherungskopie vorhanden und es sind nachweislich keine Daten in Folge des Ransomware-Angriffs abgeflossen bzw. im Zuge des Angriffs an unbefugte Dritte übermittelt worden.

Der Inhalt der Meldung richtet sich nach Artikel 33 Absatz 3 DSGVO. Es sind mindestens folgende Informationen zu übermitteln:

- eine Beschreibung der Art der Datenschutzverletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien der Daten und der ungefähren Zahl der betroffenen personenbezogenen Datensätze,
- den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung,
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Gemäß Artikel 33 Absatz 4 DSGVO können diese Informationen schrittweise zur Verfügung gestellt werden, wenn es nicht möglich ist, alle Informationen zur gleichen Zeit bereitzustellen. Die DSGVO trägt somit der Tatsache Rechnung, dass einem Verantwortlichen nicht immer binnen 72 Stunden alle erforderlichen Informationen vorliegen. Bei komplexen Datenschutzverletzungen wird der Verantwortliche daher auch weitere Untersuchungen durchführen und zu einem späteren Zeitpunkt zusätzliche Informationen nachreichen müssen. Eine solche Verzögerung muss jedoch gemäß Artikel 33 Absatz 1 DSGVO gegenüber der Aufsichtsbehörde begründet und daher entsprechend dokumentiert werden.

12.3 Benachrichtigung von betroffenen Personen (Artikel 34 DSGVO)

Besteht die Wahrscheinlichkeit, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen zur Folge hat, müssen neben der zuständigen Aufsichtsbehörde auch die betroffenen Personen informiert werden. Für die Benachrichtigung an die betroffenen Personen besteht demnach eine höhere Schwelle (ein voraussichtlich hohes Risiko) als für die Meldung an die Aufsichtsbehörde (ein „normales“ bzw. „einfaches“ Risiko). Der Verantwortliche hat die betroffenen Personen unverzüglich über die Datenschutzverletzung zu informieren.

Beispiel für eine Datenschutzverletzung, die in der Regel eine Benachrichtigung erfordert:
Eine öffentliche Stelle wird Opfer eines Ransomware-Angriffs, bei dem sämtliche Daten verschlüsselt werden. Es sind keine Sicherungskopien vorhanden und die Daten können nicht wiederhergestellt werden.

Eine Benachrichtigung der betroffenen Personen ist in folgenden Fällen gemäß Artikel 34 Absatz 3 DSGVO nicht erforderlich:

- Es wurden präventiv geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen auf die Datenschutzverletzung angewandt. Dazu gehören insbesondere Maßnahmen, die eine Kenntnisnahme der personenbezogenen Daten durch Dritte verhindern, etwa durch Verschlüsselung.
- Es wurde durch Maßnahmen, die nach der Kenntnis der Datenschutzverletzung ergriffen wurden, sichergestellt, dass mit aller Wahrscheinlichkeit nach kein hohes Risiko mehr für die Rechte und Freiheiten der betroffenen Personen besteht.
- Die Benachrichtigung der betroffenen Personen wäre mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall ist stattdessen in einer öffentlichen Bekanntmachung oder in ähnlicher Weise vergleichbar wirksam über die Datenschutzverletzung zu informieren. Dies könnte beispielsweise durch eine Veröffentlichung im Amtsblatt, in einer Tageszeitung oder in Online-Medien erfolgen.

Verzichtet der Verantwortliche auf eine Benachrichtigung, weil er zu der Einschätzung gelangt, dass die Datenschutzverletzung voraussichtlich zu keinem hohen Risiko führt oder eine der oben genannten Ausnahmen greift, sollte dies entsprechend dokumentiert werden. Unabhängig davon kann die Aufsichtsbehörde den Verantwortlichen dazu auffordern, eine nicht erfolgte Benachrichtigung nachzuholen, sofern die Aufsichtsbehörde der Auffassung ist, dass die Datenschutzverletzung voraussichtlich ein hohes Risiko zur Folge hat (Artikel 34 Absatz 4 DSGVO).

Der Inhalt der Meldung richtet sich nach Artikel 34 Absatz 2 in Verbindung mit Artikel 33 Absatz 3 Buchstabe b, c und d DSGVO. Die Verantwortlichen können sich zur Benachrichtigung und insbesondere auch zu den Inhalten von der zuständigen Aufsichtsbehörde beraten lassen (siehe Erwägungsgrund 86 DSGVO). Es sind mindestens die folgenden Informationen an die betroffenen Personen zu übermitteln:

- eine Beschreibung der Art der Datenschutzverletzung in klarer und einfacher Sprache,
- der Name und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle,
- eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung,
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

12.4 Risikobewertung und Dokumentationspflicht

Als Risiken für die Rechte und Freiheiten sind gemäß Erwägungsgründen 75 und 85 DSGVO alle drohenden physischen, materiellen oder immateriellen Schäden zu berücksichtigen. Gemäß Erwägungsgrund 76 DSGVO ist ein solches Risiko anhand einer objektiven Bewertung unter Berücksichtigung der Eintrittswahrscheinlichkeit und Schwere der Auswirkungen zu beurteilen. Laut den Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten der Artikel-29-Gruppe (WP 250 Rev.01), die vom EDSA bestätigt wurden, sind bei der Risikobewertung insbesondere die folgenden Faktoren zu berücksichtigen:

- Art der Datenschutzverletzung,
- Art, Sensibilität und Umfang der personenbezogenen Daten,
- Identifizierbarkeit der betroffenen Personen,

- Schwere der Folgen für die betroffenen Personen,
- besondere Eigenschaften der betroffenen Personen (zum Beispiel Kinder),
- besondere Eigenschaften des Verantwortlichen
- sowie die Zahl der betroffenen Personen.

Ausführlichere Informationen dazu finden sich in den angesprochenen Leitlinien (WP 250 Rev.01, Seiten 26 ff.), die auf der Internetseite der DSK unter dem Link https://www.datenschutzkonferenz-online.de/edsa.html heruntergeladen werden können. Überdies finden sich in den Leitlinien weitere Hinweise zum Umgang mit Datenschutzverletzungen sowie im Anhang konkrete Beispiele für Verletzungen mit und ohne Melde- bzw. Benachrichtigungspflicht.

Unabhängig davon, ob aufgrund einer Datenschutzverletzung voraussichtlich ein Risiko und demzufolge eine Meldepflicht besteht oder nicht, muss der Verantwortliche alle Datenschutzverletzungen gemäß Artikel 33 Absatz 5 DSGVO dokumentieren. Beispielsweise kann für die öffentliche Stelle ein internes Verzeichnis für Datenschutzverletzungen angelegt werden. Dokumentiert werden sollten die Details zur Datenschutzverletzung wie etwa die genauen Vorkommnisse, Ursachen, Kategorien der betroffenen Personen und der personenbezogenen Datensätze. Weiterhin sind die Risikobewertung und deren Ergebnisse einschließlich der wahrscheinlichen Auswirkungen auf die betroffenen Personen sowie die ergriffenen Abhilfemaßnahmen zu beschreiben. Werden die Aufsichtsbehörde und die betroffenen Personen über eine Datenschutzverletzung informiert, sollten auch die entsprechenden Meldungen nach Artikel 33 DSGVO bzw. die Benachrichtigungen nach Artikel 34 DSGVO dokumentiert werden. Wurde ein Vorfall nicht an die Aufsichtsbehörde gemeldet, weil der Verantwortliche anhand einer objektiven Beurteilung zu dem Ergebnis gekommen ist, dass voraussichtlich kein Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen besteht, sollte in der Dokumentation begründet werden, warum eine Meldung nicht erfolgt ist. Gleiches gilt für den Fall, dass betroffenen Personen nicht im Sinne von Artikel 34 DSGVO benachrichtigt wurden: Hier ist insbesondere zu begründen, warum aus Sicht des Verantwortlichen eine oder mehrere der Ausnahmen von Artikel 34 Absatz 3 DSGVO greifen.

Aus diesen Gründen sollten öffentliche Stellen interne Vorkehrungen treffen, um eine Datenschutzverletzung erkennen, bewerten und beheben oder eindämmen zu können. Dafür eignet sich zum Beispiel ein Reaktionsplan mit Regelungen zu internen Meldewegen, zur Risikobewertung, zu Abhilfemaßnahmen und zu Dokumentationen. Dabei ist zu berücksichtigen, an wen intern gemeldet wird, wer für die Risikobewertung und Dokumentation zuständig ist und wer erforderliche Meldungen an die Aufsichtsbehörde erstattet und die betroffenen Personen benachrichtigt. Entsprechende Regelungen können im Datenschutzkonzept der öffentlichen Stelle getroffen werden (siehe auch Ziffer 14).

➔ **Handlungserfordernisse:**

- Interne Vorkehrungen treffen, um eine Datenschutzverletzung erkennen, bewerten und beheben oder eindämmen zu können.
- Interne Vorkehrungen treffen, um nach Bekanntwerden von Datenschutzverletzungen die Frist von 72 Stunden zur Meldung an die Aufsichtsbehörde einhalten zu können.

- Reaktionspläne schaffen, die interne Meldewege unter Beachtung des zeitlichen Rahmens, die Risikobewertung und Abhilfemaßnahmen, Meldung an die Aufsichtsbehörde und Benachrichtigung betroffener Personen, Dokumentationen und die entsprechenden Zuständigkeiten innerhalb der öffentlichen Stelle festlegen.

13 Datengeheimnis und Dienstanweisungen

Artikel 29 DSGVO sieht vor, dass Beschäftigte eines Verantwortlichen oder eines Auftragsverarbeiters, die Zugang zu personenbezogenen Daten haben, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten dürfen. Eine gesetzliche Regelung zur Wahrung des Datengeheimnisses, wie es zuvor in § 6 BbgDSG-alt geregelt war, sieht die DSGVO hingegen nicht vor. Ebenso besteht keine Verpflichtung, die für eine öffentliche Stelle tätigen Personen bei Aufnahme ihrer Tätigkeit auf die Einhaltung des Datengeheimnisses bzw. auf die Einhaltung der datenschutzrechtlichen Vorschriften zu verpflichten. Demensprechend ist die alte Regelung im BbgDSG zum Datengeheimnis entfallen.

Dennoch wird empfohlen, eine entsprechende Verpflichtung (zum Beispiel in einer Dienstanweisung oder im Einzelnen durch eine Verpflichtung bestimmter Personen) vorzunehmen, denn der Verantwortliche hat nach Artikel 24 DSGVO sicherzustellen, dass personenbezogene Daten in einer Weise verarbeitet werden, die ein angemessenes Sicherheitsniveau gewährleistet. Dies beinhaltet auch den Schutz gegen unberechtigte oder ungesetzliche Verarbeitung.

Darüber hinaus sollen angemessene technische und organisatorische Maßnahmen getroffen werden, die gegen Verlust, Zerstörung oder Beschädigung der Daten schützen sollen. Auch die Mitarbeitenden als diejenigen, die personenbezogene Daten verarbeiten, sind von diesen Maßnahmen betroffen. Die öffentliche Stelle muss deshalb sicherstellen, dass die Mitarbeitenden die Daten nicht unberechtigt oder gegen geltende Gesetze verarbeiten. Auch daraus lässt sich eine explizite Pflicht zur Verpflichtung auf das Datengeheimnis nicht ableiten. Sicher ist aber, dass die öffentliche Stelle im Rahmen eines „angemessenen Schutzniveaus“ dafür Sorge tragen muss, dass die Mitarbeitenden erkennen können, wann sie gegebenenfalls mit der Datenverarbeitung gegen Gesetze verstoßen bzw. unberechtigt Daten verarbeiten.

Darüber hinaus sieht Artikel 32 Absatz 4 DSGVO vor, dass der Verantwortliche oder der Auftragsverarbeiter Maßnahmen festlegen, die sicherstellen, dass die ihnen unterstellten Personen personenbezogene Daten nur auf Anweisung des Verantwortlichen verarbeiten. Solche Maßnahmen können beispielsweise konkrete Verhaltensvorgaben in Dienstanweisungen, die Einweisung der Mitarbeitenden zum Umgang mit personenbezogenen Daten an ihrem konkreten Arbeitsplatz oder Weisungen bezogen auf Einzelfälle sein.

Ergänzend wird zudem auf das Kurzpapier Nummer 19 der DSK zur Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO hingewiesen (aufrufbar unter https://www.datenschutzkonferenz-online.de/kurzpapiere.html).

→**Anlage 9** enthält ein Muster für eine schriftliche Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DSGVO und ein Merkblatt mit ausgewählten datenschutzrechtlichen Vorschriften, das gegebenenfalls durch behördenspezifische Regelungen zu ergänzen ist. Zudem bietet es

sich an, den Beschäftigten ein Merkblatt mit grundlegenden Informationen zum Datenschutz zur Verfügung zu stellen. Ein Muster für ein solches Merkblatt findet sich in →**Anlage 10**. Sofern in der Vergangenheit eine formelle Verpflichtung auf das Datengeheimnis erfolgt ist, ist eine „Nachverpflichtung" der Mitarbeitenden aufgrund der Geltung der DSGVO nicht erforderlich. Die verwendeten Formulare und Merkblätter sind jedoch für die künftige Verwendung entsprechend der DSGVO inhaltlich anzupassen.

➔ **Handlungserfordernisse:**

- Im Rahmen organisatorischer Maßnahmen ist zu entscheiden, ob und in welcher Weise die Beschäftigten zur Einhaltung der datenschutzrechtlichen Vorschriften verpflichtet und entsprechend belehrt werden.
- Gegebenenfalls bereits verwendete Vordrucke und Merkblätter sind an die DSGVO anzupassen.

14 Dokumentationspflichten und Datenschutzmanagement

Die DSGVO enthält eine Vielzahl von Dokumentationspflichten. Mit der Erfüllung dieser Pflichten wird gemäß Artikel 5 Absatz 2 DSGVO der Nachweis erbracht, dass die Grundsätze für die Verarbeitung personenbezogener Daten nach Artikel 5 Absatz 1 DSGVO eingehalten werden. Insbesondere sind hervorzuheben:

- Nachweis der erteilten Einwilligungen (Artikel 7 Absatz 1 DSGVO),
- Nachweis der Einhaltung der Betroffenenrechte (gemäß Artikel 12 ff. DSGVO),
- Nachweis der technischen und organisatorischen Maßnahmen (Artikel 24 Absatz 1, Artikel 32 DSGVO),
- Führung eines Verzeichnisses von Verarbeitungstätigkeiten (Artikel 30 DSGVO),
- Dokumentation von Datenschutzvorfällen (Artikel 33 Absatz 5 DSGVO),
- Durchführung des Freigabeverfahrens und Freigabeerklärung (gemäß § 4 BbgDSG),
- Durchführung der Datenschutz-Folgenabschätzung (gemäß Artikel 35 DSGVO) und
- Dokumentation der Verträge über Auftragsverarbeitungen (gemäß Artikel 28 DSGVO).

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. Wesentliche Bausteine und Regelungspunkte eines solchen Konzepts können sein:

- Ziel und Geltungsbereich,
- übergreifende Leitlinien zum Datenschutz und Grundsätze der Verarbeitung personenbezogener Daten,
- datenschutzrechtliche Zuständigkeiten in der öffentlichen Stelle (übergreifend und in Spezialfragen):
  - Festlegung des Fachbereichs (zum Beispiel Abteilung, Referat, Sachgebiet), welches für die Verarbeitung der Daten zuständig ist,
  - Zuständigkeit für die Bearbeitung von Beschwerden oder Auskunftsersuchen,
  - gegebenenfalls Festlegungen zur Auftragsverarbeitung,
  - frühzeitige Einbeziehung und Beteiligung der oder des bDSB bei der Einführung oder wesentlichen Änderung von Verfahren bzw. bereits zum Zeitpunkt der Verfahrensausschreibung,

- Aufgaben und Stellung der oder des bDSB ergänzend zu den Regelungen der DSGVO,
- Abläufe bzw. Verfahrenswege zur Gewährleistung datenschutzrechtlicher Verpflichtungen:
  - Verzeichnis von Verarbeitungstätigkeiten (Zuständigkeiten und beteiligte Stellen, Erstellung, Führung, Überarbeitungen/Aktualisierungen, Informationsaustausch zwischen den beteiligten Stellen)
  - Datenschutz-Folgenabschätzung (Zuständigkeiten und beteiligte Stellen, Dokumentation, gegebenenfalls Erläuterungen zur Bestimmung des Schutzbedarfs bzw. zur Durchführung der Risikoanalyse),
  - Freigabeverfahren bei Einführung oder wesentlicher Änderung von Verfahren zur Verarbeitung personenbezogener Daten (Zuständigkeiten und beteiligte Stellen, Sicherheitskonzept, Beschreibung für das Verzeichnis von Verarbeitungstätigkeiten, Durchführung der Datenschutz-Folgenabschätzung, Freigabeerklärung, Dokumentation),
  - Umgang mit Datenschutzverletzungen (interne Meldung und Informationsaustausch unter Beachtung des zeitlichen Rahmens, Risikobewertung, Meldung an die Aufsichtsbehörde und betroffene Personen, Abhilfemaßnahmen, Dokumentation),
  - Gewährleistung der Betroffenenrechte (interne Meldung und Informationsaustausch, Zuständigkeiten und beteiligte Stellen, Dokumentation),
  - Vereinbarungen über Auftragsverarbeitungen (Zuständigkeiten und beteiligte Stellen, Dokumentation),
- Erläuterungen zur Risikoanalyse und zum Schutzbedarf sowie ein Verfahren, um den Schutzbedarf zu bestimmen,
- Maßnahmen für die Sicherheit der Verarbeitung, übergreifend und für spezielle Verarbeitungen bzw. Datenkategorien,
- organisatorische Richtlinien (wie zum Beispiel zum Backup von Daten bzw. zu Sicherungskopien, zum Virenschutz, zur Protokollierung oder Erstellung eines Löschkonzepts),
- Organisation und Durchführung von Datenschutz-Schulungen und
- Durchführung von regelmäßigen Datenschutz-Kontrollen und Audits.

➔ **Handlungserfordernis:**
Es ist ein auf die Bedürfnisse der öffentlichen Stelle angepasstes Datenschutzkonzept zu erstellen.

15 Handlungsempfehlungen

Empfehlungen	Anmerkungen
Prüfung der Zulässigkeit der Datenverarbeitungen	– Prüfung, ob das neue Recht für alle Prozesse eine Rechtsgrundlage bereitstellt – Prüfung von vorhandenen Einwilligungen zur Sicherstellung, dass diese gemäß DSGVO wirksam sind – Überprüfung von Dienstvereinbarungen, Satzungsrecht, Verwaltungsvorschriften und Geschäftsordnungen im Hinblick auf die Vereinbarkeit mit der DSGVO

Empfehlungen	Anmerkungen
Einführung eines Datenschutzmanagements insbesondere zur Erfüllung der Dokumentationspflichten	– Festlegung von Zuständigkeiten – Entwicklung eines Datenschutzkonzepts – Anpassung technischer und organisatorischer Maßnahmen an die Prinzipien der DSGVO, insbesondere Berücksichtigung der Prinzipien privacy bei design und privacy by default bereits im Zuge der vergaberechtskonformen Ausschreibung von IT-Produkten – Dokumentation der technischen und organisatorischen Maßnahmen (im Rahmen des Datenschutzkonzepts) – Etablierung eines Verfahrens zur regelmäßigen Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen – Vorkehrungen zur Erkennung, Bewertung und Behebung oder Eindämmung von Datenschutzverletzungen – Schaffung von Reaktions- und Ablaufplänen zum Umgang mit Datenschutzverletzungen (im Rahmen des Datenschutzkonzepts)
Organisatorische Maßnahmen zu Betroffenenrechten festlegen	– Festlegungen von Zuständigkeiten – Bearbeitung der Anliegen von Betroffenen unter Beachtung der Monatsfrist nach DSGVO – Festlegung der Art und Weise der Bearbeitung von Anliegen (Stichworte: Geheimhaltung, Vertraulichkeit) – Benennung von Ansprechpartnern für verschiedene Datenverarbeitungssysteme (um beispielsweise den Auskunftsanspruch überall in der öffentlichen Stelle gewährleisten zu können) – Festlegungen zur Umsetzung der Informationspflichten nach Artikel 13 und 14 DSGVO (zum Beispiel durch Aushänge, Standard-Texte in E-Mail-Signaturen und Veröffentlichungen auf der Internetseite)
Einführung oder Anpassung von Verfahren zur - **Führung eines Verzeichnisses von Verarbeitungstätigkeiten** - **Durchführung des Freigabeverfahrens** - **Durchführung der Datenschutz-Folgenabschätzung**	– Anpassung eventuell noch bestehender Verfahrensverzeichnisse an Artikel 30 DSGVO – Prüfung, ob für alle Verarbeitungen eine Beschreibung bzw. ein Eintrag im Verzeichnis von Verarbeitungstätigkeiten vorliegt – Berücksichtigung der an die DSGVO angepassten Inhalte des Freigabeverfahrens und der Freigabeerklärung (gemäß § 4 BbgDSG) – Ablösung der Vorabkontrolle gemäß § 10a BbgDSG-alt durch die Datenschutz-Folgenabschätzung nach Artikel

Empfehlungen	Anmerkungen
	35 DSGVO, die eine umfangreiche Dokumentation erfordert – bis spätestens Mai 2021: Überprüfung der Verarbeitungen, die nach altem Recht einer Vorabkontrolle unterlagen, unter Berücksichtigung des Artikel 35 DSGVO
Bestellung bDSB und Anpassungen des Aufgabenbereichs	– bei bereits bestellten bDSB: gegebenenfalls Überprüfung der Qualifikation und Unabhängigkeit, Beachtung neuer Aufgaben und Verantwortlichkeiten – Regelungen treffen, sofern weitere Aufgaben auf die bDSB übertragen werden sollen – Prüfung, ob angesichts der geänderten bzw. erweiterten Aufgaben die Ressourcen der bDSB ausreichend sind – Veröffentlichung der Kontaktdaten und Mitteilung an die LDA (Artikel 37 Absatz 7 DSGVO)
Beschäftigte gegebenenfalls zur Geheimhaltung verpflichten	– Festlegung, ob und wie Beschäftigte im Rahmen organisatorischer Maßnahmen zur Einhaltung des Datenschutzes verpflichtet und belehrt werden – gegebenenfalls Anpassung bereits verwendete Vordrucke und Merkblätter an die DSGVO
Prüfung und Abschluss von Vereinbarungen bei gemeinsam Verantwortlichen	– Überprüfung bestehender Kooperationen im Hinblick auf eine gemeinsame Verantwortung und gegebenenfalls Abschluss einer Vereinbarung nach Artikel 26 DSGVO – Überprüfung der entsprechenden Rechtsgrundlagen und bestehender Vereinbarungen im Hinblick auf die Anforderungen gemäß Artikel 26 DSGVO – Dokumentation der Vereinbarung nach Artikel 26 DSGVO und weiterer erforderlicher Dokumente (zum Beispiel zur Datenschutz-Folgenabschätzung, Freigabeerklärung und Beschreibung für das Verarbeitungsverzeichnis)
Anpassung von Verträgen über Auftragsverarbeitungen	– Überprüfung der bestehenden Verträge – Dokumentation der Verträge

16 Weitere Informationen und weiterführende Links

Internetauftritt des Europäischen Datenschutzausschusses:
https://edpb.europa.eu/edpb_de

Internetauftritt der Datenschutzkonferenz des Bundes und der Länder:
https://www.datenschutzkonferenz-online.de

Internetauftritt der Landesbeauftragten für den Datenschutz und das Recht auf Akteneinsicht:
https://www.lda.brandenburg.de

Infothek des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit:
https://www.bfdi.bund.de/DE/Infothek/Informationsmaterial/informationsmaterial-node.html
(hier können u.a. die Texte zur DSGVO mit Erläuterung kostenfrei als Druckexemplar bestellt oder als PDF heruntergeladen werden)

Antworten des Bundesministeriums des Innern, für Bau und Heimat auf häufig gestellte Fragen zur DSGVO:
https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/it-digitalpolitik/datenschutz/datenschutzgrundvo-liste.html

Arbeitshilfen des Bayerischen Staatsministeriums des Innern, für Sport und für Integration:
http://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen/index.php

Praxishilfen der Stiftung Datenschutz:
https://stiftungdatenschutz.org/dsgvo-info/praxishilfen/