Anwendungshinweise des Ministeriums des Innern und für Kommunales des Landes Brandenburg vom 9. Mai 2018 in Bezug auf die Geltung der EU-Datenschutz-Grundverordnung und Inkrafttreten des Brandenburgischen Datenschutzgesetzes am 25. Mai 2018

1. Vorwort

Ab dem 25. Mai 2018 ist die von der Europäischen Union erlassene Datenschutz-Grundverordnung (DSGVO) für die öffentlichen Stellen des Landes Brandenburg unmittelbar anzuwenden. Nahezu zum gleichen Zeitpunkt (6. Mai 2018) ist 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 ist an die beiden Rechtakte der EU anzupassen. Der Bund hat bereits 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-neu) sowie das Gesetz zur Anpassung des bereichsspezifischen Rechts an die Verordnung (EU) 2016/679 am 25. April 2018 verabschiedet. Sie wurden am 08. Mai 2018 im Gesetz- und Verordnungsblatt für das Land Brandenburg verkündet (GVBI. 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 treten gemeinsam mit dem Wirksamwerden der DSGVO am 25. Mai 2018 in Kraft.

Dies führt ab dem 25. Mai 2018 zu einer neuen Struktur des Datenschutzrechts:
Ergänzend zur DSGVO als direkt anwendbares Recht haben die öffentlichen Stellen Brandenburgs künftig das neu gefasste Brandenburgische Datenschutzgesetz und – je nach Verwaltungsbereich – weiterhin auch bereichsspezifische datenschutzrechtliche Vorschriften zu beachten. Wegen der Strukturveränderungen bleiben im BbgDSG nur wenige materielle Kernelemente wie z.B. die Zulässigkeit der Datenverarbeitung zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgaben (§ 5 BbgDSG-neu) oder zur Zweckbindung (§ 6 BbgDSG-neu) 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 zukünftig 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 dem behördlichen Datenschutzbeauftragten eine beratende 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 Pro-

zesse 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.

Ergänzend zu den in diesen Hinweisen enthaltenen Informationen wird auf die Veröffentlichungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hingewiesen, die unter dem folgenden Link abgerufen werden können:
http://www.lda.brandenburg.de/sixcms/detail.php/bb1.c.523474.de

2. Einführung

2.1 Die Datenschutzreform der Europäischen Union

Ab 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 ab 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 bereits ein neues Bundesdatenschutzgesetz (BDSG 2018) und weitere Änderungen datenschutzrechtlicher Vorschriften verabschiedet, z.B. 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 in Planung. In Brandenburg werden die oben angesprochenen Anpassungsgesetze am 25. Mai 2018 in Kraft treten. Im bereichsspezifischen Recht werden weitere Rechtsänderungen auf Gesetz- und Verordnungsebene folgen.

Neben der DSGVO ist die Richtlinie zum Datenschutz bei Polizei und Justiz (Richtlinie (EU) 2016/680) von den Mitgliedstaaten der Europäischen Union in nationales Recht umzusetzen. Anders als die DSGVO ist diese Richtlinie nicht unmittelbar anwendbar, sondern muss zuvor vom Gesetzgeber in Bundes- bzw. Landesrecht umgesetzt werden. Die Umsetzung erfolgt in Brandenburg durch die entsprechende Anwendung der DSGVO, soweit nicht bereichsspezifische Regelungen vorgehen (§ 2 Abs. 6 BbgDSG-neu).

2.2 Der Anwendungsbereich der DSGVO

Der sachliche Anwendungsbereich der DSGVO ist in Art. 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 Art. 4 Nr. 6 DSGVO definiert. Darunter ist jede strukturierte Samm-

lung personenbezogener Daten zu verstehen, die nach bestimmten Kriterien zugänglich ist. In der Kommentarliteratur werden dabei überwiegend zwei Zuordnungskriterien wie z. B. 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 (vgl. Erwägungsgrund 15 DSGVO).

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

- Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen (z. B. Tätigkeit der Abgeordneten im Landtag, Tätigkeit des Landesamtes für Verfassungsschutz),
- 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 (Richtlinie (EU) 2016/680).

2.3 Der Anwendungsvorrang der DSGVO

Da - wie oben bereits dargelegt - die DSGVO unmittelbar, also ohne weiteren Umsetzungsakt gilt, ist sie künftig 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 z. B. die Vorschriften zur Verarbeitung personenbezogener Daten im Landesbeamtengesetz oder im Schulgesetz bleiben grundsätzlich erhalten, wurden aber soweit notwendig an die Vorgaben der DSGVO angepasst.

Was heißt das aber nun konkret für die künftige Rechtsanwendung? Hier einige Antworten:

- Das Verständnis datenschutzrechtlicher Begriffe ergibt sich ausschließlich aus den Definitionen der DSGVO (vgl. Art. 4 DSGVO, Erwägungsgründe 26 – 37 DSGVO).
- Die Pflichten, die den öffentlichen Stellen als Verantwortliche (näheres unten unter Ziffer 3) für die Verarbeitung personenbezogener Daten obliegen, sind in der DSGVO verankert (vgl. insbesondere Art. 5, 24 ff., 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, wird künftig Art. 6 Abs. 1 DSGVO sein. Wie sich die Prüfungsreihenfolge im Zusammenspiel mit nationalen spezialgesetzlichen Regelungen gestaltet, wird unter Ziffer 5 dargestellt.
- Soweit die Verarbeitung auf einer Einwilligung der betroffenen Person beruht, ergeben sich die Bedingungen für die Einwilligung aus der DSGVO (vgl. Art. 7 und 8 DSGVO). Als Rechtsgrundlage für die Verarbeitung durch eine Behörde kommt die Einwilligung in aller Regel nicht in Betracht (vgl. Erwägungsgründe 43 und 45 der DSGVO).

- Die DSGVO schreibt für öffentliche Stellen zwingend vor, dass ein Datenschutzbeauftragter zu benennen ist und welche Aufgaben dieser hat (vgl. Art. 37 ff. DSGVO).
- Aufgaben und Befugnisse der Aufsichtsbehörde ergeben sich unmittelbar aus der DSGVO (vgl. Art. 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 Brandenburgische Datenschutzgesetz 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. Dies betrifft beispielsweise die Datenverarbeitung durch den Verfassungsschutz oder auch die Datenverarbeitung durch die Polizei und Justiz, soweit keine speziellen Regelungen getroffen wurden. Ebenso unterfällt die Datenverarbeitung in unstrukturierten Akten der DSGVO. Davon ausgenommen sind jedoch Art. 30, 35 und 36 DSGVO, die auf die Verarbeitung personenbezogener Daten in unstrukturierten Akten nicht sinnvoll anwendbar sind und deren Geltung daher auf diese nicht automatisierte Verarbeitung gemäß § 2 Abs. 6 Satz 2 BbgDSG-neu insgesamt ausgeschlossen ist.
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 Art. 8 der EU-Grundrechte-Charta auch das vom Bundesverfassungsgericht entwickelte Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gewährleistet.

Inhaltlich enthält das Gesetz folgende Regelungsschwerpunkte:
- Beibehaltung des Freigabeverfahrens für automatisierte Datenverarbeitungen (§ 4 BbgDSG-neu).
- Beibehaltung einer Auffangnorm, die die Verarbeitung personenbezogener Daten zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgaben erlaubt (§ 5 BbgDSG-neu).
- Definition der Voraussetzungen, unter denen personenbezogene Daten zu anderen als den ursprünglichen Erhebungszwecken verarbeitet werden dürfen (§ 6 BbgDSG-neu).
- Es werden Regelungen getroffen, unter welchen Voraussetzungen die Rechte der betroffenen Personen auf Auskunft und Löschung sowie die Pflichten der verantwortlichen Stelle zur Information der betroffenen Person beschränkt werden können (§§ 10 – 13 BbgDSG-neu).
- Unter weitgehender Beibehaltung der bisherigen Rechtslage werden Regelungen zu besonderen Verarbeitungssituationen getroffen (Abschnitt 5 des BbgDSG-neu).
- In Abschnitt 4 des BbgDSG-neu erfolgen Regelungen, die die Anforderungen der DSGVO an die Tätigkeit und Unabhängigkeit der Aufsichtsbehörden umsetzen.

Als Anlage 2 ist eine Übersicht beigefügt, die die bisherigen Regelungen des BbgDSG den neuen Rechtsvorschriften (DSGVO und BbgDSG-neu) 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 und gehen teilweise über die bisher bekannten Definitionen hinaus. Die Zulässigkeit der Verarbeitung personenbezogener Daten beurteilt sich aus einem Zusammenspiel von DSGVO, bereichsspezifischem Recht und dem neuen Brandenburgischen Datenschutzgesetz. Die DSGVO enthält teilweise neue bzw. gegenüber dem bisherigen Stand modifizierende verfahrensrechtliche Vorgaben und Dokumentationspflichten. Dem (behördlichen) Datenschutzbeauftragten werden konkrete Aufgaben zugewiesen und seine Rolle als Berater des Verantwortlichen klargestellt. In Bezug auf den technischen Datenschutz sind die neuen Vorgaben in Bezug auf „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ gemäß Art. 25 DSGVO zu beachten. Die Betroffenenrechte sind erheblich gestärkt und um Informationspflichten bei der Datenerhebung und Zweckänderung ergänzt worden.
Der Aufsichtsbehörde werden neue Befugnisse übertragen, die bis hin zur Untersagung von Verarbeitungen reichen können.

3. Rolle des Verantwortlichen nach der DSGVO

Die DSGVO weist dem „Verantwortlichen“ bei der Verarbeitung personenbezogener Daten eine zentrale Rolle zu. „Verantwortlicher“ ist nach Art. 4 Nr. 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 Abs. 1 BbgDSG-neu, also wie bisher z.B. 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 Art. 5, 6 und 9 DSGVO, in den §§ 5 und 6 BbgDSG-neu und in fachgesetzlichen Datenschutzvorschriften geregelt,
- die Verfahrensvorschriften der DSGVO beachtet werden. Dies gilt z.B. für die Führung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DSGVO, die Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO und die Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO,
- die datenschutzrechtlichen Informationspflichten nach Art. 13 und 14 DSGVO i.V.m. § 6 Abs. 2 und § 10 BbgDSG-neu und die sonstigen Rechte der Betroffenen beachtet werden (z.B. das Auskunftsrecht nach Art. 15 DSGVO i.V.m. § 11 BbgDSG-neu, das Recht auf Löschung nach Art. 17 DSGVO und das Widerspruchsrecht nach Art. 21 DSGVO),

- geeignete technische und organisatorische Maßnahmen zum Schutz der verarbeiteten Daten und zur Befolgung des Ziels Datenschutz durch Technikgestaltung getroffen werden (Art. 24 Abs. 1, 25 und Art. 32 DSGVO) und
- geeignete sonstige Datenschutzvorkehrungen getroffen werden (z.B. Datenschutzrichtlinien oder sonstige Datenschutzanweisungen nach Art. 24 Abs. 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.

Handlungserfordernisse:

- Festlegung von Zuständigkeiten und Umsetzung der erforderlichen Maßnahmen (siehe Ziffer 14)

4. Begriffe

Die Begriffsbestimmungen ergeben sich zukünftig unmittelbar aus Art. 4 DSGVO. Lediglich in Bezug auf das Anonymisieren enthält § 3 BbgDSG eine ergänzende Begriffsbestimmung.
Gegenüber den bisher im BbgDSG verwendeten Begriffen ergeben sich u.a. aus Art. 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“

5. Zulässigkeit der Verarbeitung personenbezogener Daten

Wie bisher gilt hinsichtlich der Zulässigkeit der Verarbeitung personenbezogener Daten das Prinzip des Verbots mit Erlaubnisvorbehalt. Zentrale Vorschrift ist Art. 6 DSGVO:

Art. 6 Abs. 1 DSGVO definiert dabei als Erlaubnistatbestände

a) die Einwilligung (siehe auch Art. 7 und 8 DSGVO) oder

die Erforderlichkeit der Datenverarbeitung:

b) für die Erfüllung eines Vertrages
c) zur Erfüllung einer rechtlichen Verpflichtung (i.V.m. Art. 6 Abs. 2 u. 3 DSGVO – Erfordernis einer EU-Norm oder nationalen Rechtsvorschrift!)
d) zur Wahrung lebenswichtiger Interessen
e) für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt (i.V.m. Art. 6 Abs. 2 u. 3 DSGVO – Erfordernis einer EU-Norm oder nationalen Rechtsvorschrift!)

f) zur Wahrung berechtigter Interessen des Verantwortlichen (eingeschränkt im öffentlichen Bereich)

Dabei gelten die Erlaubnistatbestände von Art. 6 Abs. 1 Buchst. a, b, d und f DSGVO unmittelbar. Eine Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung (Buchst. c) oder zur Wahrnehmung einer öffentlichen Aufgaben (Buchst. 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 ggf. anzupassen. Entsprechende Hinweise sind als Anlage 3 beigefügt.

Erteilte Einwilligungen wirken nach Erwägungsgrund 171 DSGVO fort. Sofern sie die Grundlage für eine Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 Buchst. a DSGVO sein sollen, gilt dies jedoch nur, sofern sie auch der Art nach und inhaltlich den Bedingungen der DSGVO entsprechen. Sofern dies nicht der Fall ist, können sie nicht als Einwilligung im Sinne des Art. 6 Abs. 1 Buchst. a DSGVO i. V. m. Art. 7 und 8 DSGVO angesehen und eine künftige Verarbeitung nicht auf sie gestützt werden.

Art. 6 Abs. 4 DSGVO enthält Vorschriften über zulässige Zweckänderungen, die durch § 6 BbgDSG-neu umgesetzt bzw. ergänzt werden.
Hinsichtlich der Verarbeitung besonderer Datenkategorien enthält Art. 9 DSGVO spezifische Anforderungen.

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-neu (§§ 5, 6 oder 25 bis 31 BbgDSG-neu) eine Erlaubnisnorm zur Verfügung?
3. Kann die Datenverarbeitung auf Art. 6 Abs. 1 Buchst. a, b, d oder f DSGVO gestützt werden? Dabei ist zu beachten, dass öffentliche Stellen die Datenverarbeitung im Zusammenhang mit der Erfüllung ihrer zugewiesenen Aufgaben i.d.R. nicht auf Art. 6 Abs. 1 Buchst. 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-, sei es im Bundesrecht) im Zusammenhang zu lesen und anzuwenden sein.

<u>Handlungserfordernisse:</u>

- Prüfen, ob das neue Recht für alle Prozesse eine Rechtsgrundlage bereitstellt.

- Vorhandene Einwilligungen prüfen, um sicherzustellen, dass sie nach Wirksamwerden der DSGVO fortgelten.
- Überprüfen von Dienstvereinbarungen, Satzungsrecht, Verwaltungsvorschriften und Geschäftsordnungen im Hinblick auf die Vereinbarkeit mit der DSGVO.

6. Verfahrensänderungen

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

6.1 Verarbeitungsverzeichnis

Das bisherige Verfahrensverzeichnis nach § 8 BbgDSG wird durch das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO abgelöst. Anders als nach bisherigem Recht ist ein Verarbeitungsverzeichnis unabhängig davon zu führen, ob die Verarbeitung automatisiert erfolgt oder nicht. Das heißt, auch soweit personenbezogene Daten in (strukturierten) Papierakten (siehe oben zum Anwendungsbereich) verarbeitet werden, ist ein Verarbeitungsverzeichnis zu führen. Darüber hinaus gelten die bisher in § 8 Abs. 5 BbgDSG geregelten Ausnahmen für das Verfahrensverzeichnis nicht mehr, so dass auch für diese Verarbeitungen ein Verarbeitungsverzeichnis zu erstellen ist.
Dieses Verzeichnis ist vom Verantwortlichen zu führen. Der Verantwortliche hat im Rahmen seiner Organisationshoheit zu bestimmen, wer die jeweiligen Verzeichnisse erstellt und wer diese führt. Die Erstellung sollte zweckmäßiger Weise durch den für die jeweilige Fachaufgabe verantwortlichen Bereich, ggf. unter Beteiligung der IT-Stelle erfolgen. Es ist empfehlenswert, wenn der Datenschutzbeauftragte zumindest eine Kopie der Verzeichnisse vorhält, um seine Aufgaben wahrnehmen zu können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zur Erstellung der Verzeichnisse Arbeitshilfen entwickelt, die als Anlage 4a beigefügt sind. Des Weiteren stellt die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg Muster für das Verzeichnis von Verarbeitungstätigkeiten zur Verfügung, die als Anlagen 4b und 4c beigefügt sind. Die Arbeitshilfen und Muster sind zudem unter dem Link http://www.lda.brandenburg.de/sixcms/detail.php/bb1.c.587757.de abrufbar.

Handlungserfordernisse:

- Anpassung der bestehenden Verfahrensverzeichnisse an Art. 30 DSGVO.
- Prüfung, ob für alle Verarbeitungen ein Verarbeitungsverzeichnis vorliegt.

6.2 Freigabe

Die datenschutzrechtliche Freigabe automatisierter Verfahren durch den Verantwortlichen wird beibehalten und ist in § 4 Abs. 1 BbgDSG-neu geregelt. Danach ist in den Fällen, in denen die Verarbeitung personenbezogener Daten mittels automatisierter Verfahren erfolgen soll, vor Beginn dieser Verarbeitung ein Freigabeverfahren durchzuführen. Zu beachten ist, dass § 4 Abs. 2 BbgDSG-neu bestimmte Verfahren von der Freigabepflicht ausnimmt. Gleichwohl ist auch für diese Verfahren, anders als nach bisherigem Recht, ein Verarbeitungsverzeichnis gemäß Art. 30 DSGVO zu erstellen.
Bislang erteilte Freigaben bleiben wirksam. Es empfiehlt sich, im Rahmen des Freigabeverfahrens dem behördlichen Datenschutzbeauftragten Gelegenheit zur Stellungnahme zu geben.

Handlungserfordernisse:

- Berücksichtigung der an die DSGVO angepassten Inhalte des Freigabeverfahrens und der Freigabeerklärung.

6.3 Datenschutz-Folgenabschätzung

Vor dem Einsatz „hochrisikoträchtiger" und eingriffsintensiver Verarbeitungen ist künftig eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen. Die Landesbeauftragte für den Datenschutz wird hierzu ergänzend eine – nicht abschließende – Liste von Verarbeitungen veröffentlichen, für die ein solches Verfahren durchzuführen ist. Für Datenverarbeitungen, die am 25. Mai 2018 bereits durchgeführt werden und die in die Kategorie „hochrisikoträchtiger" Verarbeitungen im Sinne des Art. 35 DSGVO einzustufen wären, ist keine Datenschutz-Folgenabschätzung durchzuführen, wenn eine Vorabkontrolle durch den behördlichen Datenschutzbeauftragten 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 (Art. 24 Abs. 1 Satz 2 DSGVO), so dass eine Art. 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 hat Leitlinien zur Datenschutz-Folgenabschätzung entwickelt (working paper 248 Rev. 1, siehe Anlage 5), die nähere Ausführungen zu diesem Verfahren enthalten.
Zuständig für die Durchführung der Folgenabschätzung ist der Verantwortliche. Dabei holt der Verantwortlich zwingend die Stellungnahme des Datenschutzbeauftragten ein (Art. 35 Abs. 2 DSGVO). Nicht DSGVO-konform wäre es, dem Datenschutzbeauftragten die Zuständigkeit für die Durchführung der Datenschutz-Folgeabschätzung zu übertragen.

Handlungserfordernisse:

- Die Vorabkontrolle durch den behördlichen Datenschutzbeauftragten gemäß § 10a BbgDSG wird durch die Datenschutz-Folgenabschätzung, die der Verantwortliche durchzuführen hat, nach Art. 35 DSGVO abgelöst und erfordert eine umfangreiche Dokumentation.
- Für Verarbeitungen, von denen hohe Risiken ausgehen, muss keine Folgenabschätzung vorgenommen werden, wenn sie der Vorabkontrolle durch den Datenschutzbeauftragten unterlegen haben und ohne wesentliche Änderung fortgeführt werden. Einer Überprüfung der Verarbeitungen innerhalb der nächsten 2-3 Jahre sind die Anforderungen von Art. 35 DSGVO zugrunde zu legen.

7. Der behördliche Datenschutzbeauftragte

Mit Anwendbarkeit der DSGVO am 25. Mai 2018 werden auch die Stellung und die Aufgaben des behördlichen Datenschutzbeauftragten neu geregelt (Art. 37 bis 39 DSGVO). Nach Art. 37 Abs. 1 Buchst. a DSGVO hat jede öffentliche Stelle einen Datenschutzbeauftragten zu benennen.
Der behördliche Datenschutzbeauftragte ist auf der Grundlage seiner beruflichen Qualifikation und insbesondere seines datenschutzrechtlichen Fachwissens zu benennen (Art. 37 Abs. 5 DSGVO). Dazu gehören Rechtskenntnisse bezüglich der einschlägigen datenschutzrechtlichen Regelungen sowie Grundkenntnisse der eingesetzten IuK-Technik.
Der behördliche Datenschutzbeauftragte ist frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden (Art. 38 Abs. 1 DSGVO). Er muss Zugang zum Verzeichnis

der Verarbeitungstätigkeiten nach Art. 30 DSGVO haben. Der behördliche Datenschutzbeauftragte ist berechtigt und verpflichtet, der Behördenleitung unmittelbar zu berichten (Art 38 Abs. 3 Satz 3 DSGVO).

Wesentliche Aufgaben des behördlichen Datenschutzbeauftragten gemäß Art. 39 Abs. 1 DSGVO sind insbesondere

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

Die Führung des Verzeichnisses der Verarbeitungstätigkeiten und die Durchführung der Datenschutz-Folgenabschätzung sind nach der DSGVO keine Pflichtaufgaben des behördlichen Datenschutzbeauftragten – anders als früher die Führung des Verfahrensverzeichnisses und die Durchführung der Vorabkontrolle.
Der Verantwortliche kann dem Datenschutzbeauftragten im Einklang mit der DSGVO weitere Aufgaben übertragen. Dies betrifft z.B. die Übertragung der Aufgabe, das Verarbeitungsverzeichnis zu führen oder die Vorgabe, dass vor jedem beabsichtigten Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden, die Stellungnahme des Datenschutzbeauftragten einzuholen ist. Aus Artikel 35 Abs. 1 Satz 1 und Abs. 2 DSGVO ergibt sich aber, dass die Durchführung der Datenschutz-Folgenabschätzung nicht auf den Datenschutzbeauftragten übertragen werden kann.
Dem Datenschutzbeauftragten sind die zur Erfüllung seiner Aufgaben erforderlichen Ressourcen zur Verfügung zu stellen (Art. 39 Abs. 2 DSGVO).

<u>Handlungserfordernisse:</u>

- Bereits bestellte Datenschutzbeauftragte bleiben in ihrer Funktion, ggf. Überprüfung der Qualifikation und Unabhängigkeit, neue Aufgaben und Verantwortlichkeiten beachten.
- Sollen weitere Aufgaben übertragen werden, ist dies durch den Verantwortlichen zu regeln.
- Prüfung, ob angesichts der geänderten bzw. erweiterten Aufgaben die Ressourcen des Datenschutzbeauftragten ausreichend sind.
- Veröffentlichung der Kontaktdaten und Mitteilung an die LDA (Art. 37 Abs. 7 DSGVO).

8. Befugnisse der Aufsichtsbehörde

Die LDA erhält als Aufsichtsbehörde verstärkte Befugnisse bis hin zur Untersagung einzelner Datenverarbeitungen (Art. 57 und 58 DSGVO). Anstelle des bisherigen Beanstandungsverfahrens teilt die LDA der zuständigen Fach- oder Rechtsaufsicht mit, wenn sie von ihren Befugnissen nach Art. 58 Abs. 2 DSGVO Gebrauch gemacht hat (§ 22 Satz 1 BbgDSG-neu). 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-neu).

Verletzungen des Schutzes personenbezogener Daten (Datenpannen), die voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen, sind künftig der LDA zu melden (Art. 33 DSGVO.
Geht von der Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen aus, sind auch die betroffenen Personen zu benachrichtigen (Art. 34 DSGVO).

9. Betroffenenrechte (Art. 12 – 22 DSGVO)

Die Rechte der betroffenen Personen sind von der DSGVO erheblich gestärkt worden. Dies gilt insbesondere für die Information der betroffenen Person bei einer Datenerhebung (z.B. mittels eines Formulars) und das Recht auf Datenportabilität.
Die §§ 10-13 BbgDSG-neu 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 (z.B. § 32c AO, § 82 und § 83 SGB X in der ab dem 25. Mai 2018 in Kraft tretenden Fassung).

Für Informationen und Mitteilungen an den Betroffenen im Zusammenhang mit Betroffenenrechten enthält Art. 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 (Art. 12 Abs. 1 DSGVO).

Art. 12 Abs. 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 Art. 12 Abs. 3 DSGVO, dass Anträge Betroffener nach Möglichkeit auf elektronischem Wege zu beantworten sind, wenn sie auf elektronischem Wege gestellt wurden.

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

Informationen über Datenerhebungen und Mitteilungen bzw. Maßnahmen auf Anträge, mit denen die betroffene Person ihre Rechte geltend macht, erfolgen wie bisher unentgeltlich (Art. 12 Abs. 5 DSGVO).

<u>Handlungserfordernisse:</u>

- Zur Erfüllung von Rechten der betroffenen Personen und von entsprechenden Pflichten der öffentlichen Stelle sind organisatorische Maßnahmen zu folgenden Fragen festzulegen:
    - Wer ist innerhalb der öffentlichen Stelle zuständig, wenn ein Betroffener seine Rechte geltend macht?

- In welcher Frist soll das Anliegen des Betroffenen weitergeleitet und bearbeitet werden (beachte: Monatsfrist nach DSGVO für die Antwort)?
- In welcher Form soll das Anliegen weitergeleitet werden (Stichwort: Geheimhaltung, Vertraulichkeit)?
- Wer sind die Ansprechpartner für verschiedene Datenverarbeitungssysteme (um beispielsweise den Auskunftsanspruch überall in der öffentlichen Stelle gewährleisten zu können)?

- Es sind Verfahren zu definieren, wie die Informationspflichten nach Art. 13 und 14 DSGVO erfüllt werden sollen. Für Standardverarbeitungen empfiehlt sich die Verwendung von Mustern (Näheres Ziffer 9.1).

9.1 Informationspflichten des Verantwortlichen nach Art. 13 und 14 DSGVO

Ein wesentliches Anliegen der DSGVO ist die Stärkung des Transparenzgrundsatzes (Art. 5 Abs. 1 Buchst. 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 Art. 13 und 14 DSGVO daher einen umfangreichen Katalog proaktiver Benachrichtigungen bei der Erhebung personenbezogener Daten vor.
In den Anlagen 6a und 6b finden sich Mustertexte mit Ausfüllhinweisen. Wesentliche Angaben zur Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO decken sich mit den Angaben im Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 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 (Art. 13 DSGVO);
- personenbezogene Daten nicht direkt bei der betroffenen Person erhoben werden, diese also z.B. aus öffentlichen Quellen oder von Dritten stammen (Art. 14 DSGVO);
- oder beabsichtigt wird, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den diese Daten erhoben oder erlangt wurden („Zweckänderung“, Art. 13 Abs. 3 bzw. Art. 14 Abs. 4 DSGVO).

Für alle der drei genannten Fälle wird folgendes Prüfschema vorgeschlagen:

1. Liegt ein Fall von Art. 13 oder Art. 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?

9.1.1 Informationspflicht bei einer Erhebung bei der betroffenen Person (Art. 13 DSGVO)

1. <u>Liegt ein Fall des Art. 13 DSGVO vor?</u>

Voraussetzung für die Informationspflicht nach Art. 13 DSGVO ist, dass der Verantwortliche die personenbezogenen Daten bei der betroffenen Person erhebt.

Eine Erhebung setzt voraus, dass der Verantwortliche die Daten selbst aktiv beschafft. Werden personenbezogene Daten von der betroffenen Person selbst (preis)gegeben, liegt keine Erhebung vor.

Beispiele für eine Erhebung bei der betroffenen Person:

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

Beispiele für nicht aktiv beschaffte Daten:

- Eine Person wendet sich mit einer Anfrage an die Behörde.
- Eine Person zeigt beispielsweise einen Schwarzbau an.
- Eine Person sendet initiativ Bewerbungsunterlagen per Post oder E-Mail an die öffentliche Stelle.

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

2. Gibt es Ausnahmen?

Ausnahmen finden sich in Art. 13 Abs. 4 DSGVO und § 10 BbgDSG-neu oder können sich aus Fachgesetzen ergeben.

Verfügt die betroffene Person bereits über die Informationen, besteht keine Informationspflicht für den Verantwortlichen (Art. 13 Abs. 4 DSGVO). In einem Verwaltungsverfahren ist es z. B. ausreichend, die betroffene Person zu Beginn des Verfahrens – in der Regel bei Antragseinreichung – zu informieren. Sollten sich im weiteren Verfahren Anfragen oder Rückfragen ergeben, die zu einer 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 und eine Wiederholung der Information nicht erforderlich ist (Beispiel: wiederholte Lebensmittelkontrollen im gleichen Betrieb).

Die Pflicht zur Information der betroffenen Person besteht des Weiteren nach § 10 Abs. 1 BbgDSG-neu 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 Abs. 1 BbgDSG-neu, so hat der Verantwortliche gemäß § 10 Abs. 2 BbgDSG-neu jedoch die Informationen nach Art. 13 DSGVO in allgemeiner Form für die Öffentlichkeit zur Verfügung zu stellen. Zudem hat der Verantwortliche festzuhalten, aus welchen Gründen von einer Information abgesehen wird.

Beispiel für einen Fall des § 10 Abs. 1 BbgDSG-neu:
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 Abs. 1 Nr. 1 BbgDSG-neu).
Entfällt die individuelle Mitteilung der Informationen nach Art. 13 DSGVO, sollte – aus Transparenzgründen und um dem Erfordernis des § 10 Abs. 2 BbgDSG-neu nachzukommen – eine allgemeine Information, die die nach Art. 13 DSGVO erforderlichen Angaben umfasst, für die Öffentlichkeit auf der Internetseite des Verantwortlichen bereitgestellt werden.

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

3. Zeitpunkt, Form und Inhalt der Information

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.

Bei Erhebungen durch Papierformulare können den betroffenen Personen die erforderlichen Informationen nach Art. 13 DSGVO auf dem jeweiligen Formular oder durch ein separates Begleitdokument mitgeteilt werden. Werden Formulare auf der Internetseite zum Download zur Verfügung gestellt, können die Informationen nach Art. 13 DSGVO in einem separaten Begleitdokument deutlich sichtbar auf der gleichen Seite zum Download zur Verfügung gestellt werden. In den Formularen wäre auf dieses Begleitdokument zudem hinzuweisen.

In den Fällen, in denen eine Person Daten auf einer Internetseite in vorgegebene Datenfelder eingibt, kann durch einen deutlich sichtbaren Link auf eine gesonderte Seite mit den Informationen nach Art. 13 DSGVO hingewiesen werden. Des Weiteren besteht die Möglichkeit, zusätzlich begleitende Sofortinformationen zu den Datenfeldern durch Pop-Up-Fenster oder Mouseover-Effekte mitzuteilen.
Insbesondere für die Veröffentlichung von Informationen auf Internetseiten ist zu beachten, dass für jede Verarbeitungstätigkeit einer öffentlichen Stelle spezifische Informationen bereitzustellen sind. Im Ergebnis werden auf der Internetseite einer öffentlichen Stelle damit viele unterschiedliche Hinweise mit Informationen nach Art. 13 DSGVO zum Abruf oder Download zur Verfügung stehen.

Auch bei der mündlichen Erhebung von personenbezogenen Daten (wie z. B. in persönlichen Gesprächen oder Telefonaten) besteht die Informationspflicht, wenn nicht eine der o. g. Ausnahmen greift. Gibt eine Person bspw. unaufgefordert personenbezogene Daten über sich Preis und werden (ggf. im weiteren Verlauf des Gesprächs) auch keine personenbezogenen Daten selbst aktiv beschafft, handelt es sich grundsätzlich nicht um eine Erhebung bzw. verfügt die betroffene Person aufgrund der Umstände ggf. bereits über die Information. In diesen Fällen besteht dem Grunde nach keine Informationspflicht nach Art. 13 DSGVO.
Werden personenbezogene Daten mündlich erhoben, wird empfohlen, die betroffene Person auf die Erhebung der Daten hinzuweisen und anzugeben, wo die Informationen nach Art. 13 DSGVO zur Verfügung gestellt werden (z. B. durch Aushänge vor Ort, auf der Internetseite). Des Weiteren können Informationsblätter vorgehalten, auf diese hingewiesen und auf Anfrage der betroffenen Person an diese ausgegeben werden. Sofern den Umständen nach angemessen, besteht z. B. bei der Erhebung von Daten im Rahmen von Telefongesprächen die Möglichkeit, der betroffenen Person während des Gesprächs kurz und bündig die Informationen nach Art. 13 DSGVO mündlich mitzuteilen.

Anlage 6a enthält einen Mustertext mit allen nach Art. 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 bestehende Formulare für Datenerhebungen sind an die neuen gesetzlichen Vorgaben anzupassen und zu ergänzen.

9.1.2 Informationspflicht bei der Erhebung nicht bei der betroffenen Person (Art. 14 DSGVO)

1. Liegt ein Fall des Art. 14 DSGVO vor?

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

Die öffentliche Stelle muss die Daten selbst aktiv beschaffen. Werden personenbezogene Daten von Dritten ohne Aufforderung an die öffentliche Stelle gegeben, liegt kein Fall des Art. 14 DSGVO vor.

Beispiele für eine Erhebung nicht bei der betroffenen Person:

- Die öffentliche Stelle erlangt Daten der betroffenen Person aus allgemein zugänglichen Quellen wie aus der Zeitung, dem Internet oder durch beispielsweise Besichtigung allgemein zugänglicher Verkehrsflächen.
- Personenbezogene Daten werden von einer anderen öffentlichen Stelle auf Anfrage 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 bei der übermittelnden öffentlichen Stelle aus. Es liegt vielmehr aus Sicht der anfragenden öffentlichen Stelle eine Erhebung nach Art. 14 DSGVO vor. In diesem Fall hat also grundsätzlich die empfangende Stelle entsprechend dem Mustertext der Anlage 6b eine umfassende Information der betroffenen Person sicherzustellen und dabei unter Nr. 5 „Angabe der Quelle“ darzulegen, von welcher anderen Stelle die Daten übermittelt wurden.

Im Übrigen ist nach § 7 BbgDSG-neu 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 Ausnahmen?

Ausnahmen finden sich in Art. 14 Abs. 5 DSGVO und § 10 BbgDSG-neu oder können sich aus Fachgesetzen ergeben.

Eine Information der betroffenen Person kann nach Art. 14 Abs. 5 DSGVO unterleiben, wenn und soweit

- die betroffene Person bereits über die Informationen verfügt,
- sich die Erteilung einer Information als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, insbesondere bei Verarbeitungen für
    - im öffentlichen Interesse liegende Archivzwecke,
    - wissenschaftliche oder historische Forschungszwecke oder
    - Statistikzwecke,
- wenn die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen vorsehen, ausdrücklich geregelt ist oder
- wenn die personenbezogenen Daten dem Berufsgeheimnis unterliegen und daher vertraulich behandelt werden müssen (z.B. ein Rechtsanwalt, der von seinem Mandanten personenbezogene Daten über den Prozessgegner erhält).

Die Pflicht zur Information der betroffenen Person besteht des Weiteren nach § 10 Abs. 1 BbgDSG-neu 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 Abs. 1 BbgDSG-neu, so hat der Verantwortliche gemäß § 10 Abs. 2 BbgDSG-neu jedoch die Informationen nach Art. 14 DSGVO in allgemeiner Form für die Öffentlichkeit zur Verfügung zu stellen. Zudem hat der Verantwortliche festzuhalten, aus welchen Gründen von einer Information abgesehen wird.

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

3. Zeitpunkt, Form und Inhalt der Information

Werden personenbezogene Daten nicht direkt bei der betroffenen Person erhoben, weiß diese im Regelfall nichts von der Datenerhebung. Zur Information der betroffenen Person wird daher in aller Regel eine aktive Kontaktaufnahme erforderlich sein. Die notwendigen Informationen müssen nicht zwingend in Schriftform bereitgestellt werden, auch eine Information per E-Mail ist denkbar.

Die Informationen über eine Erhebung i. S. v. Art. 14 DSGVO sind der betroffenen Person innerhalb einer angemessenen Frist, spätestens jedoch innerhalb eines Monats nach Erlangung der Daten mitzuteilen (Art. 14 Abs. 3 Buchst. a DSGVO).
Diese Frist verkürzt sich ggf., wenn die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen (z. B. in einem Anschreiben). In diesem Fall ist die Information spätestens zu erteilen, wenn mit der Person das erste Mal in Kontakt getreten wird (Art. 14 Abs. 3 Buchst. b DSGVO). Erfolgt diese erste Kommunikation daher vor der Einmonatsfrist, muss der Informationspflicht spätestens bei der ersten Kontaktaufnahme nachgekommen werden, unabhängig davon, ob die Einmonatsfrist bisher nicht abgelaufen ist. Im umgekehrten Fall, wenn die erste Kommunikation später als einen Monat nach Erlangung der Daten erfolgt, gilt Art. 14 Abs. 3 Buchst. a DSGVO, sodass die betroffene Person spätestens innerhalb eines Monats informiert werden muss.
Falls eine Offenlegung an einen anderen Empfänger beabsichtigt ist, ist die Information spätestens zum Zeitpunkt der ersten Offenlegung zu erteilen (Art. 14 Abs. 3 Buchst. c DSGVO). Auch in diesem Fall verkürzt sich die Einmonatsfrist des Art. 14 Abs. 3 Buchst. b DSGVO, wenn die erste Offenlegung vor Ablauf von einem Monat nach Erlangung der Daten erfolgt. Werden die Daten später als einen Monat nach Erlangung der Daten zum ersten Mal gegenüber einem anderen Empfänger offengelegt, gilt Art. 14 Abs. 3 Buchst. a DSGVO, sodass die betroffene Person spätestens innerhalb eines Monats informiert werden muss.

Anlage 6b enthält einen Mustertext mit allen nach Art. 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 bestehende Formulare für Datenerhebungen sind an die neuen gesetzlichen Vorgaben anzupassen und zu ergänzen.

9.1.3 Zweckänderung (Art. 13 Abs. 3 bzw. Art. 14 Abs. 4 DSGVO)

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 (Art. 13 Abs. 3 DSGVO bzw. Art. 14 Abs. 4 DSGVO).

Generell liegt keine Zweckänderung vor, wenn die Daten für die in § 5 Abs. 2 BbgDSG-neu 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-neu geregelt, ergeben sich aus bereichsspezifischem Fachrecht oder aus Art. 6 Abs. 4 DSGVO unmittelbar (Stichwort: Vereinbarkeit des neuen Zwecks mit den Erhebungszwecken).

2. Gibt es Ausnahmen?

Gemäß § 6 Abs. 1 BbgDSG-neu 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, u. a. 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 Abs. 1 Nr. 1 BbgDSG-neu),
- es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist (§ 6 Abs. 1 Nr. 2 BbgDSG-neu),
- 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 Abs. 1 Nr. 3 BbgDSG-neu),
- es erforderlich ist, Angaben der betroffenen Person zu überprüfen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen (§ 6 Abs. 1 Nr. 4 BbgDSG-neu).

Eine Information der betroffenen Person kann unter den Voraussetzungen des § 6 Abs. 2 i. V. m. Abs. 1 Nr. 1 bis 4 BbgDSG-neu unterbleiben.

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 Art. 14 Abs. 5 Buchst. c DSGVO.

3. Zeitpunkt, Form und Inhalt der Information

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

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

Anlage 6a enthält unter dem Punkt „Sonderfall“ einen Mustertext und Ausfüllhinweise für Zweckänderungen, wenn die Daten direkt bei der betroffenen Person erhoben wurden (Art. 13 Abs. 3 DSGVO). Anlage 6b enthält unter dem Punkt „Sonderfall“ einen Mustertext und Ausfüllhinweise für Zweckänderungen, wenn die Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 Abs. 4 DSGVO). Bei Verwendung dieser Mustertexte sind die dort enthaltenen Angaben vollständig und auf die jeweilige Verarbeitungstätigkeit angepasst zur Verfügung zu stellen.

9.1.4 Informationspflicht bei einer Videoüberwachung öffentlich zugänglicher Räume

Für die Videoüberwachung öffentlich zugänglicher Räume enthalten § 28 Abs. 2 und Abs. 4 BbgDSG-neu besondere Regelungen der Informationspflicht. Die Videoüberwachung und die Informationen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen (z.B. durch Hinweisschilder, siehe auch Artikel 12 Abs. 7 DSGVO). Dabei sind der Verantwortliche, die Kontaktdaten des Datenschutzbeauftragten und die Zwecke sowie die Rechtsgrundlage der Verarbeitung anzugeben. Weiterhin ist darauf hinzuweisen, dass alle weiteren Informationen nach Art. 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 insofern der Zweck der Verarbeitung durch die Information gefährdet wird.

9.2 Auskunftsrecht der betroffenen Person

Das Auskunftsrecht nach Art. 15 DSGVO i.V.m. § 11 BbgDSG-neu entspricht im Wesentlichen dem bisherigen Recht auf Auskunft nach § 18 BbgDSG. Neu ist, dass explizit geregelt ist, 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 die Umstände der Datenverarbeitung.
Anders als bisher ist Auskunft über die Empfänger oder Kategorien von Empfängern zu erteilen, unabhängig davon, ob diese gespeichert sind (bisher gemäß § 18 Abs. 1 Satz 1 Nr. 3 BbgDSG nur, wenn die Empfänger gespeichert waren). Gegenüber der bisherigen Auskunftspflicht erweitert Art. 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 (Art. 12 Abs. 6 DSGVO).
Gemäß Erwägungsgrund 63 Satz 6 DSGVO kann der Verantwortliche verlangen, dass die betroffene Person präzisiert, auf welche Informationen oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht.

§ 11 Abs. 2 BbgDSG-neu enthält eine spezifizierende 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 (vgl. Begründung zu § 11 Abs. 2 BbgDSG-neu, Landtags-Drucksache 6/7365).

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

9.3 Löschung (Art. 17 DSGVO)

Die wichtigsten Fallgruppen, in denen die Löschung von Daten verlangt werden kann, bleiben erhalten.
Anders als der Wortlaut von Art. 17 Abs. 1 Buchst. a DSGVO zunächst vermuten lässt, besteht eine Löschpflicht - wie bisher - nicht nur, wenn die betroffene Person dies verlangt, sondern immer dann, wenn die personenbezogenen Daten für die Zwecke, für die sie verarbeitet wurden, nicht mehr erforderlich sind.
Nach Art. 17 Abs. 3 Buchst. b DSGVO scheidet eine Löschung z. B. auch weiterhin aus, wenn gesetzliche Aufbewahrungsfristen bestehen. Außerdem geht gemäß § 9 BbgDSG-neu auch weiterhin die archivrechtliche Anbietungspflicht einer Löschung vor.

Keine Ausnahme besteht mehr in den Fällen, in denen personenbezogene Daten in Akten gespeichert waren. Anders als bisher ist bei einer Verarbeitung (i. R. d. Speicherung von Vorgängen) in Akten zu prüfen, ob ein Vorgang weiterhin gespeichert werden muss, weil er für die Aufgabenerfüllung erforderlich ist oder ob er und die dabei verarbeiteten Daten gelöscht werden können. Begrifflich ist dabei die „Akte“ vom „Vorgang“ zu unterscheiden. Ein Vorgang umfasst in der Regel ein in sich abgeschlossenes (Verwaltungs-)Verfahren, beispielsweise die Bearbeitung eines Antrags von der Antragstellung bis zur Bescheidung, einschließlich eines etwaigen Rechtsbehelfsverfahrens oder die Bearbeitung einer Anfrage/Beschwerde. Vorgänge werden in Akten geführt. Enthält eine Akte mehrere Vorgänge mit personenbezogenen Daten ist zu prüfen, ob der konkrete Vorgang weiterhin für die Aufgabenerfüllung (Zweck der 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. In diesen Fällen ist zu prüfen, in welcher Weise dem für diese Teile bestehenden Löschungsgebot Rechnung getragen werden kann.

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

9.4 Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)

Unter „Einschränkung der Verarbeitung" sind nach den Erwägungsgründen Methoden zur Beschränkung der Verarbeitung personenbezogener Daten zu verstehen, z. B. dass ausgewählte personenbezogene Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzer gesperrt werden oder dass veröffentlichte Daten vorübergehend von einer Webseite entfernt werden. Damit entspricht dieses Recht im weitesten Sinne dem bisherigen Recht auf Sperrung nach § 19 Abs. 3 BbgDSG.

Unter Geltendmachung seines 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, den Betroffenen vor der Aufhebung der Einschränkung zu unterrichten.

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

9.5 Sonstige Rechte der betroffenen Person

9.5.1 Recht auf Berichtigung (Art. 16 DSGVO)

Eine ähnliche Regelung gibt es bereits in § 19 Abs. 1 BbgDSG. Die betroffene Person hat nach Art. 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. Hierzu folgendes Beispiel: Bei einem Gewerbetreibenden wird seine Zuverlässigkeit überprüft. Aus den Akten geht hervor, dass er Steuerschulden hat, was gegen seine Zuverlässigkeit sprechen kann. Diese Information ist dann unvollständig, wenn in der Sache ein finanzgerichtliches Verfahren anhängig ist und darauf nicht hingewiesen wird.

9.5.2 Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Nach Art. 20 DSGVO haben betroffene Personen in Zukunft das Recht, die sie betreffenden personenbezogenen Daten, die sie einem für die Verarbeitung Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie haben das Recht, diese Daten einem anderen 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 (vgl. Art. 20 Abs. 3 Satz 2 DSGVO). Der Anwendungsbereich wird somit für öffentliche Stellen sehr gering sein.

9.5.3 Widerspruchsrecht (Art. 21 DSGVO)

Gemäß Art. 21 DSGVO hat die betroffene Person – wie bisher gemäß § 4b BbgDSG - 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 (Art. 6 Abs. 1 Buchst. e oder f DSGVO). Dabei ist Voraussetzung, dass sie 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.

10. Auftragsverarbeitung

Die DSGVO regelt die Auftragsverarbeitung insbesondere in den Art. 28 und 29. Das bereichsspezifischen Bundes- oder Landesrecht kann Regelungen enthalten, die das „Ob“ der Auftragsverarbeitung bestimmen, also die Frage betreffen, ob in bestimmten Fällen eine Auftragsverarbeitung zulässig ist (vgl. z. B. § 80 SGB X). Im Hinblick auf die Frage, wann von einer Auftragsverarbeitung ausgegangen werden muss und das „Wie“ der Auftragsverarbeitung, also die spezifischen Anforderungen an die Aus-

gestaltung der Auftragsverarbeitung, sind die Art. 28 und 29 DSGVO dagegen abschließend und gelten unmittelbar.

10.1 Welche Neuerungen gibt es?

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

- Der Mindestinhalt eines Vertrages zur Auftragsverarbeitung ist umfassender.
- Der Vertrag zur Auftragsverarbeitung kann nicht nur schriftlich sondern auch in einem elektronischen Format geschlossen werden.
- Weisungen des Verantwortlichen an den Auftragsverarbeiter sind zu dokumentieren.
- Der Auftragsverarbeiter hat ein eigenes Verzeichnis von Verarbeitungstätigkeiten zu erstellen (Artikel 30 Abs. 2 DSGVO).
- Will der Auftragsverarbeiter Subunternehmen als weitere Auftragsverarbeiter bei der Erbringung der vereinbarten Dienstleistung einsetzen, so bedarf dies der vorherigen (schriftlichen oder elektronischen) Genehmigung durch den Verantwortlichen. Später beabsichtigte Änderungen bei den eingesetzten Subunternehmen muss der Auftragsverarbeiter vorher mitteilen, wobei der Verantwortliche dann bei Bedarf Einspruch gegen die geplante Einbeziehung des neuen Subunternehmens einlegen kann.
- Der Spielraum bei der Kontrolle des Auftragsverarbeiters durch den Verantwortlichen vergrößert sich. Es ist z. B. nicht mehr zwingend eine Vorort-Kontrolle erforderlich, sondern es kann auch auf Zertifizierungen zurückgegriffen werden.
- 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

Art. 28 Abs.3 DSGVO legt detailliert fest, welcher Mindestinhalt in den Vertrag aufgenommen werden muss. Die dortigen Festlegungen gehen über die bisherigen Regelungen in § 11 BbgDSG hinaus. Im Vertrag sind Festlegungen zu treffen

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

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

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

Für den Anpassungsprozess bedeutet dies insbesondere, dass bestehende Verträge zu überprüfen und ggf. durch ergänzende Vereinbarungen an die neue Rechtslage anzupassen sind. Als Grundlage des Überprüfungsprozesses kann der als Anlage 7 beigefügte Mustervertragsentwurf genutzt werden. Auf welche Weise eine ggf. 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.

Da bislang noch nicht abschließend geklärt wurde, ob bzw. in welchen Fällen Abweichungen von den Vorgaben von Art. 28 DSGVO zur Rechtswidrigkeit einer Auftragsverarbeitung führen, empfiehlt es sich, die erforderlichen Anpassungen möglichst noch vor dem 25. Mai 2018 vorzunehmen bzw. zu vereinbaren, zumindest aber auf den Weg zu bringen.

<u>Handlungserfordernisse:</u>

- Überprüfung der bestehenden Verträge, ob diese die Vorgaben von Art. 28 DSGVO einhalten.

11. Technischer und organisatorischer Datenschutz

Die DSGVO enthält vor allem in Art. 5 und Art. 32 Vorgaben zur „Sicherheit der Verarbeitung“. Beibehalten wird das grundsätzliche Prinzip, dass geeignete technische und organisatorische Maßnahmen zu treffen sind, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten (bisher § 10 Abs. 1 BbgDSG). 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 Art. 32 Abs. 1 Buchst. a DSGVO lediglich Pseudonymisierung und Verschlüsselung der Daten.
Die bisherigen sechs Schutzziele des BbgDSG (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz) werden in Art. 32 Abs. 1 Buchst. 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 BSI 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 / starker Beanspruchung" funktionieren sollen, was ggf. in einem entsprechenden Notfallmanagement zu berücksichtigen wäre. Außerdem besteht gemäß Art. 32 Abs. 1 Buchst. c DSGVO die Forderung, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall schnell wiederhergestellt werden sollen. Dies war grundsätzlich auch schon bisher im Rahmen der Verfügbarkeit der Daten sicherzustellen. Die Wiederherstellung der Daten muss somit regelmäßig getestet werden.

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

- Vor Festlegung der technischen und organisatorischen Maßnahmen hat eine risikobasierte Abwägung zu erfolgen. Diese beinhaltet, dass alle möglichen Bedrohungen und Schwachstellen mit ihrer jeweiligen Eintrittswahrscheinlichkeit und der potentiellen Schwere des Schadens für die Rechte und Freiheiten betroffener Personen identifiziert werden.
- Die bisher bekannten Prinzipien der Datenvermeidung und -sparsamkeit werden durch Art. 25 Abs. 1 und 2 DSGVO konkretisiert und fordern künftig Datenschutz durch Technikgestaltung und durch datenschutzrechtliche Voreinstellungen (Privacy by design und Privacy by default).
- Der Verantwortliche muss die technischen und organisatorischen Maßnahmen, die er getroffen hat, nachweisen und aktuell halten. Gemäß Art. 32 Abs. 1 Buchst. d DSGVO muss nun auch die Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen getestet und ggf. nachgesteuert werden.

Handlungserfordernisse:

- Der Verantwortliche hat die technischen und organisatorischen Maßnahmen zu dokumentieren. Dies sollte im Rahmen eines Datenschutzkonzeptes (siehe Ziffer 13) 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 bei design und Privacy by default sollten künftig bereits im Zuge der vergaberechtskonformen Ausschreibung von IT-Produkten berücksichtigt werden.

12. Datengeheimnis, Dienstanweisungen

Eine gesetzliche Regelung zur Wahrung des Datengeheimnisses, wie es bisher in § 6 BbgDSG geregelt war, sieht die DSGVO 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 bisherige Regelung im BbgDSG zum Datengeheimnis entfallen. Dennoch wird empfohlen, eine entsprechende Verpflichtung (z.B. in einer Dienstanweisung oder im Einzelnen durch eine Verpflichtung bestimmter Personen) vorzunehmen, denn der Verantwortliche hat nach Art. 24 DSGVO sicherzustellen, dass per-

sonenbezogene 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 Mitarbeiter als diejenigen, die personenbezogene Daten verarbeiten, sind von diesen Maßnahmen betroffen. Die öffentliche Stelle muss deshalb sicherstellen, dass die Mitarbeiter 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 Mitarbeiter erkennen können, wann sie ggf. mit der Datenverarbeitung gegen Gesetze verstoßen bzw. unberechtigt Daten verarbeiten.

Darüber hinaus sieht Art. 32 Abs. 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 Mitarbeiter zum Umgang mit personenbezogenen Daten an ihrem konkreten Arbeitsplatz oder Weisung bezogen auf einen Einzelfall sein.

Anlage 8 enthält ein Muster für eine schriftliche Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DSGVO.

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

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.
- Ggf. bereits verwendete Vordrucke und Merkblätter sind an die DSGVO anzupassen.

13. Dokumentationspflichten und Datenschutzmanagement

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

- Nachweis der Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 u. 2 DSGVO)
- Nachweis der erteilten Einwilligungen (Art. 7 Abs. 1 DSGVO)
- Nachweis der Einhaltung der Betroffenenrechte (gemäß Art. 12 ff. DSGVO)
- Nachweis der technische und organisatorische Maßnahmen (Art. 24 Abs. 1, Art. 32 DSGVO)
- Führung von Verarbeitungsverzeichnissen (Art. 30 DSGVO)

- Dokumentation von Datenschutzvorfällen (Art. 33 Abs. 5 DSGVO)
- Durchführung des Freigabeverfahrens/Freigabeerklärung (gemäß § 4 BbgDSG-neu)
- Durchführung der Datenschutz-Folgenabschätzung (gemäß Art. 35 DSGVO)
- Verträge über Auftragsverarbeitungen **(**gemäß Art. 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 eines solchen Konzepts sind Regelungen zu:

- Ziel und Gültigkeitsbereich
- übergreifenden Leitlinien zum Datenschutz / Grundsätze der Verarbeitung personenbezogener Daten
- Festlegungen zur Verantwortlichkeit für den Datenschutz in der öffentlichen Stelle (übergreifend und in Spezialfragen)
    - z. B. Festlegung der Abteilung, des Sachgebietes etc. welches für die Verarbeitung der Daten zuständig ist,
    - Zuständigkeit für die Bearbeitung von Beschwerden oder Auskunftsersuchen,
    - evtl. Festlegungen zur Auftragsverarbeitung,
    - frühzeitige Einbeziehung des Datenschutzbeauftragten in die Verfahrenseinführung bzw. bereits zum Zeitpunkt der Verfahrensausschreibung
- Verhalten bei Datenschutzpannen (Meldewege, Zuständigkeiten)
- Datenschutzbeauftragter, Aufgaben, Stellung
- Verzeichnissen von Verarbeitungstätigkeiten
- Freigabeverfahren
- Datenschutz-Folgenabschätzungen
- Erläuterungen zum Schutzbedarf und Verfahren, um den Schutzbedarf zu bestimmen
- Maßnahmen für die Sicherheit der Verarbeitung, übergreifend und für spezielle Verarbeitungen bzw. Datenkategorien
- organisatorischen Richtlinien (wie Backup, Virenschutz, Protokollierung)
- Gewährleistung der Betroffenenrechte
- Regelungen für den Fall der Auftragsverarbeitung
- Datenschutz-Unterweisungen
- regelmäßigen Datenschutz-Kontrollen und Audits

<u>Handlungserfordernisse:</u>

- Entwicklung eines Datenschutzkonzepts
    - Datenschutzorganisation
    - Technischer Datenschutz
    - Dokumentation

14. Empfehlung für den Anpassungsprozess

Empfehlungen	Anmerkungen

Prüfung der Zulässigkeit der Datenverarbeitungen	- Prüfen, ob das neue Recht für alle Prozesse eine Rechtsgrundlage bereitstellt - Vorhandene Einwilligungen prüfen, um sicherzustellen, dass sie nach Wirksamwerden der DSGVO fortgelten - Überprüfung von Dienstvereinbarungen, Satzungsrecht, Verwaltungsvorschriften und Geschäftsordnungen im Hinblick auf die Vereinbarkeit mit der DSGVO
Einführung eines Datenschutzmanagements **Insbesondere zur Erfüllung der Dokumentationspflichten**	- Festlegung von Zuständigkeiten - Entwicklung eines Datenschutzkonzepts - Anpassung der technischen und organisatorischen Maßnahmen • Technische und organisatorischen Maßnahmen im Rahmen des Datenschutzkonzepts dokumentieren • Etablierung eines Verfahrens, das regelmäßig die Wirksamkeit der technischen und organisatorischen Maßnahmen bewertet und evaluiert • Berücksichtigung der Prinzipien Privacy bei design und Privacy by default künftig bereits im Zuge der vergaberechtskonformen Ausschreibung von IT-Produkten
Organisatorische Maßnahmen zu Betroffenenrechten festlegen	- Wer ist innerhalb der öffentlichen Stelle zuständig, wenn ein Betroffener seine Rechte geltend macht? - In welcher Frist soll das Anliegen des Betroffenen weitergeleitet und bearbeitet werden (beachte: Monatsfrist nach DSGVO für die Antwort)? - In welcher Form soll das Anliegen weitergeleitet werden (Stichwort: Geheimhaltung, Vertraulichkeit)? - Wer sind die Ansprechpartner für verschiedene Datenverarbeitungssysteme (um beispielsweise den Auskunftsanspruch überall in der öffentlichen Stelle gewährleisten zu können)? Es sind Verfahren zu definieren, wie die Informa-

	tionspflichten nach Art. 13 und 14 DSGVO erfüllt werden sollen. Für Standardverarbeitungen empfiehlt sich die Verwendung von Mustern (Näheres Ziffer 9.1).
Einführung oder Anpassung von Verfahren zur - **Führung von Verarbeitungsverzeichnissen** - **Durchführung des Freigabeverfahrens** - **Durchführung der Datenschutz-Folgenabschätzung**	- Anpassung der bestehenden Verfahrensverzeichnisse an Art. 30 DSGVO - Prüfen, ob für alle Verarbeitungen ein Verarbeitungsverzeichnis vorliegt - Berücksichtigung der an die DSGVO angepassten Inhalte des Freigabeverfahrens und der Freigabeerklärung - Die Vorabkontrolle gemäß § 10a BbgDSG wird durch die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO abgelöst und erfordert eine umfangreiche Dokumentation - Für Verarbeitungen, von denen hohe Risiken ausgehen, muss keine Folgenabschätzung vorgenommen werden, wenn sie der Vorabkontrolle durch den Datenschutzbeauftragten unterlegen haben und ohne wesentliche Änderung fortgeführt werden. Einer Überprüfung der Verarbeitungen innerhalb der nächsten 2-3 Jahre sind die Anforderungen von Art. 35 DSGVO zugrunde zu legen.
Bestellung eines behördlichen Datenschutzbeauftragten und Anpassungen des Aufgabenbereichs des behördlichen Datenschutzbeauftragten	- Bereits bestellte Datenschutzbeauftragte bleiben in ihrer Funktion - Ggf. Überprüfung der Qualifikation und Unabhängigkeit - Neue Aufgaben und Verantwortlichkeiten beachten - Sollen weitere Aufgaben übertragen werden, ist dies durch den Verantwortlichen zu regeln - Prüfen, ob angesichts der geänderten bzw. erweiterten Aufgaben die Ressourcen des Datenschutzbeauftragten ausreichend sind - Veröffentlichung der Kontaktdaten und Mitteilung an die LDA (Art. 37 Abs. 7 DSGVO)
Beschäftigte ggf. zur Geheimhaltung verpflichten	- Im Rahmen organisatorischer Maßnahmen ist zu entscheiden ob und in welcher Weise die Beschäftigten zur Einhaltung der datenschutz-

	rechtlichen verpflichtet und entsprechend belehrt werden - Ggf. bereits verwendete Vordrucke und Merkblätter sind an die DSGVO anzupassen
Anpassung von Verträgen über Auftragsverarbeitungen	Überprüfung der bestehenden Verträge, ob diese die Vorgaben von Art. 28 DSGVO einhalten