Abgeordnetenhaus BERLIN

Drucksache 18/1033
09.05.2018

18. Wahlperiode

Antrag

der Fraktion der SPD, der Fraktion Die Linke und der Fraktion Bündnis 90/Die Grünen

Gesetz zur Anpassung des Berliner Datenschutzgesetzes und weiterer Gesetze an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Berliner Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – BlnDSAnpUG-EU)

Das Abgeordnetenhaus wolle beschließen:

Gesetz zur Anpassung des Berliner Datenschutzgesetzes und weiterer Gesetze an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Berliner Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – BlnDSAnpUG-EU)

Vom ...

Das Abgeordnetenhaus hat das folgende Gesetz beschlossen:

Artikel 1
Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz - BlnDSG)

Inhaltsübersicht

Kapitel 3
Rechte der betroffenen Personen

Kapitel 4
Pflichten der Verantwortlichen und Auftragsverarbeiter

Kapitel 5
Sanktionen

Teil 3
Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680

Kapitel 1
Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Kapitel 2
Rechtsgrundlagen der Verarbeitung

Kapitel 3
Rechte der betroffenen Person

Kapitel 4
Pflichten der Verantwortlichen und Auftragsverarbeiter

Kapitel 5
Datenübermittlungen an Drittstaaten und an internationale Organisationen

Kapitel 6
Zusammenarbeit der Aufsichtsbehörden

Kapitel 7
Haftung und Sanktionen

Teil 4
Besondere Verarbeitungssituationen außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680

Teil 5
Schlussvorschrift

Teil 1
Gemeinsame Bestimmungen

Kapitel 1
Allgemeine Bestimmungen

§ 1
Zweck

(1) Dieses Gesetz trifft in den Teilen 1 und 2 sowohl ergänzende als auch abweichende Regelungen zur Durchführung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72).

(2) Darüber hinaus erfolgt in den Teilen 1 und 3 dieses Gesetzes die Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. 5.2016, S. 89).

(3) In den Teilen 1 und 4 trifft dieses Gesetz Regelungen für die Verarbeitung personenbezogener Daten, die weder in den Anwendungsbereich der Verordnung (EU) 2016/679 noch der Richtlinie (EU) 2016/680 fallen.

§ 2
Anwendungsbereich

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen (insbesondere nichtrechtsfähige Anstalten, Krankenhausbetriebe, Eigenbetriebe und Gerichte) des Landes Berlin und der landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts im Sinne des § 28 des Allgemeinen Zuständigkeitsgesetzes (öffentliche Stellen).

(2) Als öffentliche Stellen gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen auch Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen das Land Berlin mit absoluter Mehrheit der Anteile oder mit absoluter Mehrheit der Stimmen beteiligt ist. Nehmen nicht-öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes.

(3) Das Abgeordnetenhaus, seine Mitglieder, die Fraktionen sowie ihre jeweiligen Verwaltungen und Beschäftigten unterliegen nicht den Bestimmungen dieses Gesetzes, soweit sie zur Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten.

(4) Für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit zuständigen öffentlichen Stellen gelten nur Teil 1 und Teil 3 dieses Gesetzes, soweit diese Stellen personenbezogene Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten.

(5) Die Vorschriften dieses Gesetzes finden keine Anwendung, soweit das Recht der Europäischen Union, im Besonderen die Verordnung (EU) 2016/679 in der jeweils geltenden Fassung, unmittelbar gilt.

(6) Abweichend von den Absätzen 1 und 2 gelten öffentliche Stellen, soweit diese als Unternehmen am Wettbewerb teilnehmen, als nicht-öffentliche Stellen. Insoweit sind für sie nur die Regelungen der §§ 4 bis 6 und § 20 sowie § 22 anwendbar. Im Übrigen finden für sie die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) in der jeweils geltenden Fassung Anwendung mit Ausnahme von § 4 und § 38 des Bundesdatenschutzgesetzes.

(7) Abweichend von Absatz 1 gilt § 19 auch für nicht-öffentliche Stellen, soweit diese personenbezogene Daten in Ausübung des Rechts auf freie Meinungsäußerung und Informationsfreiheit zu journalistischen, künstlerischen oder literarischen Zwecken verarbeiten. Dies gilt nicht, soweit die Verarbeitung ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten erfolgt.

(8) Besondere Rechtsvorschriften über den Datenschutz gehen den Bestimmungen dieses Gesetzes vor. Regeln sie einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften dieses Gesetzes Anwendung.

(9) Für Verarbeitungen personenbezogener Daten im Rahmen von Tätigkeiten, die nicht in den Anwendungsbereich der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallen, finden die Verordnung (EU) 2016/679 und Teil 1 und 2 dieses Gesetzes entsprechend Anwendung, soweit nicht in Teil 4 oder in einem anderen Gesetz Abweichendes geregelt ist.

(10) Bei Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679 stehen die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und die Schweiz den Mitgliedsstaaten der Europäischen Union gleich. Andere Staaten gelten insoweit als Drittstaaten.

(11) Bei Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 stehen die bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands assoziierten Staaten den Mitgliedstaaten der Europäischen Union gleich. Andere Staaten gelten insoweit als Drittstaaten.

Kapitel 2
Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 3
Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist. Diese Regelung tritt am 30. Juni 2020 außer Kraft.

Kapitel 3
Datenschutzbeauftragte öffentlicher Stellen

§ 4
Benennung

(1) Öffentliche Stellen benennen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten. Dies gilt auch für öffentliche Stellen, die am Wettbewerb teilnehmen.

(2) Für mehrere öffentliche Stellen kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe eine gemeinsame Datenschutzbeauftragte oder ein gemeinsamer Datenschutzbeauftragter benannt werden.

(3) Für die aufgrund Absatz 1 Satz 1 oder Absatz 2 benannte Person wird eine Vertreterin oder ein Vertreter benannt. Für die Vertreterin oder den Vertreter gelten die Vorschriften dieses Kapitels mit Ausnahme von § 5 Absatz 4 entsprechend.

(4) Die oder der Datenschutzbeauftragte wird auf der Grundlage der beruflichen Qualifikation und insbesondere des Fachwissens benannt, das sie oder er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage ihrer oder seiner Fähigkeit zur Erfüllung der in § 6 genannten Aufgaben.

(5) Die oder der Datenschutzbeauftragte kann Beschäftigte oder Beschäftigter der öffentlichen Stelle sein oder ihre oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(6) Die öffentliche Stelle veröffentlicht die Kontaktdaten der oder des Datenschutzbeauftragten und teilt diese Daten der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit mit.

§ 5
Stellung

(1) Die öffentliche Stelle stellt sicher, dass die oder der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Die öffentliche Stelle unterstützt die Datenschutzbeauftragte oder den Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben gemäß § 6, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung ihres oder seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt.

(3) Die öffentliche Stelle stellt sicher, dass die oder der Datenschutzbeauftragte bei der Erfüllung ihrer oder seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Die oder der Datenschutzbeauftragte berichtet unmittelbar der höchsten Leitungsebene der öffentlichen Stelle. Die oder der Datenschutzbeauftragte darf von der öffentlichen Stelle wegen der Erfüllung ihrer oder seiner Aufgaben nicht abberufen oder benachteiligt werden.

(4) Die Abberufung der oder des Datenschutzbeauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs zulässig. Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach dem Ende der Tätigkeit als Datenschutzbeauftragte oder als Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig, es sei denn, dass die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

(5) Betroffene Personen können die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der Verordnung (EU) 2016/679, diesem Gesetz sowie anderen Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen. Die oder der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Personen sowie über Umstände, die Rückschlüsse auf die betroffenen Personen zulassen, verpflichtet, soweit sie oder er nicht davon durch die betroffenen Personen befreit wird.

(6) Wenn die oder der Datenschutzbeauftragte bei ihrer oder seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch der oder dem Datenschutzbeauftragten und den ihr oder ihm unterstellten Beschäftigten zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht der oder des Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Dokumente einem Beschlagnahmeverbot.

§ 6
Aufgaben

(1) Der oder dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

1. Unterrichtung und Beratung der öffentlichen Stelle und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach diesem Gesetz und sonstigen Vor-

schriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften;

2. Überwachung der Einhaltung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, sowie der Strategien der öffentlichen Stelle für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und der Schulung der an den Verarbeitungsvorgängen beteiligten Beschäftigten und der diesbezüglichen Überprüfungen;

3. Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß § 53;

4. Zusammenarbeit mit der Aufsichtsbehörde;

5. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß § 55 und gegebenenfalls Beratung zu allen sonstigen Fragen.

(2) Die in Absatz 1 genannten Aufgaben der oder des Datenschutzbeauftragten beziehen sich nicht auf die Verarbeitung von personenbezogenen Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit und durch den Rechnungshof im Rahmen seiner unabhängigen Tätigkeit.

(3) Die oder der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Die öffentliche Stelle stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

(4) Die oder der Datenschutzbeauftragte trägt bei der Erfüllung ihrer oder seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei sie oder er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Kapitel 4
Berliner Beauftragte oder Beauftragter für Datenschutz und Informationsfreiheit

§ 7
Errichtung

Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist eine oberste Landesbehörde.

§ 8
Zuständigkeit

(1) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist Aufsichtsbehörde für die öffentlichen Stellen des Landes Berlin. Die Vorschriften dieses Kapitels gelten auch für Auftragsverarbeiter, soweit sie nicht-öffentliche Stellen sind, bei denen dem Land die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle des Landes ist.

(2) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist Aufsichtsbehörde nach § 40 des Bundesdatenschutzgesetzes für die Datenverarbeitung nichtöffentlicher Stellen und öffentlicher Stellen, soweit diese am Wettbewerb teilnehmen.

(3) Die oder der Beauftragte für Datenschutz und Informationsfreiheit ist nicht zuständig für die Aufsicht über die von den Gerichten im Rahmen ihrer justiziellen Tätigkeit oder über die vom Rechnungshof in unabhängiger Tätigkeit vorgenommenen Verarbeitungen personenbezogener Daten.

§ 9
Ernennung und Beendigung des Amtsverhältnisses

(1) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit wird vom Abgeordnetenhaus mit den Stimmen der Mehrheit seiner Mitglieder gewählt und von der Präsidentin oder dem Präsidenten des Abgeordnetenhauses ernannt. Sie oder er nimmt zugleich die Aufgaben der oder des Landesbeauftragten für das Recht auf Akteneinsicht nach § 18 Absatz 1 des Berliner Informationsfreiheitsgesetzes vom 15. Oktober 1999 (GVBl. S. 561), das zuletzt durch Gesetz vom 7. Juli 2016 (GVBl. S. 434) geändert worden ist, wahr und führt die Amts- und Funktionsbezeichnung "Berliner Beauftragter für Datenschutz und Informationsfreiheit“ in weiblicher oder männlicher Form. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit muss über die zur Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Sie oder er muss über durch einschlägige Berufserfahrung erworbene Kenntnisse des Datenschutzrechts verfügen und die Befähigung zum Richteramt oder höheren Verwaltungsdienst besitzen.

(2) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit leistet vor der Präsidentin oder dem Präsidenten des Abgeordnetenhauses folgenden Eid: "Ich schwöre, mein Amt gerecht und unparteiisch getreu dem Grundgesetz, der Verfassung von Berlin und den Gesetzen zu führen und meine ganze Kraft dafür einzusetzen, so wahr mir Gott helfe.“ Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit beträgt fünf Jahre. Das Amtsverhältnis endet mit Ablauf der Amtszeit, durch Entlassung oder Rücktritt. Nach dem Ende der Amtszeit bleibt die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit auf Aufforderung des Präsidiums des Abgeordnetenhauses bis zur Ernennung einer Nachfolgerin oder eines Nachfolgers im Amt, längstens jedoch für neun Monate. Die einmalige Wiederwahl ist zulässig. Vor Ablauf der Amtszeit kann die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit entlassen werden, wenn sie oder er eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung der Aufgaben nicht mehr erfüllt sind.

§ 10
Rechtsstellung

(1) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit steht nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis.

(2) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit handelt bei der Erfüllung ihrer oder seiner Aufgaben und bei der Ausübung ihrer oder seiner Befugnisse völlig unabhängig. Sie oder er unterliegt weder direkter noch indirekter Beeinflussung von außen und ersucht weder um Weisung noch nimmt sie oder er Weisungen entgegen.

(3) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit untersteht der Rechnungsprüfung des Rechnungshofs, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

(4) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit sieht von allen mit den Aufgaben dieses Amtes nicht zu vereinbarenden Handlungen ab und übt während der Amtszeit keine andere mit diesem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus. Insbesondere darf sie oder er neben diesem Amt kein weiteres besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung, dem Aufsichtsrat oder dem Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Sie oder er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(5) Die oder der Berliner Beauftragte für Datenschutz ist, auch nach Beendigung des Amtsverhältnisses, verpflichtet, über die ihr oder ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit entscheidet nach pflichtgemäßem Ermessen, ob und inwieweit sie oder er über solche Angelegenheiten vor Gericht oder außergerichtlich aussagt oder Erklärungen abgibt; wenn sie oder er nicht mehr im Amt ist, ist die Genehmigung der oder des amtierenden Berliner Beauftragten für Datenschutz und Informationsfreiheit erforderlich.

(6) Im Übrigen wird die Rechtsstellung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit durch Vertrag geregelt. Soweit in diesem Gesetz und im Vertrag keine abweichenden Bestimmungen getroffen worden sind, finden die für Beamtinnen und Beamte des Landes Berlin geltenden Vorschriften in dem Umfang sinngemäß Anwendung, als sie dem Wesen des Amtsverhältnisses entsprechen.

§ 11
Aufgaben

(1) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat unbeschadet anderer in der Verordnung (EU) 2016/679 genannten Aufgaben die Aufgaben,

1. die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zu überwachen und durchzusetzen,

2. die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären, wobei spezifische Maßnahmen für Kinder besondere Beachtung finden,

3. das Abgeordnetenhaus, den Senat und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten,

4. die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich den zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, entstehenden Pflichten zu sensibilisieren,

5. auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zur Verfügung zu stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden des Bundes, der Länder oder anderer Mitgliedstaaten der Europäischen Union zusammenzuarbeiten,

6. sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 55 der Richtlinie (EU) 2016/680 zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführenden innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist,

7. mit anderen Aufsichtsbehörden zusammenzuarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe zu leisten, um die einheitliche Anwendung und Durchsetzung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zu gewährleisten,

8. Untersuchungen über die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, durchzuführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde,

9. maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken,

10. Beratung in Bezug auf die in § 55 genannten Verarbeitungsvorgänge zu leisten und

11. Beiträge zur Tätigkeit des Europäischen Datenschutzausschusses zu leisten.

Im Anwendungsbereich der Richtlinie (EU) 2016/680 nimmt die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit zudem die Aufgabe nach § 46 wahr.

(2) Zur Erfüllung der in Absatz 1 Satz 1 Nummer 3 genannten Aufgabe kann die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an das Abgeordnetenhaus oder einen seiner Ausschüsse, den Senat, sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit richten.

(3) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit erleichtert das Einreichen der in Absatz 1 Satz 1 Nummer 6 genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(4) Die Erfüllung der Aufgaben der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit ist für die betroffene Person unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anfragen, insbesondere im Fall von häufiger Wiederholung, kann die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In diesem Fall trägt die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

§ 12
Tätigkeitsbericht

(1) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit erstellt einen Jahresbericht über ihre oder seine Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen, einschließlich der verhängten Sanktionen und der Maßnahmen nach Artikel 58 Absatz 2 der Verordnung (EU) 2016/679, enthalten kann. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit übermittelt den Bericht dem Abgeordnetenhaus und dem Senat und macht ihn der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich.

(2) Der Senat legt dem Abgeordnetenhaus zu dem Tätigkeitsbericht innerhalb von sechs Monaten nach dessen Vorlage eine Stellungnahme vor, soweit der Tätigkeitsbericht seinen Zuständigkeits- beziehungsweise Verantwortungsbereich betrifft.

§ 13
Befugnisse

(1) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit nimmt im Anwendungsbereich der Verordnung (EU) 2016/679 die Befugnisse gemäß Artikel 58 der Verordnung (EU) 2016/679 wahr. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann im Falle von Verstößen gegen Vorschriften der Verordnung (EU) 2016/679, dieses Gesetzes sowie andere Vorschriften über den Datenschutz, diese mit der Aufforderung beanstanden, innerhalb einer bestimmten, angemessenen Frist Stellung zu nehmen sowie Maßnahmen darzustellen, die die Verstöße beseitigen sollen.

(2) Stellt die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit bei Datenverarbeitungen durch öffentliche Stellen zu Zwecken außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet sie oder er dies gegenüber dem Verantwortlichen und fordert diese zur Stellungnahme innerhalb einer von ihr oder ihm zu be-

stimmenden angemessenen Frist auf. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit getroffen worden sind. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann den Verantwortlichen auch davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstoßen.

(3) Sofern in den Fällen des Absatzes 1 Satz 2 und Absatz 2 Satz 1 die beanstandeten Verstöße oder Mängel auch unter Berücksichtigung der Stellungnahme weiterhin bestehen, kann die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit dem für die öffentliche Stelle jeweils zuständigen Ausschuss des Abgeordnetenhauses Bericht erstatten und hierfür die Aufnahme auf die Tagesordnung einer Sitzung des Ausschusses verlangen, wenn ein vorheriger Einigungsversuch mit der öffentlichen Stelle erfolglos geblieben ist. Dieses Recht besteht auch ohne vorherigen Einigungsversuch, wenn die Stellungnahme nicht innerhalb der bestimmten Frist erfolgt; dies gilt auch, wenn die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit die öffentliche Stelle zu einer weiteren Stellungnahme unter Setzung einer angemessenen Frist auffordert. Verfahren, Form und Frist für die Aufnahme auf die Tagesordnung des jeweils zuständigen Ausschusses richten sich nach den durch das Abgeordnetenhaus festgelegten Regelungen. Die Rechte der Abgeordneten, insbesondere zur Gestaltung der Sitzung in dem Ausschuss, bleiben unberührt. Andere Rechte der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit, insbesondere das Recht aus Artikel 58 Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 und aus § 11 Absatz 2, bleiben unberührt.

(4) Die öffentlichen Stellen sind verpflichtet, der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit und ihren oder seinen Beauftragten

1. jederzeit Zugang zu den Diensträumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, zu gewähren und

2. alle Informationen, die für die Erfüllung ihrer oder seiner Aufgaben erforderlich sind, bereitzustellen.

(5) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist befugt, die durch sie oder ihn festgestellten Verstöße gegen Vorschriften der Verordnung (EU) 2016/679, dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den zuständigen Justizbehörden zur Kenntnis zu bringen und personenbezogene Daten zu übermitteln, soweit dies zur Durchführung des jeweiligen Ermittlungsverfahrens erforderlich ist.

(6) Soweit es für die Erfüllung ihrer oder seiner Aufgaben erforderlich ist, kann die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit personenbezogene Daten verarbeiten. Dies gilt auch für die Verarbeitung von besonderen Kategorien personenbezogener Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679, soweit ein erhebliches öffentliches Interesse dies erfordert. Ein erhebliches öffentliches Interesse nach Satz 2 liegt insbesondere vor, wenn die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit Aufgaben nach Artikel 57 Absatz 1 Buchstaben a, d bis h, l, o und t der Verord-

nung (EU) 2016/679 und nach § 11 Absatz 1 Nummern 1, 4 bis 8 und 10 bis 11 sowie § 46 und § 68 wahrnimmt.

(7) Soweit die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit Adressatin oder Adressat eines Beschlusses des Europäischen Datenschutzausschusses ist, hat sie oder er das Recht, unter den in Artikel 263 des Vertrages über die Arbeitsweise der Europäischen Union genannten Voraussetzungen binnen zwei Monaten nach dessen Übermittlung beim Europäischen Gerichtshof eine Klage auf Nichtigerklärung des Beschlusses zu erheben.

(8) Für die Verpflichtung nach Absatz 4 wird das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes, Artikel 28 Absatz 2 Satz 1 der Verfassung von Berlin) für die Betriebs- und Geschäftszeit eingeschränkt.

Teil 2
Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679

Kapitel 1
Grundsätze der Verarbeitung personenbezogener Daten

§ 14
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Neben den in Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 unmittelbar genannten Ausnahmen vom Verarbeitungsverbot können besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 in Ausgestaltung von Artikel 9 Absatz 2 Buchstaben b, h und i verarbeitet werden, wenn dies erforderlich ist

1. um die aus dem Dienst- und Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und den diesbezüglichen Pflichten nachkommen zu können,

2. zum Zweck der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit der Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen oder Diensten im Gesundheits- oder Sozialbereich unter den Voraussetzungen des Artikels 9 Absatz 3 der Verordnung (EU) 2016/679 oder

3. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten; ergänzend zu den in Absatz 3 genannten Maßnahmen sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist über Absatz 1 hinaus in Ausgestaltung von Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 zulässig, wenn sie erforderlich ist

1. zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit oder

2. zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls,

und die Interessen des Verantwortlichen an der Datenverarbeitung die Interessen der betroffenen Person überwiegen.

(3) Bei der Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstän-

de und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

1. die Maßnahmen gemäß § 26,

2. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,

3. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern und,

4. spezifische Verfahrensregelungen, die im Falle einer Übermittlung oder Verarbeitung für andere Zwecke, die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.

§ 15
Verarbeitung zu anderen Zwecken

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck, als demjenigen, zu dem die personenbezogenen Daten erhoben wurden, ist aufgrund von Artikel 6 Absatz 4 Satz 1 1. Halbsatz der Verordnung (EU) 2016/679 in Verbindung mit den in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 genannten Zielen zulässig, wenn

1. sie zum Schutz lebenswichtiger Interessen einer natürlichen Person erforderlich und die betroffene Person aus rechtlichen oder tatsächlichen Gründen nicht in der Lage ist, die Einwilligung zu erteilen,

2. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist;

3. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden erforderlich erscheint,

4. die Daten aus allgemein zugänglichen Quellen erhoben werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, soweit nicht schutzwürdige Interessen der betroffenen Person offensichtlich entgegenstehen

5. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der internen Revision, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient; der Zugriff auf personenbezogene Daten ist insoweit nur zulässig, als er für die Ausübung dieser Befugnisse erforderlich ist;

6. sie zu Aus- und Fortbildungszwecken erforderlich ist und schutzwürdige Belange der betroffenen Person dem nicht entgegenstehen; zu Test- und Prüfungszwecken dürfen personenbezogene Daten nicht verarbeitet werden.

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verarbeitet werden.

(2) Absatz 1 Satz 1 Nummer 2 und 3 findet keine Anwendung, wenn die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis unterliegen und sie der datenverarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden sind.

(3) In den Fällen des Absatz 1 Satz 1 Nummer 2, 3 und 5 unterbleibt abweichend von Artikel 13 Absatz 3 und Artikel 14 Absatz 4 der Verordnung (EU) 2016/679 eine Information der betroffenen Person über die Verarbeitung personenbezogener Daten, soweit und solange der Zweck der Verarbeitung gefährdet würde. Die Gründe für ein Absehen von der Information sind zu protokollieren. § 23 Absatz 3 gilt entsprechend.

(4) Sind personenbezogene Daten derart verbunden, dass ihre Trennung nach verschiedenen Zwecken auch durch Vervielfältigen und Unkenntlichmachung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, so tritt an die Stelle der Trennung ein Verwertungsverbot nach Maßgabe des Absatzes 1 für die Daten, die nicht dem Zweck der jeweiligen Verarbeitung dienen.

(5) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen nach § 14 Absatz 2 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 14 Absatz 1 vorliegen.

§ 16
Verantwortlichkeit bei der Übermittlung personenbezogener Daten

(1) Erfolgt die Übermittlung aufgrund eines Ersuchens einer öffentlichen Stelle, trägt diese die Verantwortung für die Rechtmäßigkeit der Übermittlung. Die übermittelnde Stelle hat lediglich zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden Stelle liegt. Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn im Einzelfall hierzu Anlass besteht. Die ersuchende Stelle hat in dem Ersuchen die für diese Prüfung erforderlichen Angaben zu machen.

(2) Erfolgt die Übermittlung durch ein automatisiertes Verfahren auf Abruf nach § 21, trägt die abrufende Stelle die Verantwortung für die Rechtmäßigkeit der Übermittlung. Die übermittelnde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die übermittelnde Stelle gewährleistet, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann.

Kapitel 2
Besondere Verarbeitungssituationen

§ 17
Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

(1) Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679, ist auch ohne Einwilligung für die Erfüllung einer Aufgabe zu im öffentlichen Interesse liegenden wissenschaftlichen oder historischen Forschungszwecken oder für statistische Zwecke zulässig, wenn das öffentliche Interesse an der Durchführung des Vorhabens die schutzwürdigen Belange der betroffenen Person erheblich überwiegt und der Zweck nicht auf andere Weise erreicht werden kann. Nach Satz 1 übermittelte Daten dürfen nicht für andere Zwecke verarbeitet werden.

(2) Die Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck oder dem statistischen Zweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis eine Anonymisierung erfolgt sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können; sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert. Die Daten sind zu löschen, sobald der Zweck erreicht ist. Für die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 bleibt § 14 Absatz 3 unberührt.

(3) Öffentliche Stellen, die wissenschaftliche und historische Forschung betreiben, dürfen personenbezogene Daten nur veröffentlichen, wenn

1. die betroffene Person eingewilligt hat oder

2. die Veröffentlichung für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte erforderlich ist, es sei denn, dass schutzwürdige Interessen der betroffenen Person überwiegen.

(4) Die in Artikel 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

§ 18
Verarbeitung personenbezogener Beschäftigtendaten

Verarbeiten öffentliche Stellen personenbezogene Beschäftigtendaten im Beschäftigungskontext, gelten in Ergänzung zur Verordnung (EU) 2016/679 §§ 26, 32 bis 37, 41, 43 und 44 des Bundesdatenschutzgesetzes in der jeweils geltenden Fassung entsprechend.

§ 19
Verarbeitung personenbezogener Daten zu Zwecken der freien Meinungsäußerung und der Informationsfreiheit

(1) Soweit personenbezogene Daten in Ausübung des Rechts auf freie Meinungsäußerung und Informationsfreiheit zu journalistischen, künstlerischen oder literarischen Zwecken, einschließlich der rechtmäßigen Verarbeitung aufgrund der §§ 22 und 23 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266) geändert worden ist, verarbeitet werden, gelten von Kapitel II bis VII sowie IX der Verordnung (EU) 2016/679 nur Artikel 5 Absatz 1 Buchstabe f sowie Artikel 24, 32 und 33. Artikel 82 der Verordnung (EU) 2016/679 gilt mit der Maßgabe, dass die Haftung nur Schäden umfasst, die durch eine Verletzung des Datengeheimnisses oder durch unzureichende technische oder organisatorische Maßnahmen im Sinne des Artikels 5 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 eintreten.

(2) Führt die Verarbeitung personenbezogener Daten gemäß Absatz 1 Satz 1 zur Verbreitung von Gegendarstellungen der betroffenen Person oder zu Verpflichtungserklärungen, Beschlüssen oder Urteilen über die Unterlassung der Verbreitung oder über den Widerruf des Inhalts der Daten, sind diese zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren, wie die Daten selbst, und bei einer Übermittlung der Daten gemeinsam zu übermitteln.

§ 20
Videoüberwachung

(1) Die Verarbeitung personenbezogener Daten in öffentlich zugänglichen Räumen mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen.

(2) Videoüberwachte Bereiche sind so zu kennzeichnen, dass Personen vor dem Betreten über den Umstand der Videoüberwachung sowie über den Namen und die Kontaktdaten des Verantwortlichen informiert werden.

(3) Eine Verarbeitung zu anderen Zwecken ist nur zulässig, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist.

(4) Für die Verarbeitung personenbezogener Daten aus öffentlich zugänglichen Räumen des öffentlichen Personennahverkehrs gilt abweichend von Absatz 3, dass

1. sie für einen anderen Zweck nur verarbeitet werden dürfen, soweit dies für die Verhütung oder Verfolgung von Straftaten erforderlich ist, und

2. für diesen Zweck ihre Übermittlung ausschließlich an den Polizeipräsidenten in Berlin und an die Strafverfolgungsbehörden zulässig ist.

Der Verantwortliche hat durch ein mit dem Polizeipräsidenten in Berlin abzustimmenden Sicherheitskonzept zu gewährleisten, dass Aufzeichnungen spätestens nach 48 Stunden gelöscht werden, sofern deren Speicherung nicht für einen der Zwecke des Satzes 1 Nummer 1 erforderlich ist.

(5) Unbeschadet der Verpflichtung des Verantwortlichen zur Löschung aufgrund anderer Vorschriften sind nach Absatz 1 erhobene personenbezogene Daten unverzüglich zu löschen, wenn schutzwürdige Interessen der betroffenen Person einer weiteren Speicherung entgegenstehen.

§ 21
Gemeinsames Verfahren und automatisiertes Verfahren auf Abruf

(1) Die Einrichtung eines automatisierten Verfahrens, das mehreren öffentlichen Stellen die Verarbeitung personenbezogener Daten in oder aus einem gemeinsamen Datenbestand (gemeinsames Verfahren) oder die Übermittlung an Dritte auf Abruf (automatisiertes Verfahren auf Abruf) ermöglicht, ist nur zulässig, soweit dieses Verfahren unter Berücksichtigung der Rechte und Freiheiten der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist und durch technische und organisatorische Maßnahmen Risiken für die Rechte und Freiheiten der betroffenen Personen vermieden werden können. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist vor der Einrichtung zu unterrichten. Verfahren nach Satz 1, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen beinhalten können, sind nur zulässig, wenn die Einrichtung durch Gesetz oder aufgrund eines Gesetzes zugelassen ist.

(2) Unbeschadet des Artikels 26 der Verordnung (EU) 2016/679 ist für gemeinsame Verfahren insbesondere festzulegen, welche Verfahrensweise angewendet wird und welche Stelle jeweils für die Festlegung, Änderung, Fortentwicklung und Einhaltung von fachlichen und technischen Vorgaben für das gemeinsame Verfahren verantwortlich ist.

(3) Nicht-öffentliche Stellen können sich an gemeinsamen Verfahren und automatisierten Abrufverfahren beteiligen, wenn eine Rechtsvorschrift dies zulässt und sie sich insoweit den Vorschriften dieses Gesetzes unterwerfen.

(4) Für die Einrichtung gemeinsamer Verfahren und automatisierter Abrufverfahren für verschiedene Zwecke innerhalb einer öffentlichen Stelle gelten die Absätze 1 und 2 entsprechend.

(5) Die Absätze 1 bis 4 gelten nicht für Datenbestände, die jedermann ohne oder nach besonderer Zulassung offen stehen oder deren Veröffentlichung zulässig wäre.

(6) Die Absätze 1, 3 und 5 gelten für die Zulassung regelmäßiger automatisierter Datenübermittlungen entsprechend.

§ 22
Fernmess- und Fernwirkdienste

(1) Öffentliche Stellen dürfen ferngesteuerte Messungen oder Beobachtungen (Fernmessdienste) in Wohnungen oder Geschäftsräumen nur vornehmen oder mittels einer Übertragungseinrichtung in Wohnungen oder Geschäftsräumen andere Wirkungen nur auslösen (Fernwirkdienste), wenn die betroffene Person zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes der Dienste unterrichtet worden ist und nach der Unterrichtung schriftlich oder elektronisch eingewilligt hat. Die betroffene Person kann ihre Einwilligung jederzeit widerrufen. Das Abschalten eines Dienstes gilt im Zweifel als Widerruf der Einwilligung.

(2) Die Einrichtung von Fernmess- und Fernwirkdiensten ist nur zulässig, wenn die betroffene Person erkennen kann, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist, und wenn der Teilnehmer den Dienst jederzeit abschalten kann, soweit dies mit dem Vertragszweck vereinbar ist.

(3) Eine Leistung, der Abschluss oder die Abwicklung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, dass die betroffene Person nach Absatz 1 Satz 1 einwilligt. Wird die Einwilligung verweigert oder widerrufen, dürfen der betroffenen Person keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen.

(4) Soweit im Rahmen von Fernmess- und Fernwirkdiensten personenbezogene Daten erhoben werden, dürfen diese nur zu den vereinbarten Zwecken verarbeitet werden. Artikel 7 und 8 der Verordnung (EU) 2016/679 bleiben unberührt.

Kapitel 3
Rechte der betroffenen Personen

§ 23
Informationspflicht bei Erhebung von personenbezogenen Daten

(1) Neben den in Artikel 13 Absatz 4 und Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen besteht keine Pflicht zur Information der betroffenen Person über die Erhebung ihrer personenbezogenen Daten, sofern die Erteilung der Information hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter aus zwingenden Gründen zurücktreten muss.
Ein Fall des Satzes 1 liegt insbesondere vor, wenn die Erteilung der Information

1. die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes erhebliche Nachteile bereiten würde,

2. die Verfolgung von Straftaten und Ordnungswidrigkeiten gefährden würde oder

3. dazu führen würde, dass Tatsachen, die nach einer öffentlichen Interessen dienenden Rechtsvorschrift oder zum Schutz der Rechte und Freiheiten anderer Personen geheim zu halten sind, aufgedeckt werden.

(2) Die Entscheidung über das Absehen von der Information trifft die Leitung der öffentlichen Stelle oder eine von ihr bestimmte, bei der öffentlichen Stelle beschäftigte Person. Die Gründe für ein Absehen von der Information sind zu dokumentieren und der oder dem behördlichen Datenschutzbeauftragten mitzuteilen. Der Verantwortliche ergreift auch weitere geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 13 Absatz 1 und 2 und Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache.

(3) Unterbleibt die Information in den Fällen des Absatzes 1 wegen eines vorübergehenden Hinderungsgrundes, kommt der Verantwortliche der Informationspflicht unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist ab Fortfall des Hinderungsgrundes nach, spätestens jedoch nach Ablauf von zwei Wochen.

§ 24
Auskunftsrecht der betroffenen Person

(1) Unbeschadet von § 17 Absatz 4 besteht das Recht der betroffenen Person auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 nicht, sofern die Erteilung der Auskunft hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter aus zwingenden Gründen zurücktreten muss.
Ein Fall des Satzes 1 liegt insbesondere vor, wenn die Erteilung der Auskunft

1. die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes erhebliche Nachteile bereiten würde,

2. die Verfolgung von Straftaten und Ordnungswidrigkeiten gefährden würde oder

3. dazu führen würde, dass Tatsachen, die nach einer öffentlichen Interessen dienenden Rechtsvorschrift oder zum Schutz der Rechte und Freiheiten anderer Personen geheim zu halten sind, aufgedeckt werden.

Die betroffene Person kann keine Auskunft über personenbezogene Daten verlangen, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind und deren Verarbeitung durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(2) Bezieht sich das Auskunftsersuchen auf personenbezogene Daten, die von Stellen des Verfassungsschutzes, der Gerichte, der Staatsanwaltschaft und der Polizei oder von Landesfi-

nanzbehörden, soweit diese personenbezogene Daten für Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zu Zwecken der Strafverfolgung speichern, sowie vom Bundesnachrichtendienst, des Amtes für den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, von anderen Behörden im Geschäftsbereich des für Verteidigung zuständigen Bundesministeriums übermittelt wurden, ist eine Auskunft nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt für die Erteilung einer Auskunft, die sich auf die Übermittlung personenbezogener Daten an diese Stellen bezieht. Hierfür dürfen personenbezogene Daten der betroffenen Person im erforderlichen Umfang verarbeitet werden. Die Zustimmung nach Satz 1 und 2 darf nur versagt werden, wenn dies zum Schutz der in Artikel 23 Absatz 1 Buchstabe a bis e der Verordnung (EU) 2016/679 genannten Rechtsgüter notwendig ist.

(3) Die vollständige oder teilweise Ablehnung eines Antrags auf Auskunft bedarf keiner Begründung, soweit durch die Begründung der Zweck der Ablehnung gefährdet würde. Sowohl die Entscheidung über die Ablehnung des Antrags auf Auskunft als auch die Entscheidung über das Absehen von der Begründung obliegt der Leiterin oder dem Leiter des für die Datenverarbeitung Verantwortlichen. Die Entscheidung kann an eine der Leitung unmittelbar nachgeordnete Person übertragen werden. Die Gründe der Ablehnung sind zu dokumentieren. Soweit der Antrag auf Auskunft abgelehnt wird, hat der Verantwortliche die betroffene Person darauf hinzuweisen, dass sie ihr Auskunftsrecht auch über die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit ausüben kann. Macht die betroffene Person von ihrem Recht nach Satz 3 Gebrauch, ist auf ihr Verlangen der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit die Auskunft zu erteilen, soweit nicht die jeweils zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie oder ihn stattgefunden hat. Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. Die Mitteilung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Ausnahme zugestimmt hat.

(4) Unterbleibt die Auskunft in den Fällen des Absatzes 1 wegen eines vorübergehenden Hinderungsgrundes, kommt der Verantwortliche der Auskunftspflicht unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist ab Fortfall des Hinderungsgrundes nach, spätestens jedoch nach Ablauf von zwei Wochen.

(5) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die durch eine öffentliche Stelle nicht automatisiert verarbeitet werden, besteht nur soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

(6) Sind personenbezogene Daten in Akten gespeichert, so kann die betroffene Person bei der datenverarbeitenden Stelle zusätzlich zu der Auskunft nach Artikel 15 der Verordnung (EU) 2016/679 Einsicht in die Akten verlangen. Werden die Akten nicht zur betroffenen Person geführt, so können Hinweise zum Auffinden der zur betroffenen Person gespeicherten personenbezogenen Daten gefordert werden, wenn das Auffinden auf andere Weise nicht oder nur

mit unverhältnismäßigem Aufwand möglich wäre. Die Einsichtnahme ist grundsätzlich unzulässig, wenn die Daten der betroffenen Person mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nach verschiedenen Zwecken auch durch Vervielfältigen und Unkenntlichmachung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. Im Übrigen gelten für die Verweigerung der Einsicht in die Akten die Absätze 1 bis 3 entsprechend.

(7) Der Senat legt dem Abgeordnetenhaus bis zum 30. Juni 2020 einen Bericht über die Anwendung der Absätze 1 bis 5 vor.

§ 25
Recht auf Löschung

Soweit öffentliche Stellen verpflichtet sind, Unterlagen einem öffentlichen Archiv zur Übernahme anzubieten, sind personenbezogene Daten zu löschen, wenn die Übernahme der angebotenen Unterlagen von dem öffentlichen Archiv als nicht archivwürdig abgelehnt oder wenn nach Ablauf der in § 7 Absatz 1 Satz 2 des Archivgesetzes des Landes Berlin vom 14. März 2016 (GVBl. S. 96) bestimmten Frist nach dem Angebot keine Entscheidung über die Archivwürdigkeit getroffen wurde. Soweit eine Verpflichtung nach Satz 1 besteht, tritt an die Stelle des Rechts auf Löschung nach Artikel 17 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 die Verpflichtung des Verantwortlichen, die Unterlagen unverzüglich dem öffentlichen Archiv anzubieten.

Kapitel 4
Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 26
Spezifische technische und organisatorische Maßnahmen zur Gewährleistung einer rechtmäßigen Verarbeitung

(1) Soweit die Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken, zu statistischen Zwecken oder für Verarbeitungen im Beschäftigungskontext automatisiert erfolgt oder wenn unabhängig vom Zweck in nicht geringfügigem Umfang Daten besonderer Kategorien im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 erfasst werden, hat der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung Maßnahmen zu ergreifen, die gewährleisten, dass

1. personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können,

2. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat,

3. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können und

4. bei der Bereitstellung personenbezogener Daten eine Trennung der Daten nach den jeweils verfolgten Zwecken und betroffenen Personen möglich ist.

(2) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung einer automatisierten Verarbeitung personenbezogener Daten sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse zu ermitteln und in einem Datenschutzkonzept zu dokumentieren. Entsprechend der technischen Entwicklung und bei Änderungen der mit den Verarbeitungsvorgängen verbundenen Risiken ist die Ermittlung der Maßnahmen in angemessenen Abständen zu wiederholen.

(3) Werden Systeme und Dienste, die für Verarbeitungen nach Absatz 1 genutzt werden, gewartet, so ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass nur auf die für die Wartung erforderlichen personenbezogenen Daten zugegriffen werden kann. Diese Maßnahmen müssen insbesondere Folgendes gewährleisten

1. die Wartung darf nur durch autorisiertes Personal erfolgen,

2. jeder Wartungsvorgang darf nur mit Wissen und Wollen der speichernden Stelle erfolgen,

3. die unbefugte Entfernung oder Übertragung personenbezogener Daten im Rahmen der Wartung ist zu verhindern und

4. es ist sicherzustellen, dass alle Wartungsvorgänge kontrolliert und nach der Durchführung nachvollzogen werden können.

Soweit eine Wartung durch Auftragsverarbeiter erfolgt, muss der Vertrag oder das Rechtsinstrument nach Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 Regelungen enthalten, die sicherstellen, dass der Auftragsverarbeiter keine personenbezogenen Daten, die ihm zur Kenntnis gelangen, an andere Stellen übermittelt. Die Durchführung von Wartungsarbeiten mit der Möglichkeit der Kenntniserlangung personenbezogener Daten durch Stellen außerhalb des Geltungsbereichs der Verordnung (EU) 2016/679 ist nur zulässig, wenn sie erforderlich sind und bei einer Übermittlung die Voraussetzungen des Artikels 45 oder 46 der Verordnung (EU) 2016/679 vorliegen.

§ 27
Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

Ergänzend zu Artikel 34 Absatz 3 der Verordnung (EU) 2016/679 gilt § 23 Absatz 1 für die Verpflichtung des Verantwortlichen, die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person zu benachrichtigen, entsprechend.

Kapitel 5
Sanktionen

§ 28
Geldbußen

Gegen öffentliche Stellen im Sinne des § 2 Absatz 1 und 2 sowie Stellen, die nach § 2 Absatz 3 den Bestimmungen dieses Gesetzes unterliegen, werden keine Geldbußen verhängt.

§ 29
Ordnungswidrigkeiten, Strafvorschriften

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften der Verordnung (EU) 2016/679, dieses Gesetzes sowie anderer Vorschriften über den Datenschutz personenbezogene Daten, die nicht offenkundig sind, unbefugt verarbeitet. Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50 000 Euro geahndet werden.

(2) Wer die in Absatz 1 bezeichneten Handlungen gegen Entgelt oder in der Absicht begeht, sich oder eine andere Person zu bereichern oder zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bestraft.

(3) Die Tat nach Absatz 2 wird nur auf Antrag verfolgt. Antragsberechtigt ist die betroffene Person, der Verantwortliche und die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Straf- oder Bußgeldverfahren gegen die meldepflichtige oder benachrichtigende Person oder deren in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung der meldepflichtigen oder benachrichtigenden Person verwendet werden.

Teil 3
Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680

Kapitel 1
Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

§ 30
Anwendungsbereich

(1) Die Vorschriften dieses Teils gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche.

(2) Absatz 1 findet zudem Anwendung auf diejenigen öffentlichen Stellen, die für die Vollstreckung von Strafen, von Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuches, von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes und von Geldbußen zuständig sind.

(3) Soweit Teil 3 Vorschriften für Auftragsverarbeiter enthält, gilt er auch für diese.

§ 31
Begriffsbestimmungen

Es bezeichnen die Begriffe:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann;

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte der Arbeitsleistung, der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben, der Interessen, der Zuverlässigkeit, des Verhaltens, der Aufenthaltsorte oder der Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, in der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die Daten keiner betroffenen Person zugewiesen werden können;

6. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

7. „Verantwortlicher“ die juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

8. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

9. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht; Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder anderen Rechtsvorschriften personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

10. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat, die verarbeitet wurden;

11. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern, insbesondere solche, die aus der Analyse einer biologischen Probe der Person gewonnen wurden;

12. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten;

13. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

14. „besondere Kategorien personenbezogener Daten“

    a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,

    b) genetische Daten,

    c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,

    d) Gesundheitsdaten und

    e) Daten zum Sexualleben oder zur sexuellen Orientierung;

15. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 41 der Richtlinie (EU) 2016/680 eingerichtete unabhängige staatliche Stelle;

16. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen sowie jede sonstige Einrichtung, die durch eine von zwei oder mehr Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde;

17. „Einwilligung“ jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

§ 32
Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

1. auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,

2. für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,

3. dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung darf nicht außer Verhältnis zu diesem Zweck stehen,

4. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden und

5. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

(2) Personenbezogene Daten dürfen nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht.

Kapitel 2
Rechtsgrundlagen der Verarbeitung

§ 33
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie erforderlich ist

1. zur Aufgabenerfüllung,

2. zur Wahrung lebenswichtiger Interessen einer natürlichen Person oder

3. wenn sie sich auf Daten bezieht, die von der betroffenen Person offensichtlich öffentlich gemacht wurden.

(2) Werden besondere Kategorien personenbezogener Daten verarbeitet, sind geeignete Garantien für die Rechtsgüter der betroffenen Personen vorzusehen. Geeignete Garantien können insbesondere sein

1. verbindliche Verfahrensvorschriften, die spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle festlegen,

2. die Festlegung von besonderen Aussonderungsprüffristen,

3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,

4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle,

5. die von anderen Daten getrennte Verarbeitung,

6. die Pseudonymisierung personenbezogener Daten,

7. die Verschlüsselung personenbezogener Daten oder

8. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmäßigkeit der Verarbeitung sicherstellen.

§ 34
Verarbeitung zu anderen Zwecken

Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen der in § 30 Absatz 1 und 2 genannten Zwecke handelt, der Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten, und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist. Die Verarbeitung personenbezogener Daten zu einem anderen, in § 30 Absatz 1 und 2 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

§ 35
Verarbeitung zu wissenschaftlichen, historischen, archivarischen und statistischen Zwecken

(1) Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten, ist auch ohne Einwilligung für die Erfüllung einer der in § 30 Absatz 1 und 2 genannten Aufgaben zu im öffentlichen Interesse liegenden, wissenschaftlichen oder historischen Forschungszwecken oder für archivarische oder statistische Zwecke zulässig, wenn das öffentliche Interesse an der Durchführung des Vorhabens die schutzwürdigen Belange der betroffenen Person erheblich überwiegt und der jeweilige Zweck nicht auf andere Weise erreicht werden kann. Nach Satz 1 übermittelte Daten dürfen nicht für andere Zwecke verarbeitet werden.

(2) Der Verantwortliche sieht geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vor. Die Daten sind insbesondere zu anonymisieren, sobald dies nach dem jeweiligen Zweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis eine Anonymisierung erfolgt, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der jeweilige Zweck dies erfordert. Sie sind zu löschen, sobald der jeweilige Zweck erreicht ist.

(3) Die in den §§ 41 bis 44 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Auskunftsrecht nach § 43 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(4) Diese Regelung tritt am 30. September 2025 außer Kraft.

§ 36
Einwilligung

(1) Soweit die Verarbeitung personenbezogener Daten nach einer Rechtsvorschrift auf der Grundlage einer Einwilligung erfolgen kann, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können.

(2) Erfolgt die Einwilligung der betroffenen Person durch schriftliche oder elektronische Erklärung und betrifft diese Erklärung noch andere Sachverhalte, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person ist vor Abgabe der Einwilligung hiervon in Kenntnis zu setzen.

(4) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden. Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. Die betroffene Person ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern kann.

(5) Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

§ 37
Verarbeitung auf Weisung des Verantwortlichen

Jede einem Verantwortlichen oder einem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach einer Rechtsvorschrift zur Verarbeitung verpflichtet ist.

§ 38
Datengeheimnis

Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). Sie sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort.

§ 39
Automatisierte Einzelentscheidung

(1) Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist, die geeignete Garantien für die Rechte und Freiheiten der betroffenen Person bietet, zumindest aber das Recht auf persönliches Eingreifen seitens des Verantwortlichen.

(2) Entscheidungen nach Absatz 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Personen getroffen wurden.

(3) Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten.

§ 40
Gemeinsames Verfahren und automatisiertes Verfahren auf Abruf

Die Vorschrift des § 21 findet mit der Maßgabe Anwendung, dass § 49 an die Stelle des Artikels 26 der Verordnung (EU) 2016/679 tritt. Zudem findet § 16 Absatz 2 Anwendung.

Kapitel 3
Rechte der betroffenen Person

§ 41
Allgemeine Informationen zu Datenverarbeitungen

Der Verantwortliche hat für jedermann zugänglich zumindest Informationen zur Verfügung zu stellen über

1. die Zwecke der von ihm vorgenommenen Verarbeitungen,

2. die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,

3. den Namen und die Kontaktdaten des Verantwortlichen und der oder des Datenschutzbeauftragten,

4. das Recht, die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit anzurufen und

5. die Erreichbarkeit der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit.

§ 42
Benachrichtigung betroffener Personen

(1) Ist die Benachrichtigung betroffener Personen über die Verarbeitung sie betreffender personenbezogener Daten in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet, so hat diese Benachrichtigung zumindest die folgenden Angaben zu enthalten:

1. die in § 41 genannten Angaben,

2. die Rechtsgrundlage der Verarbeitung,

3. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,

4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten, bei Übermittlungen an Empfänger in Drittländern oder internationale Organisationen auch Angaben dazu sowie

5. erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

(2) In den Fällen des Absatzes 1 kann der Verantwortliche die Benachrichtigung insoweit und solange aufschieben, einschränken oder unterlassen, wie andernfalls

1. die Erfüllung der in § 30 Absatz 1 und 2 genannten Aufgaben,

2. die öffentliche Sicherheit oder

3. Rechtsgüter Dritter

gefährdet würden, wenn das Interesse an der Vermeidung dieser Gefahren das Informationsinteresse der betroffenen Person überwiegt.

(3) Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Im Fall der Einschränkung nach Absatz 2 gilt § 43 Absatz 7 entsprechend.

§ 43
Auskunftsrecht

(1) Der Verantwortliche hat betroffenen Personen auf Antrag Auskunft darüber zu erteilen, ob er sie betreffende Daten verarbeitet. Betroffene Personen haben darüber hinaus das Recht, Informationen zu erhalten über

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und die Kategorie, zu der sie gehören,

2. die verfügbaren Informationen über die Herkunft der Daten,

3. die Zwecke der Verarbeitung und deren Rechtsgrundlage,

4. die Empfänger oder die Kategorien von Empfängern, gegenüber denen die Daten offengelegt worden sind,

5. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,

6. das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten durch den Verantwortlichen,

7. das Recht nach § 46, die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit anzurufen,

8. Angaben zur Erreichbarkeit der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit sowie

9. das Bestehen einer automatisierten Entscheidungsfindung und Informationen über die involvierte Logik.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die in der Verarbeitung eingeschränkt sind und die nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(3) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die durch eine öffentliche Stelle nicht automatisiert verarbeitet werden, besteht nur soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

(4) Der Verantwortliche kann unter den Voraussetzungen des § 42 Absatz 2 von der Auskunft nach Absatz 1 Satz 1 absehen oder die Auskunftserteilung nach Absatz 1 Satz 2 teilweise oder vollständig einschränken.

(5) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(6) Der Verantwortliche hat die betroffene Person über das Absehen von oder die Einschränkung einer Auskunft unverzüglich schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 42 Absatz 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von oder der Einschränkung der Auskunft verfolgten Zweck gefährden würde.

(7) Wird die betroffene Person nach Absatz 6 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, kann sie ihr Auskunftsrecht auch über die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie gemäß § 46 die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit anrufen oder gerichtlichen Rechtsschutz suchen kann. Macht die betroffene Person von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit zu erteilen, soweit nicht die zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie oder ihn stattgefunden hat. Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. Die Mitteilung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. Der Verantwortliche darf die Zustimmung nur insoweit und solange verweigern, wie er nach Absatz 4 von einer Auskunft absehen oder sie einschränken könnte. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

(8) Der Verantwortliche hat die sachlichen und rechtlichen Gründe für die Entscheidung zu dokumentieren.

§ 44
Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder Beurteilung. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung.

In diesem Fall hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wieder aufhebt. Die betroffene Person kann zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

(2) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender Daten zu verlangen, wenn deren Verarbeitung unzulässig ist, deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder diese zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

(3) Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigen würde,

2. die Daten zu Beweiszwecken in Verfahren, die Zwecken des § 30 Absatz 1 oder 2 dienen, weiter aufbewahrt werden müssen oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

In ihrer Verarbeitung nach Satz 1 eingeschränkte Daten dürfen nur zu dem Zweck, der ihrer Löschung entgegenstand oder sonst mit Einwilligung der betroffenen Person verarbeitet werden.

(4) Bei automatisierten Dateisystemen ist technisch sicherzustellen, dass eine Einschränkung der Verarbeitung eindeutig erkennbar ist und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung möglich ist.

(5) Hat der Verantwortliche eine Berichtigung vorgenommen, hat er der öffentlichen Stelle, die ihm die personenbezogenen Daten zuvor übermittelt hat, die Berichtigung mitzuteilen. In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1 bis 3 hat der Verantwortliche Empfängern, denen die Daten übermittelt wurden, diese Maßnahmen mitzuteilen. Die Empfänger haben die Daten in eigener Verantwortung zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken.

(6) Der Verantwortliche hat die betroffene Person über ein Absehen von der Berichtigung, Vervollständigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 42 Absatz 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde.

(7) § 43 Absatz 7 und 8 findet entsprechende Anwendung.

§ 45
Verfahren für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche hat mit betroffenen Personen unter Verwendung einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form zu kommunizieren. Unbeschadet besonderer Formvorschriften und insbesondere der Anforderungen gemäß § 50 Absatz 3 Nummer 8 soll er bei der Beantwortung von Anträgen grundsätzlich die für den Antrag gewählte Form verwenden.

(2) Bei Anträgen hat der Verantwortliche die betroffene Person unbeschadet des § 43 Absatz 6 und des § 44 Absatz 6 unverzüglich schriftlich darüber in Kenntnis zu setzen, wie verfahren wurde.

(3) Die Erteilung von Informationen nach § 41, die Benachrichtigungen nach den §§ 42 und 52 und die Bearbeitung von Anträgen nach den §§ 43 und 44 erfolgen unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 43 und 44 kann der Verantwortliche entweder eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall muss der Verantwortliche den offenkundig unbegründeten oder exzessiven Charakter des Antrags belegen können.

(4) Hat der Verantwortliche begründete Zweifel an der Identität einer betroffenen Person, die einen Antrag nach den §§ 43 oder 44 gestellt hat, soll er von ihr zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

§ 46
Anrufung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit

(1) Jede betroffene Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden, wenn sie der Auffassung ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen zu den in § 30 genannten Zwecken in ihren Rechten verletzt worden zu sein. Dies gilt nicht für die Verarbeitung von personenbezogenen Daten durch die Gerichte, soweit diese die Daten im Rahmen ihrer justiziellen Tätigkeit verarbeitet haben. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat die betroffene Person über den Stand und das Ergebnis der Beschwerde zu unterrichten und sie hierbei auf die Möglichkeit gerichtlichen Rechtsschutzes nach § 47 hinzuweisen.

(2) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat eine bei ihr oder ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer Aufsichtsbehörde des Bundes, eines anderen Landes oder in einem anderen Mitgliedstaat der Europäischen Union fällt, unverzüglich an die zuständige Aufsichtsbehörde weiterzuleiten. Sie oder er hat in diesem Fall die betroffene Person über die Weiterleitung zu unterrichten und ihr auf deren Ersuchen weitere Unterstützung zu leisten.

§ 47
Rechtsschutz gegen Entscheidungen oder bei Untätigkeit der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit

(1) Jede natürliche oder juristische Person kann unbeschadet anderer Rechtsbehelfe gerichtlich gegen eine sie betreffende verbindliche Entscheidung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit vorgehen.

(2) Absatz 1 gilt entsprechend zugunsten betroffener Personen, wenn sich die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit mit einer Beschwerde nach § 46 nicht befasst oder die betroffene Person nicht innerhalb von drei Monaten nach Einlegung der Beschwerde über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.

Kapitel 4
Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 48 Auftragsverarbeitung

(1) Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, hat der Verantwortliche für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz zu sorgen. Die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind in diesem Fall gegenüber dem Verantwortlichen geltend zu machen.

(2) Ein Verantwortlicher darf nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

(3) Auftragsverarbeiter dürfen ohne vorherige schriftliche Genehmigung des Verantwortlichen keine weiteren Auftragsverarbeiter hinzuziehen. Hat der Verantwortliche dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, hat der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung zu informieren. Der Verantwortliche kann in diesem Fall die Hinzuziehung oder Ersetzung untersagen.

(4) Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so hat er diesem dieselben Verpflichtungen aus seinem Vertrag mit dem Verantwortlichen nach Absatz 5 aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon aufgrund anderer Vorschriften verbindlich sind. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

(5) Die Verarbeitung durch einen Auftragsverarbeiter hat auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments zu erfolgen, der oder das den Auftragsverarbeiter an den Verantwortlichen bindet und der oder das den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument haben insbesondere vorzusehen, dass der Auftragsverarbeiter

1. nur auf dokumentierte Weisung des Verantwortlichen handelt; ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, hat er den Verantwortlichen unverzüglich zu informieren;

2. gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

3. den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten;

4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht;

5. dem Verantwortlichen alle erforderlichen Informationen, insbesondere die gemäß § 62 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt;

6. Überprüfungen, die von dem Verantwortlichen oder einer oder einem von diesem beauftragten Prüferin oder Prüfer durchgeführt werden, ermöglicht und dazu beiträgt;

7. die in den Absätzen 3 und 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

8. alle gemäß § 50 erforderlichen Maßnahmen ergreift und

9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in §§ 51 bis 54 und 56 genannten Pflichten unterstützt.

(6) Der Vertrag im Sinne des Absatzes 5 ist schriftlich oder elektronisch abzufassen.

(7) Die Absätze 1 bis 6 gelten entsprechend, wenn die Wartung automatisierter Verfahren durch Dritte im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(8) Ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoß gegen diese Vorschrift bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

§ 49
Gemeinsam Verantwortliche

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie als gemeinsam Verantwortliche. Gemeinsam Verantwortliche haben ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten in transparenter Form in einer Vereinbarung festzulegen, soweit diese nicht bereits in Rechtsvorschriften festgelegt sind. Aus der Vereinbarung muss insbesondere hervorgehen, wer welchen Informationspflichten nachzukommen hat und wie und gegenüber wem betroffene Personen ihre Rechte wahrnehmen können. Eine entsprechende Vereinbarung hindert die betroffene Person nicht, ihre Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend zu machen.

§ 50
Anforderungen an die Sicherheit der Datenverarbeitung

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten.

(2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

(3) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),

2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns, Löschens oder Entfernens von Datenträgern (Datenträgerkontrolle),

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),

4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),

5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),

6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),

7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),

8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),

9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit),

10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),

11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),

12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Eine geeignete Maßnahme, die zur Verwirklichung der Zwecke nach Satz 1 Nr. 2 bis 5 und 8 beiträgt, besteht in der Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

(4) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung einer automatisierten Verarbeitung personenbezogener Daten sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse zu ermitteln und in einem Datenschutzkonzept zu dokumentieren. Entsprechend der technischen Entwicklung und bei Änderungen der mit den Verarbeitungsvorgängen verbundenen Risiken ist die Ermittlung der Maßnahmen in angemessenen Abständen zu wiederholen.

(5) Werden Systeme und Dienste, die für automatisierte Verarbeitungen genutzt werden, gewartet, so ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen,

dass nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann. Diese Maßnahmen müssen insbesondere Folgendes gewährleisten

1. die Wartung darf nur durch autorisiertes Personal erfolgen,

2. jeder Wartungsvorgang darf nur mit Wissen und Wollen der speichernden Stelle erfolgen,

3. die unbefugte Entfernung oder Übertragung personenbezogener Daten im Rahmen der Wartung ist zu verhindern,

4. es ist sicherzustellen, dass alle Wartungsvorgänge kontrolliert und nach der Durchführung nachvollzogen werden können.

Soweit eine Wartung durch Auftragsverarbeiter erfolgt, muss der Vertrag oder das Rechtsinstrument nach § 48 Absatz 5 Regelungen enthalten, die sicherstellen, dass der Auftragsverarbeiter keine personenbezogenen Daten, die ihm zur Kenntnis gelangen, an andere Stellen übermittelt. Die Durchführung von Wartungsarbeiten mit der Möglichkeit der Kenntniserlangung personenbezogener Daten durch Stellen außerhalb des Geltungsbereichs der Richtlinie (EU) 2016/680 ist nur zulässig, wenn sie erforderlich sind und bei einer Übermittlung die Voraussetzungen des § 64 oder 65 vorliegen.

§ 51
Meldung von Verletzungen des Schutzes personenbezogener Daten an die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit

(1) Der Verantwortliche hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie ihm bekannt geworden ist, der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit zu melden, es sei denn, dass die Verletzung voraussichtlich zu keiner Gefahr für die Rechtsgüter natürlicher Personen führt. Erfolgt die Meldung an die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit nicht innerhalb von 72 Stunden, ist die Verzögerung zu begründen.

(2) Ein Auftragsverarbeiter hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich dem Verantwortlichen zu melden.

(3) Die Meldung nach Absatz 1 hat zumindest folgende Informationen zu enthalten:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den Kategorien und der ungefähren Anzahl der betroffenen Personen, zu den betroffenen Kategorien personenbezogener Daten und zu der ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat,

2. den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Person oder Stelle, die weitere Informationen erteilen kann,

3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

4. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung und der getroffenen Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn die Informationen nach Absatz 3 nicht zusammen mit der Meldung übermittelt werden können, hat der Verantwortliche sie unverzüglich nachzureichen, sobald sie ihm vorliegen.

(5) Der Verantwortliche hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen.

(6) Soweit von einer Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betroffen sind, die von einem oder an einen Verantwortlichen in einem anderen Mitgliedstaat der Europäischen Union übermittelt wurden, sind die in Absatz 3 genannten Informationen dem dortigen Verantwortlichen unverzüglich zu übermitteln.

(7) Weitere Pflichten des Verantwortlichen zu Benachrichtigungen über Verletzungen des Schutzes personenbezogener Daten bleiben unberührt.

§ 52
Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

(1) Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich eine erhebliche Gefahr für Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche die betroffenen Personen unverzüglich über den Vorfall zu benachrichtigen.

(2) Die Benachrichtigung nach Absatz 1 hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in § 51 Absatz 3 Nummer 2 bis 4 genannten Informationen und Maßnahmen zu enthalten.

(3) Von der Benachrichtigung nach Absatz 1 kann abgesehen werden, wenn

1. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung des Schutzes personenbezogener Daten betroffenen Daten angewandt wurden; dies gilt insbesondere für Vorkehrungen, durch die die Daten für unbefugte Personen unzugänglich gemacht wurden;

2. der Verantwortliche durch im Anschluss an die Verletzung getroffene Maßnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach keine erhebliche Gefahr im Sinne des Absatzes 1 mehr besteht, oder

3. dies mit einem unverhältnismäßigen Aufwand verbunden wäre; in diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffenen Personen über eine Verletzung des Schutzes personenbezogener Daten nicht benachrichtigt hat, kann die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit förmlich feststellen, dass ihrer oder seiner Auffassung nach die in Absatz 3 genannten Voraussetzungen nicht erfüllt sind. Hierbei hat sie oder er die Wahrscheinlichkeit zu berücksichtigen, dass die Verletzung eine erhebliche Gefahr im Sinne des Absatzes 1 zur Folge hat.

(5) Die Benachrichtigung der betroffenen Personen nach Absatz 1 kann unter den in § 42 Absatz 2 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht die Interessen der betroffenen Person aufgrund der von der Verletzung ausgehenden erheblichen Gefahr im Sinne des Absatzes 1 überwiegen.

§ 53
Durchführung einer Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen.

(2) Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohem Gefahrenpotential kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.

(3) Der Verantwortliche hat die Datenschutzbeauftragte oder den Datenschutzbeauftragten an der Durchführung der Folgenabschätzung zu beteiligen.

(4) Die Folgenabschätzung hat den Rechten der von der Verarbeitung betroffenen Personen Rechnung zu tragen und zumindest Folgendes zu enthalten:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,

2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,

3. eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und

4. die Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden soll, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden sollen.

(5) Soweit erforderlich, hat der Verantwortliche eine Überprüfung durchzuführen, ob die Verarbeitung den Maßgaben folgt, die sich aus der Folgenabschätzung ergeben haben.

§ 54
Zusammenarbeit mit der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit

Der Verantwortliche hat mit der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit bei der Erfüllung ihrer oder seiner Aufgaben zusammenzuarbeiten.

§ 55
Anhörung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit

(1) Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit anzuhören, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 53 hervorgeht, dass die Verarbeitung trotz Abhilfemaßnahmen eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hätte oder

2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hat.

Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur Anhörung nach Satz 1 unterliegen.

(2) Der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit sind im Falle des Absatzes 1 vorzulegen:

1. die nach § 53 durchgeführte Datenschutz-Folgenabschätzung,

2. gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter,

3. Angaben zu den Zwecken und Mitteln der beabsichtigten Verarbeitung,

4. Angaben zu den zum Schutz der Rechtsgüter der betroffenen Personen vorgesehenen Maßnahmen und Garantien und

5. Name und Kontaktdaten der oder des Datenschutzbeauftragten.

Auf Anforderung sind ihr oder ihm zudem alle sonstigen Informationen zu übermitteln, die sie oder er benötigt, um die Rechtmäßigkeit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Personen bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

(3) Falls die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder keine ausreichenden Abhilfemaßnahmen getroffen hat, kann sie oder er dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders komplex ist. Sie oder er hat in diesem Fall innerhalb eines Monats nach Einleitung der Anhörung den Verantwortlichen und gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung zu informieren.

(4) Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 3 Satz 1 genannten Frist beginnen. In diesem Fall sind die Empfehlungen der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit im Nachhinein zu berücksichtigen und sind die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.

§ 56
Verzeichnis von Verarbeitungstätigkeiten

(1) Der Verantwortliche hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in seine Zuständigkeit fallen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten,

2. die Zwecke der Verarbeitung,

3. die Herkunft regelmäßig empfangener personenbezogener Daten,

4. Angaben über die Rechtsgrundlage der Verarbeitung,

5. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen,

6. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,

7. gegebenenfalls die Verwendung von Profiling,

8. gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation sowie geplante Übermittlungen,

9. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten,

10. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 50 und

11. Kategorien zugriffsberechtigter Personen oder Personengruppen.

(2) Der Auftragsverarbeiter hat ein Verzeichnis aller Kategorien von Verarbeitungen zu führen, die er im Auftrag eines Verantwortlichen durchführt, das Folgendes zu enthalten hat:

1. den Namen und die Kontaktdaten des Auftragsverarbeiters, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls der oder des Datenschutzbeauftragten,

2. gegebenenfalls Übermittlungen von personenbezogenen Daten an Stellen in einem Drittstaat oder an eine internationale Organisation unter Angabe des Staates oder der Organisation und

3. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 50.

(3) Die in den Absätzen 1 und 2 genannten Verzeichnisse sind schriftlich oder elektronisch zu führen.

(4) Verantwortliche und Auftragsverarbeiter haben auf Anforderung ihre Verzeichnisse der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit zur Verfügung zu stellen.

§ 57
Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Der Verantwortliche hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen Anforderungen eingehalten und die Rechte der betroffenen Personen geschützt werden. Er hat hierbei den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen zu berücksichtigen. Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten (Datensparsamkeit). Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist.

(2) Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezoge-

nen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies betrifft die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Die Maßnahmen müssen insbesondere gewährleisten, dass die Daten durch Voreinstellungen nicht automatisiert einer unbestimmten Anzahl von Personen zugänglich gemacht werden können.

§ 58
Unterscheidung zwischen verschiedenen Kategorien betroffener Personen

Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. Dies betrifft insbesondere folgende Kategorien:

1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben,

2. Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden,

3. strafrechtlich Verurteilte,

4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und

5. andere Personen im Zusammenhang mit einer Straftat oder Personen, die mit den in den Nummern 1 bis 3 genannten Personen in Kontakt oder in Verbindung stehen.

§ 59
Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen

Der Verantwortliche hat bei der Verarbeitung so weit wie möglich danach zu unterscheiden, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. Zu diesem Zweck soll er, soweit dies im Rahmen der jeweiligen Verarbeitung möglich und angemessen ist, Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich machen. Es muss außerdem feststellbar sein, welche Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Beurteilung zugrunde liegen.

§ 60
Verfahren bei Übermittlungen

(1) Der Verantwortliche hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht übermittelt oder sonst zur Verfügung gestellt werden. Zu diesem Zweck hat er, soweit dies mit angemes-

senem Aufwand möglich ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. Bei jeder Übermittlung personenbezogener Daten hat er zudem, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.

(2) Gelten für die Verarbeitung von personenbezogenen Daten besondere Bedingungen, so hat bei Datenübermittlungen die übermittelnde Stelle den Empfänger auf diese Bedingungen und die Pflicht zu ihrer Beachtung hinzuweisen. Die Hinweispflicht kann dadurch erfüllt werden, dass die Daten entsprechend markiert werden.

(3) Die übermittelnde Stelle darf auf Empfänger in anderen Mitgliedstaaten der Europäischen Union und auf Einrichtungen und sonstige Stellen, die nach den Kapiteln 4 und 5 des Titels V des Dritten Teils des Vertrags über die Arbeitsweise der Europäischen Union errichtet wurden, keine Bedingungen anwenden, die nicht auch für entsprechende innerstaatliche Datenübermittlungen gelten.

§ 61
Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung

(1) Der Verantwortliche hat personenbezogene Daten zu berichtigen, wenn sie unrichtig sind und unvollständige Daten zu vervollständigen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

(2) Der Verantwortliche hat personenbezogene Daten unverzüglich zu löschen, wenn ihre Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist.

(3) § 44 Absatz 3 bis 5 ist entsprechend anzuwenden. Sind unrichtige personenbezogene Daten oder personenbezogene Daten unrechtmäßig übermittelt worden, ist auch dies dem Empfänger mitzuteilen.

(4) Unbeschadet von in Rechtsvorschriften festgesetzten Höchstspeicher- oder Löschfristen hat der Verantwortliche für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

§ 62
Protokollierung

(1) In automatisierten Verarbeitungssystemen haben Verantwortliche und Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge zu protokollieren:

1. Erhebung,

2. Veränderung,

3. Abfrage,

4. Offenlegung einschließlich Übermittlung,

5. Kombination und

6. Löschung.

(2) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen.

(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten, die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit und die betroffene Person sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.

(4) Die Protokolldaten sind nach Ablauf von zwei Jahren seit ihrer Erstellung zu löschen.

(5) Der Verantwortliche und der Auftragsverarbeiter haben die Protokolle der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit auf Anforderung zur Verfügung zu stellen.

§ 63
Vertrauliche Meldung von Verstößen

Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können.

Kapitel 5
Datenübermittlungen an Drittstaaten und an internationale Organisationen

§ 64
Allgemeine Voraussetzungen

(1) Die Übermittlung personenbezogener Daten an Stellen in Drittstaaten oder an internationale Organisationen ist bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen zulässig, wenn

1. die Stelle oder internationale Organisation für die in § 30 Absatz 1 und 2 genannten Zwecke zuständig ist und

2. die Europäische Kommission gemäß Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat.

(2) Die Übermittlung personenbezogener Daten hat trotz des Vorliegens eines Angemessenheitsbeschlusses im Sinne des Absatzes 1 Nummer 2 und des zu berücksichtigenden öffentlichen Interesses an der Datenübermittlung zu unterbleiben, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegende schutzwürdige Interessen einer betroffenen Person entgegenstehen. Bei seiner Beurteilung hat der Verantwortliche maßgeblich zu berücksichtigen, ob der Empfänger im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert.

(3) Wenn personenbezogene Daten, die aus einem anderen Mitgliedstaat der Europäischen Union übermittelt oder zur Verfügung gestellt wurden, nach Absatz 1 übermittelt werden sollen, muss diese Übermittlung zuvor von der zuständigen Stelle des anderen Mitgliedstaats genehmigt werden. Übermittlungen ohne vorherige Genehmigung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Staates oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Im Fall des Satzes 2 ist die Stelle des anderen Mitgliedstaats, die für die Erteilung der Genehmigung zuständig gewesen wäre, unverzüglich über die Übermittlung zu unterrichten.

(4) Der Verantwortliche, der Daten nach Absatz 1 übermittelt, hat durch geeignete Maßnahmen sicherzustellen, dass der Empfänger die übermittelten Daten nur dann an andere Drittstaaten oder andere internationale Organisationen weiterübermittelt, wenn der Verantwortliche diese Übermittlung zuvor genehmigt hat. Bei der Entscheidung über die Erteilung der Genehmigung hat der Verantwortliche alle maßgeblichen Faktoren zu berücksichtigen, insbesondere die Schwere der Straftat, den Zweck der ursprünglichen Übermittlung und das in dem Drittstaat oder der internationalen Organisation, an das oder an die die Daten weiterübermittelt werden sollen, bestehende Schutzniveau für personenbezogene Daten. Eine Genehmigung darf nur dann erfolgen, wenn auch eine direkte Übermittlung an den anderen Drittstaat oder die andere internationale Organisation zulässig wäre. Die Zuständigkeit für die Erteilung der Genehmigung kann auch abweichend geregelt werden.

§ 65
Datenübermittlung bei geeigneten Garantien

(1) Liegt entgegen § 64 Absatz 1 Nummer 2 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 64 auch dann zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder

2. der Verantwortliche nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, zu der Auffassung gelangt ist, dass geeignete Garantien für den Schutz personenbezogener Daten bestehen.

(2) Der Verantwortliche hat Übermittlungen nach Absatz 1 Nummer 2 zu dokumentieren. Die Dokumentation hat den Zeitpunkt der Übermittlung, die Identität des Empfängers, den Grund der Übermittlung und die übermittelten personenbezogenen Daten zu enthalten. Sie ist der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit auf Anforderung zur Verfügung zu stellen.

(3) Der Verantwortliche hat die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit jährlich über Übermittlungen zu unterrichten, die aufgrund einer Beurteilung nach Absatz 1 Nummer 2 erfolgt sind. In der Unterrichtung kann er die Empfänger und die Übermittlungszwecke angemessen kategorisieren.

§ 66
Datenübermittlung ohne geeignete Garantien

(1) Liegt entgegen § 64 Absatz 1 Nummer 2 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 65 Absatz 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 64 auch dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,

2. zur Wahrung berechtigter Interessen der betroffenen Person,

3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,

4. im Einzelfall für die in § 30 genannten Zwecke oder

5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 30 genannten Zwecken.

(2) Der Verantwortliche hat von einer Übermittlung nach Absatz 1 abzusehen, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

(3) Für Übermittlungen nach Absatz 1 gilt § 65 Absatz 2 und 3 entsprechend.

§ 67
Sonstige Datenübermittlung an Empfänger in Drittstaaten

(1) Der Verantwortliche kann bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 64 Absatz 1 Nummer 1 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung seiner Aufgaben erforderlich ist und

1. im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,

2. er die Übermittlung an die in § 64 Absatz 1 Nummer 1 genannten Stellen für wirkungslos oder ungeeignet hält, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und

3. er dem Empfänger die Zwecke der Verarbeitung mitteilt und ihn darauf hinweist, dass die übermittelten Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihre Verarbeitung für diese Zwecke erforderlich ist.

(2) Im Fall des Absatzes 1 hat der Verantwortliche die in § 64 Absatz 1 Nummer 1 genannten Behörden unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für Übermittlungen nach Absatz 1 gilt § 65 Absatz 2 und 3 entsprechend.

(4) Bei Übermittlungen nach Absatz 1 hat der Verantwortliche den Empfänger zu verpflichten, die übermittelten personenbezogenen Daten nur für den Zweck zu verarbeiten, für den sie übermittelt worden sind.

(5) Abkommen im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit bleiben unberührt.

Kapitel 6
Zusammenarbeit der Aufsichtsbehörden

§ 68
Gegenseitige Amtshilfe

(1) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat den Datenschutzaufsichtsbehörden des Bundes und der Länder sowie in den anderen Mitgliedstaaten der Europäischen Union Informationen zu übermitteln und Amtshilfe zu leisten, soweit dies für eine einheitliche Umsetzung und Anwendung der Richtlinie (EU) 2016/680 erforderlich ist. Die Amtshilfe betrifft insbesondere Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

(2) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat alle geeigneten Maßnahmen zu ergreifen, um Amtshilfeersuchen unverzüglich und spätestens innerhalb eines Monats nach deren Eingang nachzukommen.

(3) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit darf Amtshilfeersuchen nur ablehnen, wenn

1. sie oder er für den Gegenstand des Ersuchens oder für die Maßnahmen, die sie oder er durchführen soll, nicht zuständig ist oder

2. ein Eingehen auf das Ersuchen gegen Rechtsvorschriften verstoßen würde.

(4) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat die ersuchende Aufsichtsbehörde des anderen Staates über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen zu informieren, die getroffen wurden, um dem Amtshilfeersuchen nachzukommen. Sie oder er hat im Fall des Absatzes 3 die Gründe für die Ablehnung des Ersuchens zu erläutern.

(5) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat die Informationen, um die sie oder er von der Aufsichtsbehörde des anderen Staates ersucht wurde, in der Regel elektronisch und in einem standardisierten Format zu übermitteln.

(6) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat Amtshilfeersuchen kostenfrei zu erledigen, soweit sie oder er nicht im Einzelfall mit der Aufsichtsbehörde des Bundes, des jeweiligen Landes oder des anderen Mitgliedstaates der Europäischen Union die Erstattung entstandener Ausgaben vereinbart hat.

(7) Ein Amtshilfeersuchen der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit hat alle erforderlichen Informationen zu enthalten; hierzu gehören insbesondere der Zweck und die Begründung des Ersuchens. Die auf das Ersuchen übermittelten Informationen dürfen ausschließlich zu dem Zweck verwendet werden, zu dem sie angefordert wurden.

Kapitel 7
Haftung und Sanktionen

§ 69
Schadensersatz und Entschädigung

(1) Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nach einer nach Maßgabe der Richtlinie (EU) 2016/680 erlassenen Vorschrift rechtswidrig war, einen Schaden zugefügt, ist er oder sein Rechtsträger der betroffenen Person zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit bei einer nichtautomatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist.

(2) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(3) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welcher von mehreren beteiligten Verantwortlichen den Schaden verursacht hat, so haftet jeder Verantwortliche beziehungsweise sein Rechtsträger.

(4) Hat bei der Entstehung des Schadens ein Verschulden der betroffenen Person mitgewirkt, ist § 254 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden.

(5) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

§ 70
Ordnungswidrigkeiten, Strafvorschriften

Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von Tätigkeiten nach § 30 Absatz 1 Satz 1, 3 oder Absatz 2 findet § 29 entsprechende Anwendung.

Teil 4

Besondere Verarbeitungssituationen außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680

§ 71
Öffentliche Auszeichnungen und Ehrungen

(1) Zur Vorbereitung und Durchführung öffentlicher Auszeichnungen oder Ehrungen dürfen die zuständigen Stellen sowie die von ihnen besonders beauftragten Stellen die dazu erforderlichen personenbezogenen Daten einschließlich besonderer Kategorien personenbezogener Daten auch ohne Kenntnis der betroffenen Person verarbeiten. Die Verarbeitung dieser Daten für andere Zwecke ist nur mit Einwilligung der betroffenen Person zulässig.

(2) Auf Anforderung der in Absatz 1 genannten Stellen dürfen andere öffentliche Stellen die zur Vorbereitung der Auszeichnung oder Ehrung erforderlichen Daten übermitteln.

(3) Die Artikel 13, 14, 15 und 19 der Verordnung (EU) 2016/679 sind nicht anzuwenden.

Teil 5
Schlussvorschrift

§ 72
Übergangsvorschriften

(1) Vor dem 6. Mai 2016 eingerichtete automatisierte Verarbeitungssysteme sind in Ausnahmefällen, in denen dies mit einem unverhältnismäßigen Aufwand verbunden ist, spätestens bis zum 6. Mai 2023 mit § 62 Absatz 1 und 2 in Einklang zu bringen.

(2) Die oder der zum Zeitpunkt des Inkrafttretens dieses Gesetzes im Amt befindliche Berliner Beauftragte für Datenschutz und Informationsfreiheit gilt als nach § 9 Absatz 1 Satz 1 ernannt. Ihre oder seine statusrechtliche Stellung bleibt unberührt. Die Amtszeit gilt nach § 9 Absatz 3 Satz 1 als zum 28. Januar 2016 begonnen. Der Aushändigung einer Ernennungsurkunde bedarf es nicht.

Artikel 2

Änderung des Gesetzes über den Verfassungsschutz in Berlin

Das Gesetz über den Verfassungsschutz in Berlin (Verfassungsschutzgesetz Berlin-VSG Berlin) in der Fassung vom 25. Juni 2001, zuletzt geändert durch Gesetz vom 1. Dezember 2010 (GVBl., S. 534), wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach § 32 folgende Angabe eingefügt:

„§ 32a Unabhängige Datenschutzkontrolle“

2. § 2 Absatz 2 Satz 1 wird wie folgt gefasst:

„Die für den Verfassungsschutz zuständige Abteilung ist Verantwortlicher im Sinne des § 31 Nr. 7 des Berliner Datenschutzgesetzes in der Fassung vom [...].

3. § 8 Absatz 1 Satz 1 wird wie folgt geändert:

„Die Verfassungsschutzbehörde darf die zur Erfüllung ihrer Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten verarbeiten und bei öffentlichen und nichtöffentlichen Stellen, insbesondere bei Privatpersonen, erheben, soweit nicht die anzuwendenden Bestimmungen des Berliner Datenschutzgesetzes oder besondere Regelungen in diesem Gesetz entgegenstehen; die Verarbeitung ist auch zulässig, wenn die betroffene Person eingewilligt hat.“

4. § 8 Absatz 2 Satz 2 Nummer 10 wird wie folgt geändert:

„10. Überwachung des Brief-, Post-, und Fernmeldeverkehrs nach Maßgabe des Art. 10-Gesetzes, vom 26. Juni 2001 (BGBl. I S. 1254, 2298), zuletzt geändert durch Art. 12 des Gesetzes vom 14. August 2017 (BGBl. I S. 3202),“

5. § 11 wird wie folgt geändert:

In der Überschrift wird das Wort „Informationen“ durch das Wort „Daten“ ersetzt.

6. § 12 wird wie folgt geändert:

a. In der Überschrift wird das Wort „Informationen“ durch das Wort „Daten“ ersetzt.

b. In § 12 wird das Wort „Informationen“ durch das Wort „Daten“ ersetzt.

7. § 14 wird wie folgt geändert:

a. Die Überschrift wird wie folgt gefasst:
„§ 14 Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten in Dateien“

b. In Absatz 1 wird das Wort „Informationen“ durch das Wort „Daten“ ersetzt.

c. Absatz 3 wird wie folgt neu gefasst:

„(3) Die Verfassungsschutzbehörde hat die Verarbeitung von in Dateien gespeicherten personenbezogenen Daten einzuschränken, wenn die Löschung unterbleibt, weil Grund zur Annahme besteht, dass durch die Löschung schutzwürdige Interessen der betroffenen Personen beeinträchtig würden. In der Verarbeitung eingeschränkte Daten sind entsprechend zu kennzeichnen und dürfen nur mit Einwilligung der betroffenen Person verwendet werden.“

d. Absatz 4 Satz 1 wird wie folgt neu gefasst:

„Die Verarbeitung von in Dateien gelöschten Informationen ist eingeschränkt.“

e. In Absatz 5 Satz 1 wird das Wort „Informationen“ durch das Wort „Daten“ ersetzt.

8. § 15 wird wie folgt geändert:

a. Die Überschrift wird wie folgt neu gefasst:

„§ 15
Berichtigung und Einschränkung der Verarbeitung personenbezogener Daten in Akten“

b. In Absatz 1 wird das Wort „Informationen“ durch das Wort „Daten“ ersetzt.

c. Absatz 2 wird wie folgt neu gefasst:

„(2) Die Verfassungsschutzbehörde hat die Verarbeitung von personenbezogenen Daten in Akten einzuschränken, wenn sie im Einzelfall feststellt, dass ohne die Einschränkung schutzwürdige Interessen von betroffenen Personen beeinträchtigt würden und die Daten für ihre Aufgabenerfüllung nicht mehr erforderlich sind. In der Verarbeitung eingeschränkte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nicht mehr genutzt oder übermittelt werden. Eine Aufhebung der Einschränkung ist möglich, wenn ihre Voraussetzungen nachträglich entfallen.“

9. § 16 wird wie folgt geändert:

a. In Absatz 1 werden die Wörter „dem Berliner Beauftragten für den Datenschutz und für das Recht auf Akteneinsicht“ durch die Wörter „der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit“ ersetzt.

b. Dem § 16 Absatz 1 wird folgender Satz angefügt:

„Die Verfassungsschutzbehörde führt ein Verzeichnis der geltenden Dateianordnungen.“

10. In § 18 Satz 1 ist das Wort „Informationen“ durch das Wort „Daten“ zu ersetzen.

11. § 22 wird wie folgt geändert:

a. In Absatz 2 wird das Wort „Information“ durch das Wort „Daten“ ersetzt.

b. In Absatz 3 wird das Wort „Informationen“ durch das Wort „Daten“ ersetzt.

12. § 23 wird wie folgt geändert:

a. In Satz 1 wird das Wort „Information“ durch das Wort „Daten“ ersetzt.

b. In Satz 3 wird das Wort „Information“ durch das Wort „Daten“ ersetzt.

c. In Satz 5 wird das Wort „Information“ durch das Wort „Daten“ ersetzt.

13. In § 24 wird das Wort „Information“ durch das Wort „Daten“ ersetzt.

14. § 25 wird wie folgt geändert:

a. In Satz 1 wird das Wort „Information“ durch das Wort „Daten“ ersetzt.

b. In Satz 5 wird das Wort „Information“ durch das Wort „Daten“ ersetzt.

15. In § 26 Satz 1 wird das Wort „Information“ durch das Wort „Daten“ ersetzt.

16. § 27 wird wie folgt geändert:

a. In Absatz 4 Satz 1 wird das Wort „Information“ durch das Wort „Daten“ ersetzt.

b. Absatz 6 Satz 3 wird wie folgt neu gefasst:

„Die Vernichtung unterbleibt, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unvertretbarem Aufwand erfolgen kann; in diesem Fall ist die Verarbeitung solcher Informationen eingeschränkt und entsprechend zu kennzeichnen.“

17. § 31 wird wie folgt geändert:

a. In Absatz 4 werden jeweils die Wörter „den“ bzw. „Dem“ bzw. „des“ durch die Wörter „die oder den“ bzw. „Der oder dem“ bzw. „der oder des“ und die Wörter „Berliner Beauftragten für den Datenschutz und das Recht auf Akteneinsicht“ durch die Wörter „Berliner Beauftragten für Datenschutz und Informationsfreiheit“ ersetzt.

b. In Absatz 4 wird der Satz 4 gestrichen.

18. Nach § 32 wird folgender § 32a eingefügt:

„§ 32a
Unabhängige Datenschutzkontrolle

(1) Jede Person kann sich an die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer **personenbezogenen** Daten durch die Verfassungsschutzbehörde in ihren Rechten verletzt worden zu sein.

(2) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kontrolliert bei der Verfassungsschutzbehörde die Einhaltung der Vorschriften über den Datenschutz. Soweit die Einhaltung von Vorschriften der Kontrolle durch die Kommission nach § 2 des Gesetzes zur Ausführung des Gesetzes zu Art. 10 Grundgesetz unterliegt, unterliegt sie nicht der Kontrolle durch die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit, es sei denn, die Kommission ersucht die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

(3) Die Verfassungsschutzbehörde ist verpflichtet, die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit und ihre oder seine schriftlich besonders Beauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Den in Satz 1 genannten Personen ist dabei insbesondere
1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 2 stehen.
2. jederzeit Zutritt zu allen Diensträumen zu gewähren.
Dies gilt nicht, soweit das für Inneres zuständige Mitglied des Senats im Einzelfall feststellt, dass durch die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährdet würde.

(4) Die Absätze 1 bis 3 gelten ohne Beschränkung auf die Erfüllung der Aufgaben nach § 5. Sie gelten entsprechend für die Verarbeitung personenbezogener Daten durch andere Stellen, wenn diese der Erfüllung der Aufgaben der Verfassungsschutzbehörde nach § 5 dient. § 13 Absatz 1 und 4 des Berliner Datenschutzgesetzes findet in diesen Fällen keine Anwendung.“

19. § 38 wird wie folgt neu gefasst:

„§ 38

Anwendbarkeit des Berliner Datenschutzgesetzes

Bei der Erfüllung der Aufgaben nach § 5 durch die Verfassungsschutzbehörde sind neben den Bestimmungen des Teils 1 die §§ 31 und 36 Absatz 1 bis 4 und die §§ 37 bis 39, 48, 50, 69 und 70 des Berliner Datenschutzgesetzes entsprechend anzuwenden. § 2 Absatz 9 und § 13 Absatz 1 und 4 des Berliner Datenschutzgesetzes finden keine Anwendung.“

20. § 39 wird wie folgt neu gefasst:

„§ 39
Inkrafttreten, Außerkrafttreten

Dieses Gesetz tritt am Tage nach der Verkündung im Gesetz- und Verordnungsblatt für Berlin in Kraft. § 27a tritt außer Kraft, sobald das Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Artikel 2 Absatz 1 des Gesetzes vom 16. Juni 2017 (BGBl. I S. 1634) wieder in seiner am 31. Dezember 2001 maßgeblichen Fassung gilt. Der Tag des Außerkrafttretens ist im Gesetz- und Verordnungsblatt für Berlin bekannt zu machen.“

Artikel 3

Änderung des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen im Land Berlin

Das Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen im Land Berlin (Berliner Sicherheitsüberprüfungsgesetz-BSÜG) in der Fassung vom 25. Juni 2001, das zuletzt durch Artikel II des Gesetzes vom 06.07.2006 (GVBl. S. 711) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a. Die Angabe zu § 23 wird wie folgt gefasst:
„§ 23 Berichtigen, Löschen und Einschränkung der Verarbeitung personenbezogener Daten."

b. Nach der Angabe zu § 33 wird folgende Angabe eingefügt:
„§ 33a Anwendung des Berliner Datenschutzgesetzes"

c. Nach der Angabe zu § 33a wird folgende Angabe eingefügt:
„§ 33b Unabhängige Datenschutzkontrolle"

2. § 23 wird wie folgt geändert:

a. In der Überschrift wird das Wort „Sperren" durch „Einschränkung der Verarbeitung" ersetzt.

b. Absatz 1 wird Satz 3 wie folgt gefasst:

„Informationen in Dateien, deren Verarbeitung eingeschränkt ist, sind entsprechend zu kennzeichnen."

3. § 24 wird wie folgt geändert:

a. In Absatz 4 Satz 3 werden die Wörter „den Berliner Beauftragten für Datenschutz und für das Recht auf Akteneinsicht" durch die Wörter „die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit" ersetzt.

b. In Absatz 6 werden die Wörter „vom Berliner Beauftragten für Datenschutz und für das Recht auf Akteneinsicht" durch die Wörter „von der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit" und die Wörter „die Verfassungsschutzbehörde" durch die Wörter „das für Inneres zuständige Mitglied des Senats" ersetzt.

c. Absatz 7 wird gestrichen.

4. Nach § 33 wird folgender § 33a eingefügt:

„§ 33a

Anwendung des Berliner Datenschutzgesetzes

Die Vorschriften des Berliner Datenschutzgesetzes finden wie folgt Anwendung:

1. § 2 Absatz 9 und § 13 Absatz 1 und Absatz 4 finden keine Anwendung,

2. § 31, § 36 Absatz 1 und 3, die §§ 37 bis 39, 48, 50, 69, 70 sind entsprechend anzuwenden.“

5. Nach § 33a wird folgender § 33b eingefügt:

„§ 33b
Unabhängige Datenschutzkontrolle

(1) Jede Person kann sich an die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten nach diesem Gesetz durch öffentliche oder nichtöffentliche Stellen in ihren Rechten verletzt worden zu sein.

(2) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kontrolliert bei den öffentlichen und den nichtöffentlichen Stellen die Einhaltung der anzuwendenden Vorschriften über den Datenschutz bei der Erfüllung der Aufgaben dieses Gesetzes. Soweit die Einhaltung von Vorschriften der Kontrolle durch die Kommission nach § 2 des Gesetzes zur Ausführung des Gesetzes zu Art. 10 Grundgesetz unterliegt, unterliegt diese nicht der Kontrolle durch die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit, es sei denn, die Kommission ersucht die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. Der Kontrolle durch die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit unterliegen auch nicht personenbezogene Daten in Akten über die Sicherheitsüberprüfung, wenn die betroffene Person der Kontrolle der auf sie bezogenen Daten im Einzelfall gegenüber der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit widerspricht.

(3) Die öffentlichen und nicht öffentlichen Stellen sind verpflichtet, die oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit und ihre oder seine schriftlich besonders Beauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Den in Satz 1 genannten Personen ist dabei insbesondere
1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 2 stehen.
2. jederzeit Zutritt zu allen Diensträumen zu gewähren.
§ 24 Absatz 6 gilt entsprechend.“

Artikel 4
Inkraftreten, Außerkrafttreten

Dieses Gesetz tritt am 25. Mai 2018 in Kraft. Gleichzeitig tritt das Berliner Datenschutzgesetz in der Fassung der Bekanntmachung vom 17. Dezember 1990 (GVBl. 1991, S. 16, 54), das zuletzt durch Artikel 8 des Gesetzes vom 30. Mai 2016 (GVBl. S. 282) geändert worden ist, außer Kraft.

A. Begründung - Allgemeiner Teil

Am 25. Mai 2018 wird die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119/1 vom 4.5.2016, S. 1) (Datenschutz-Grundverordnung, nachfolgend Verordnung (EU) 2016/679) unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union.
Ziel des europäischen Gesetzgebers, für dessen Umsetzung die Form einer Verordnung gewählt wurde, ist ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen und die Beseitigung von Hemmnissen für den Verkehr personenbezogener Daten innerhalb der gesamten Union (Erwägungsgründe 10 und 13 der Verordnung (EU) 2016/679).
Gemäß Artikel 288 des Vertrages über die Arbeitsweise der Europäischen Union (nachfolgend AEUV) gelten EU-Verordnungen unmittelbar und bedürfen keiner Umsetzung in das mitgliedstaatliche Recht. Nichtsdestotrotz enthält die Verordnung (EU) 2016/679 Öffnungsklauseln für den nationalen Gesetzgeber mit Regelungsoptionen und konkreten Regelungsaufträgen, damit das allgemeine und das bereichsspezifische Datenschutzrecht soweit wie nötig angepasst werden kann.
Der sich ergebende Anpassungsbedarf im allgemeinen Datenschutzrecht soll mit einer Neufassung des Berliner Datenschutzgesetzes umgesetzt werden. Hierzu dürfen Wiederholungen von Regelungen der Verordnung (EU) 2016/679 im nationalen Recht nur insoweit erfolgen, als diese im Falle von Präzisierungen oder Einschränkungen von Regelungen der Verordnung (EU) 2016/679 durch das nationale Recht erforderlich sind, um die Kohärenz zu wahren und die Vorschriften des nationalen Rechts für die Personen, für die sie gelten, verständlicher zu machen (Erwägungsgrund 8 der Verordnung (EU) 2016/679).
Vom Anwendungsbereich der Verordnung (EU) 2016/679 nicht umfasst ist unter anderem die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (Artikel 2 Absatz 2 Buchstabe d der Verordnung (EU) 2016/679).
Für die Verarbeitung personenbezogener Daten zu diesen Zwecken wurde die Richtlinie des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119/89 vom 4.5.2016, S. 89) (nachfolgend Richtlinie (EU) 2016/680) erlassen, die gemäß ihrem Artikel 63 Absatz 1 bis zum 6. Mai 2018 von den Mitgliedstaaten in nationales Recht umzusetzen ist.
Aufgrund der mit dem Erlass der Verordnung (EU) 2016/679 grundlegenden strukturellen Änderung des im Bereich des Rechts auf informationelle Selbstbestimmung und Privatsphäre anwendbaren Datenschutzrechts und durch die erforderliche Umsetzung der Richtlinie (EU) 2016/680 würde eine bloße Änderung des Berliner Datenschutzgesetzes nicht genügen. Mit der Neufassung soll der Systemwechsel im Datenschutzrecht durch das Inkrafttreten der Verordnung (EU) 2016/679 und der Auftrag zur Umsetzung der strukturell ähnlichen Richtlinie (EU) 2016/680 vollzogen werden.

Weder vom Anwendungsbereich der Verordnung (EU) 2016/679 noch der Richtlinie (EU) 2016/680 umfasst ist die Tätigkeit öffentlicher Stellen zu Zwecken der nationalen Sicherheit. Dies ergibt sich aus Artikel 4 Absatz 2 Satz 3 des Vertrages über die Europäische Union (EUV) und ist auch sekundärrechtlich klargestellt, siehe Artikel 2 Absatz 2 Buchstabe a

i.V.m. Erwägungsgrund 16 der Verordnung (EU) 2016/679 sowie Artikel 2 Absatz 3 Buchstabe a i.V.m. Erwägungsgrund 14 der Richtlinie (EU) 2016/680 (siehe auch BT-Drs. 18/11325 S. 74, 79). Im Land Berlin betrifft dies die Datenverarbeitung zu Zwecken des Verfassungsschutzes und nach dem Sicherheitsüberprüfungsgesetz. Damit für diese Tätigkeiten gleichwohl ein der bisherigen Rechtslage entsprechender notwendiger Bestand an allgemeinen Datenschutzbestimmungen erhalten bleibt, müssen zeitgleich mit dem Inkrafttreten des neu gefassten Berliner Datenschutzgesetzes auch Änderungen in den Verweisungsnormen des Berliner Verfassungsschutzgesetzes und des Berliner Sicherheitsüberprüfungsgesetzes vorgenommen werden. Dies geht einher mit zusätzlichem gesetzlichen Änderungsbedarf in den beiden bereichsspezifischen Gesetzen, die den Erfordernissen der außerhalb des Anwendungsbereichs des Unionsrechts fallenden Datenverarbeitungen im Bereich der nationalen Sicherheit Rechnung tragen. Durch die Orientierung an den im Zuge der Umsetzung der EU-Datenschutzreform geänderten Bestimmungen des Bundesverfassungsschutzgesetzes und des Sicherheitsüberprüfungsgesetzes des Bundes (BT-Drs. 18/11325) wird zugleich sichergestellt, dass es nicht zu Problemen bei der länderübergreifenden nachrichtendienstlichen Zusammenarbeit, insbesondere bei der arbeitsteiligen Speicherung relevanter Informationen in einem einheitlichen Informationsverbund, aufgrund unterschiedlicher Datenverarbeitungsbestimmungen kommt.

B. Begründung - Besonderer Teil

Zu Artikel 1
Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz - BlnDSG)

Zu Teil 1 Gemeinsame Bestimmungen

Zu Kapitel 1 Allgemeine Bestimmungen

Zu § 1 Zweck

Die Vorschrift dient der Klarstellung des Regelungsgegenstandes. Wegen des Bezuges zu unterschiedlichen Rechtsakten der Europäischen Union sowie davon unabhängiger Regelungen in den verschiedenen Teilen des Gesetzes, wird in Absatz 1 vorangestellt, dass im Berliner Datenschutzgesetz Durchführungsregelungen in Ergänzung zur unmittelbar geltenden Verordnung (EU) 2016/679 getroffen werden, in Absatz 2, dass auch die Umsetzung der Richtlinie (EU) 2016/680 im Berliner Datenschutzgesetz vorgenommen wird und in Absatz 3, dass auch andere, von den Absätzen 1 und 2 nicht erfasste Fälle der Verarbeitung personenbezogener Daten in den Regelungsbereich des Berliner Datenschutzgesetzes fallen.

Zu § 2 Anwendungsbereich

Zu Absatz 1
Wie im bisherigen Berliner Datenschutzgesetz soll das Berliner Datenschutzgesetz für alle Behörden und sonstige öffentliche Stellen des Landes Berlin, einschließlich der Gerichte, so-

wie für die landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts im Sinne des § 28 des Allgemeinen Zuständigkeitsgesetzes gelten. Zugleich wird der Begriff öffentliche Stellen definiert.

Die Verordnung (EU) 2016/679 und die in Umsetzung der Richtlinie (EU) 2016/680 erlassenen Vorschriften gelten auch für Gerichte. Mit der Aufsicht über justizielle Tätigkeit sollen allerdings besondere Stellen in der Justiz betraut werden.
Nach Artikel 55 Absatz 3 der Verordnung (EU) 2016/679 sind die Aufsichtsbehörden nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen personenbezogener Daten. Nach dem Erwägungsgrund 20 der Verordnung (EU) 2016/679 soll die Unabhängigkeit der Justiz bei der Ausübung der rechtsprechenden Tätigkeit einschließlich ihrer Beschlussfassung unangetastet bleiben. Daraus ergibt sich im Umkehrschluss, dass die Verordnung (EU) 2016/679 auch für justizielle Tätigkeiten gilt und lediglich eine besondere Aufsichtsorganisation erwartet wird (so auch BeckOK DatenschutzR/Eichler DS-GVO Art. 55 Rn. 11 m.w.N.). Dies gilt auch für den Rechnungshof (so auch Körffer in Paal/Pauly, DS-.-Grundverordnung, 1. Auflage 2017, Art. 55 Rn. 8) im Rahmen seiner unabhängigen Tätigkeit.
Entsprechende Regelungen sind in Artikel 45 der Richtlinie (EU) 2016/680 enthalten.

Es ist daher zu unterscheiden, ob die Verarbeitung personenbezogener Daten durch die Gerichte im Rahmen der justiziellen Tätigkeit erfolgt und ob die Verarbeitung in den Anwendungsbereich der Verordnung (EU) 2016/679 oder der Richtlinie (EU) 2016/680 fällt:

Zivil- und Fachgerichtsbarkeit (Rechtsprechung und justizielle Verwaltung):

- Für die justizielle Tätigkeit (Rechtsprechung) von Zivilgerichten und der Fachgerichtsbarkeit finden neben der unmittelbar geltenden Verordnung (EU) 2016/679 die Teile 1 und 2 des Berliner Datenschutzgesetzes Anwendung, unter Beachtung der bereichsspezifischen Regelungen, beispielsweise in der ZPO oder in den Verfahrensgesetzen der Fachgerichtsbarkeit.
- Im Rahmen der justiziellen Verwaltung gelten für die Zivilgerichte und die Fachgerichtsbarkeiten die Verordnung (EU) 2016/679 und daneben die landesrechtlichen Regelungen in Teil 1 und 2 des Berliner Datenschutzgesetzes.

Strafgerichtsbarkeit (Rechtsprechung)
Für die Strafgerichte gelten für den Bereich der justiziellen Tätigkeit bei Datenverarbeitungen zu den in Artikel 1 Absatz 1 und Artikel 2 Absatz 1 der Richtlinie (EU) 2016/680 genannten Zwecken die in Teil 1 und 3 des Berliner Datenschutzgesetzes umgesetzten Regelungen unter Beachtung des Vorranges bereichsspezifischer Regelungen, beispielsweise in der StPO.

Strafgerichtsbarkeit (justizielle Verwaltung und Staats-/Amtsanwaltschaft)

- Für die justizielle Verwaltung der Strafgerichte und Staatsanwaltschaften (Datenverarbeitung zu Zwecken der Straftatenverhütung, -ermittlung, -verfolgung und -vollstreckung) und bei Ausführung von Landesrecht gelten Teil 1 und Teil 3 des Berliner Datenschutzgesetzes in Umsetzung der Richtlinie (EU) 2016/680 und gegebenenfalls bereichsspezifisches Landesrecht. Bei Ausführung von bereichsspezifischem Bundesrecht gelten für die Strafgerichte und die Staatsanwaltschaften wiederum die dortigen Datenschutzbestimmungen vorrangig (Artikel 31 des Grundgesetzes).
- Verarbeiten die Strafgerichte und Staatsanwaltschaften im Rahmen der justiziellen Verwaltung wiederum Daten zu anderen als den in der Richtlinie (EU) 2016/680 ge-

nannten Zwecken, gilt die Verordnung (EU) 2016/679 (Artikel 2 Absatz 1 der Verordnung (EU) 2016/679, Artikel 9 Absatz 1 der Richtlinie (EU) 2016/680) und daneben ergänzend das Berliner Datenschutzgesetz (§ 2 Absatz 2 Nummer 2) Teil 1 und 2.

Im Anwendungsbereich der Verordnung (EU) 2016/679 sind die Gerichte (Zivil- und Fachgerichtsbarkeit) auch befugt, besondere Kategorien personenbezogener Daten zu verarbeiten. Dies ergibt sich unmittelbar aus Artikel 9 Absatz 2 Buchstabe f der Verordnung (EU) 2016/679. Die Norm erfasst nur die justizielle, also originär rechtsprechende Tätigkeit der Gerichte. Sie stellt allerdings auf das Kriterium der Erforderlichkeit ab. Geht es z.B. in einem zivilgerichtlichen Verfahren über das Entgelt eines Arztes für eine Behandlung um die Frage, inwieweit ein Behandlungsfehler vorliegt, so kann und müssen Gesundheitsdaten eingeführt werden; etwas anderes gilt, wenn der Anspruchsgrund unstreitig ist, aber die Verjährungseinrede erhoben wird. Kommt es bei der Verjährungseinrede auf den genauen Behandlungszeitpunkt an, so darf dieses Gesundheitsdatum ins Verfahren eingeführt werden (Beispiel nach Weichert in: Kühling/Buchner, DSGVO, Art. 9 Rn. 86).
Soweit ein Gericht auch als Behörde fungiert, etwa als Grundbuchamt oder als Dienstherr der bei dem Gericht beschäftigten Personen, ist die Regelung aus Artikel 9 Absatz 2 Buchstabe f der Verordnung (EU) 2016/679 nicht einschlägig.

Zu Absatz 2
Wie bisher gelten unter bestimmten Voraussetzungen auch privatrechtlich organisierte staatliche Beteiligungsgesellschaften als öffentliche Stellen. Die Regelung in § 2 Absatz 1 Satz 2 des bisher geltenden Berliner Datenschutzgesetzes wird im neuen § 2 Absatz 2 konkretisiert. Der Anwendungsbereich des Berliner Datenschutzgesetzes ist für nicht-öffentliche Stellen immer eröffnet, soweit diese hoheitliche Aufgaben wahrnehmen. Hierunter fallen insbesondere Beliehene. Bei der Wahrnehmung hoheitlicher Tätigkeit kommt es auf eine eventuelle staatliche Beteiligung oder die Gewährung staatlicher Zuwendungen nicht an. Zudem ist der Anwendungsbereich des Berliner Datenschutzgesetzes eröffnet, wenn eine nicht-öffentliche Stelle öffentliche Aufgaben außerhalb hoheitlicher Tätigkeit erfüllt, dann jedoch nur, wenn eine überwiegende Beteiligung des Landes Berlin durch Anteils- oder Stimmmehrheit besteht.

Zu Absatz 3
Die genannten Stellen unterfallen nur insoweit dem Anwendungsbereich, wie sie Verwaltungstätigkeiten wahrnehmen. Die Verarbeitung personenbezogener Daten durch das Abgeordnetenhaus, seine Mitglieder, die Fraktionen sowie der jeweiligen Verwaltungen und Beschäftigten zur Wahrnehmung parlamentarischer Aufgaben ist vom Anwendungsbereich des Gesetzes nicht erfasst.

Zu Absatz 4
Die Verarbeitung personenbezogener Daten im Zusammenhang mit der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten, einschließlich der Abwehr von Gefahren für die öffentliche Sicherheit für diese Zwecke fällt nicht in den Anwendungsbereich der Verordnung (EU) 2016/679, sondern in denjenigen der Richtlinie (EU) 2016/680 (Artikel 1 Absatz 2 Buchstabe d der Verordnung (EU) 2016/679 in Verbindung mit Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680). Da die Verordnung (EU) 2016/679 in diesen Fällen nicht anwendbar ist, ist auch Teil 2 des Gesetzes nicht anzuwenden, da dieser Teil Durchführungsbestimmungen zur Verordnung (EU) 2016/679 enthält.

Die Verarbeitung personenbezogener Daten im Zusammenhang mit Straftaten oder Ordnungswidrigkeiten ist in Teil 3 geregelt, durch den die Umsetzung der Richtlinie (EU) 2016/680 erfolgt. Auch Teil 1, der ebenfalls Regelungen zur Umsetzung der Richtlinie enthält, ist vollständig anzuwenden.
Die Abgrenzung der Verarbeitung personenbezogener Daten, die der Verordnung (EU) 2016/679 und Teil 2 des Gesetzes unterfällt zu derjenigen Verarbeitung, die Teil 3 unterfällt, erfolgt in der Begründung zu § 30.

Zu Absatz 5
Absatz 5 dient der Klarstellung, dass die Regelungen der Verordnung (EU) 2016/679 unmittelbar Anwendung finden. Die in Teil 2 enthaltenen Durchführungsbestimmungen zur Verordnung (EU) 2016/679 treffen ergänzende und konkretisierende Regelungen und formulieren zum Teil Ausnahmen von Regelungen der Verordnung (EU) 2016/679, soweit die Verordnung Ergänzungen, Konkretisierungen oder Ausnahmen gestattet.

Zu Absatz 6
Für öffentliche Stellen, die als Unternehmen am Wettbewerb teilnehmen, findet das Berliner Datenschutzgesetz nur eingeschränkt Anwendung. Nur die Vorschriften über behördliche Datenschutzbeauftragte, Videoüberwachung und Fernmess- und Fernwirkdienste gelten für diese Stellen. Im Übrigen findet das Bundesdatenschutzgesetz Anwendung, so dass für die Wettbewerber möglichst einheitliche Bedingungen gelten. Nimmt eine öffentliche Stelle nur mit bestimmten Tätigkeiten als Unternehmen am Wettbewerb teil, gilt für die nichtwettbewerblichen Tätigkeiten das Berliner Datenschutzgesetz.

Zu Absatz 7
Durch die Erweiterung des Anwendungsbereichs in Satz 1 wird die Regelung des § 19 zur Privilegierung der Verarbeitung personenbezogener Daten zu Zwecken der freien Meinungsäußerung und der Informationsfreiheit auf nicht-öffentliche Stellen erweitert. Allerdings werden die nicht-öffentlichen Stellen auch von den in § 19 vorgesehenen Pflichten erfasst. In Übereinstimmung mit Artikel 2 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 wird in Satz 2 angeordnet, dass § 19 für nicht-öffentliche Stellen nicht anwendbar ist, wenn die Verarbeitung personenbezogener Daten ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten dient. Durch diese Ausnahme wird sichergestellt, dass die Privilegierung persönlicher oder familiärer Tätigkeiten, wie sie in der Verordnung (EU) 2016/679 vorgesehen ist, gewahrt wird. Ohne die Ausnahme würden nicht-öffentliche Stellen anderenfalls wegen der Regelung in Absatz 9 in Verbindung mit Satz 1 zur Einhaltung der Vorgaben aus § 19 verpflichtet werden.

Zu Absatz 8
Die Regelung entspricht inhaltlich § 2 Absatz 5 Satz 2 des bisher geltenden Berliner Datenschutzgesetzes. Besondere Rechtsvorschriften, die sich sowohl aus bereichsspezifischem Bundesrecht, wie auch aus bereichsspezifischem Berliner Landesrecht ergeben können, gehen den Bestimmungen des Berliner Datenschutzgesetzes vor.

Zu Absatz 9
Zur Vermeidung von Regelungslücken für den Schutz personenbezogener Daten wird die entsprechend Anwendung der Regelungen der Verordnung (EU) 2016/679 und der Teile 1 und 2 angeordnet. Insbesondere in den Fällen, die nicht dem Anwendungsbereich der Verordnung (EU) 2016/679 unterfallen und in denen auch keine umfassenden Regelungen im Fach-

recht enthalten sind, soll ein angemessenes und möglichst einheitliches Datenschutzniveau sichergestellt werden.
Die entsprechende Anwendung der Verordnung (EU) 2016/679 und dieses Gesetzes betrifft auch die Verarbeitung personenbezogener Daten in Akten, die weder automatisiert, noch in einem Dateisystem gespeichert sind und die gemäß Artikel 2 Absatz 1 der Verordnung (EU) 2016/679 von deren Anwendungsbereich ausgenommen sind. Dies können beispielsweise Akten in Papierform oder Aktensammlungen sein, die nicht nach bestimmten Kriterien (beispielsweise einem Aktenplan) geordnet sind. Um einen umfassenden Schutz des Grundrechts auf informationelle Selbstbestimmung zu gewährleisten, sind auch in diesen Fällen Regelungen zum Schutz der Rechte der betroffenen Personen erforderlich.

Zu den Absätzen 10 und 11
Die Regelungen stellen Klarstellungen dar und konkretisieren den Geltungsbereich der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 (Erwägungsgründe 101-103 der Richtlinie (EU) 2016/680siehe dazu Schaffland/Wiltfang, DSGVO, Art. 3 Rn. 15: § 1 Absatz 6 BDSG (neu);).

Zu Kapitel 2 Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Zu § 3 Verarbeitung personenbezogener Daten

Durch die Vorschrift in Satz 1 wird eine allgemeine Rechtsgrundlage für die Verarbeitung personenbezogener Daten geschaffen. Aufgrund der Stellung in Teil 1 gilt die Regelung für alle Verarbeitungen personenbezogener Daten, unabhängig davon, ob diese dem Anwendungsbereich der Verordnung (EU) 2016/679 oder der Richtlinie (EU) 2016/680 oder keinem der genannten Anwendungsbereiche unterfallen. Aus § 2 Absatz 8 ergibt sich jedoch, dass § 3 Satz 1 nur anwendbar ist, soweit bereichsspezifisch keine abweichenden Regelungen bestehen.
*G*emäß Erwägungsgrund 45 Sätze 2 und 3 der Verordnung (EU) 2016/679 ist kein spezifisches Gesetz für jeden individuellen Verarbeitungsvorgang notwendig. Ein Gesetz kann für mehrere Verarbeitungsvorgänge im Sinne von Artikel 6 Absatz 1 Buchstabe c und e der Verordnung (EU) 2016/679 ausreichend sein. Demnach können auch abstrakte bzw. allgemeine Normen geschaffen werden.
Eine Verarbeitung personenbezogener Daten nach § 3 Satz 1 setzt immer voraus, dass in einer gesonderten Rechtsvorschrift bestimmte Aufgaben oder die Ausübung öffentlicher Gewalt übertragen wurden und dass keine anderen, die betroffene Person weniger beeinträchtigenden Maßnahmen zur Aufgabenerfüllung oder Ausübung von öffentlicher Gewalt in Betracht kommen.
Soweit der Anwendungsbereich der Verordnung (EU) 2016/679 eröffnet ist, stellt § 3 Satz 1 eine Regelung im Sinne von Artikel 6 Absatz 1 Satz 1 Buchstabe e in Verbindung mit Absatz 3 Satz 1 der Verordnung (EU) 2016/679 dar. Die für Datenverarbeitungen im Anwendungsbereich der Richtlinie (EU) 2016/680 nach deren Artikel 8 Absatz 2 erforderliche Bestimmung der Ziele und Zwecke der Verarbeitung und die personenbezogenen Daten werden im Fachrecht geregelt.
Die Regelung des Satz 1 tritt gemäß Satz 2 am 30. Juni 2020 außer Kraft, so dass ab diesem Zeitpunkt die Verarbeitung personenbezogener Daten besonderer Rechtsgrundlagen bedarf, die sich insbesondere aus dem bereichsspezifischen Recht ergeben können.

Zu Kapitel 3 Datenschutzbeauftragte öffentlicher Stellen

Nach Artikel 37 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 und Artikel 32 Absatz 1 der Richtlinie (EU) 2016/680 ist die Benennung einer oder eines Datenschutzbeauftragten bei der verantwortlichen öffentlichen Stelle vorgesehen. Zudem sind in den jeweiligen Kapiteln IV der Verordnung (EU)2016/679 und der Richtlinie (EU) 2016/680 Vorgaben für die Stellung und Aufgaben der behördlichen Datenschutzbeauftragten enthalten, die in den §§ 4 bis 6 umgesetzt werden.
Die Regelung der Benennung, Stellung und Aufgaben der behördlichen Datenschutzbeauftragten erfolgt in Teil 1, um einheitliche Regelungen im Zusammenhang mit der Verarbeitung personenbezogener Daten zu schaffen, unabhängig davon, ob diese in den Anwendungsbereich der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 oder in keinen der Anwendungsbereiche fällt.
Soweit in den Regelungen wörtliche Wiederholungen des Verordnungstextes enthalten sind, ist dies unvermeidlich, um die Regelungen der Richtlinie (EU) 2016/680 umzusetzen.

Zu § 4 Benennung

Zur Umsetzung der Richtlinie (EU) 2016/680 werden die in Artikel 37 der Verordnung (EU) 2016/679 enthaltenen Regelungen in das Berliner Recht übernommen.

Zu Absatz 3
Die Verpflichtung zur Bestellung einer Stellvertreterin oder eines Stellvertreters wird aus § 19a Absatz 1 Satz 1 des bisher geltenden Berliner Datenschutzgesetzes übernommen.
Die Regelungen zum Datenschutzbeauftragten in Kapitell IV Abschnitt 3 der Richtlinie (EU) 2016/680 sehen weder eine Verpflichtung zur Benennung einer Stellvertretung vor, noch schließen sie eine solche aus. Die Verpflichtung zur Benennung einer Stellvertretung verbessert die Überwachung und Durchsetzung der Regelungen zum Datenschutz beim Verantwortlichen und stärkt dadurch die Rechte und Freiheiten der betroffenen Person. Zu diesem Zweck sieht Artikel 1 Absatz 3 der Richtlinie (EU) 2016/680 vor, dass auch strengere Garantien im nationalen Recht vorgesehen werden können.
Auch die Regelungen zum Datenschutzbeauftragten in Kapitel IV Abschnitt 4 der Verordnung (EU) 2016/679 schließen die Benennung einer Vertretung der oder des obligatorischen Datenschutzbeauftragten nicht aus.
Nicht auf die Vertreterin oder den Vertreter anwendbar ist die Regelung in § 5 Absatz 4 über die Unzulässigkeit der Abberufung oder der eingeschränkten Kündigungsmöglichkeit des Arbeitsverhältnisses. Durch die Regelung über die Stellvertretung soll einerseits vermieden werden, dass während der Abwesenheit der oder des Datenschutzbeauftragten, die Tätigkeiten nicht wahrgenommen werden können, andererseits soll die oder der Datenschutzbeauftragte aber auch die Möglichkeit haben, die Stellvertreterin oder den Stellvertreter im Rahmen der Arbeitsorganisation in die Wahrnehmung seiner Aufgaben einzubeziehen. Diese der oder dem Datenschutzbeauftragten nachgeordnete Stellung der Stellvertreterin oder des Stellvertreters erfordern jedoch nicht in gleichem Maße die Sicherung der Unabhängigkeit, wie bei der oder dem Datenschutzbeauftragten.

Zu § 5 Stellung

Zur Umsetzung der Richtlinie (EU) 2016/680 werden die in Artikel 38 der Verordnung (EU) 2016/679 enthaltenen Regelungen in die Absätze 1, 2, 3 und 5 übernommen.

Zu Absatz 4
Absatz 4 übernimmt die in § 19a Absatz 2 Satz 3 bis 5 des bisher geltenden Berliner Datenschutzgesetzes enthaltene Regelung zum besonderen Abberufungs- und Kündigungsschutz der oder des Datenschutzbeauftragten.

Zu Absatz 5
Absatz 5 soll die Umsetzung datenschutzrechtlicher Vorgaben erleichtern, indem eine jederzeitige Kontaktaufnahmemöglichkeit betroffener Personen mit der oder dem Datenschutzbeauftragten vorgesehen wird. Um die Kontaktaufnahme möglichst niederschwellig zu gestalten, wurde die Verschwiegenheitspflicht bezüglich der Identität oder Identifizierung der kontaktaufnehmenden betroffenen Person - auch gegenüber dem Verantwortlichen - vorgesehen. Verschwiegenheitspflichten aufgrund anderer gesetzlicher Vorschriften, beispielsweise aus § 37 des Beamtenstatusgesetzes, können neben der Pflicht aus Satz 2 bestehen.
Aufgrund der Verschwiegenheitspflicht kann der oder dem Datenschutzbeauftragten ein Auskunftsverweigerungsrecht nach § 55 Absatz 1 der Strafprozessordnung zustehen, wenn der Verstoß gegen die Verschwiegenheitspflicht beispielsweise eine Straftat nach § 203 des Strafgesetzbuches begründen würde.

Zu Absatz 6
Das Zeugnisverweigerungsrecht sichert die in Absatz 5 geregelte Verschwiegenheitspflicht ab.

Zu § 6 Aufgaben

Zur Umsetzung der Richtlinie (EU) 2016/680 werden die in Artikel 39 der Verordnung (EU) 2016/679 enthaltenen Regelungen in das Berliner Recht übernommen.

Zu Absatz 1
Satz 1 Nummer 2 weist der oder dem Datenschutzbeauftragten eine Überwachungsfunktion zu. Danach hat die oder der Datenschutzbeauftragte die Einhaltung der europäischen und nationalen Vorgaben zum Datenschutz zu überwachen. Weiterhin umfasst die Überwachung auch die Datenschutzstrategien der öffentlichen Stelle. Zur Überwachung der Datenschutzstrategien gehört auch die Überwachung, ob und in welcher Form Zuständigkeiten durch den Verantwortlichen zugewiesen werden und wie die an den Datenverarbeitungsvorgängen beteiligten Beschäftigten zum Umgang mit personenbezogenen Daten geschult werden.

Satz 1 Nummer 3 weist der oder dem Datenschutzbeauftragten die Aufgabe zur Beratung im Zusammenhang mit einer Datenschutz-Folgenabschätzung zu, ebenso die Überwachung der Durchführung. Durch die Bezugnahme auf § 53 wird die Wahrnehmung der Aufgabe im Rahmen der Richtlinie (EU) 2016/680 klargestellt. Im Anwendungsbereich der Verordnung (EU) 2016/679 ergibt sich die Aufgabe unmittelbar aus Artikel 39 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679.

In Satz 2 werden die Aufgaben der oder des Datenschutzbeauftragten bei einem Gericht oder beim Rechnungshof auf die Datenverarbeitungen beschränkt, die sich außerhalb derjenigen Tätigkeit bewegen, für die dem Gericht und dem Rechnungshof von Gesetzes wegen Unabhängigkeit garantiert wird.

Zu Kapitel 4 Berliner Beauftragte oder Beauftragter für Datenschutz und Informationsfreiheit

Artikel 51 der Verordnung (EU) 2016/679 und Artikel 41 der Richtlinie (EU) 2016/680 sehen die Errichtung unabhängiger Aufsichtsbehörden durch die Mitgliedstaaten für die Überwachung der Anwendung der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 vor. Zudem sind in den jeweiligen Kapiteln VI der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 Vorgaben für die Unabhängigkeit, die Errichtung, die Zuständigkeit, die Aufgaben und die Befugnisse der Aufsichtsbehörde enthalten, die in den §§ 7 bis 13 umgesetzt werden. Soweit in den Regelungen wörtliche Wiederholungen des Verordnungstextes enthalten sind, ist dies unvermeidlich, um die Regelungen der Richtlinie (EU) 2016/680 umzusetzen.

Zu § 7 Errichtung

Zur Umsetzung der Vorgabe in Artikel 54 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 und Artikel 41 Absatz 1 der Richtlinie (EU) 2016/680 zur Errichtung unabhängiger Aufsichtsbehörden durch die Mitgliedstaaten wird die Regelung des § 22 Absatz 2 Satz 1 Halbsatz 1 des bisher geltenden Berliner Datenschutzgesetzes übernommen. Zugleich wird dadurch den Vorgaben in Artikel 52 Absatz 1 und 2 der Verordnung (EU) und Artikel 42 Absatz 1 und 2 der Richtlinie (EU) 2016/680 nach völliger Unabhängigkeit und Weisungsfreiheit der Aufsichtsbehörden gefolgt.

Zu § 8 Zuständigkeit

Zu Absatz 1
In Absatz 1 wird der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit die Zuständigkeit der Aufsichtsbehörde bei der Verarbeitung personenbezogener Daten für alle öffentlichen Stellen des Landes Berlin übertragen, unabhängig davon, auf welcher Grundlage die öffentlichen Stellen personenbezogene Daten verarbeiten.

Zu Absatz 2
In Absatz 2 wird der oder dem Berliner Beauftragen für Datenschutz und Informationsfreiheit entsprechend § 40 Absatz 1 des Bundesdatenschutzgesetzes die Zuständigkeit als Aufsichtsbehörde für die nicht-öffentlichen Stellen übertragen.

Zu Absatz 3
Die justizielle Tätigkeit der Gerichte unterliegt nicht der Aufsicht durch die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit. Die Regelung passt die bisherige Regelung (§ 24 Absatz 2 des bisher geltenden Berliner Datenschutzgeset-

zes), nach welcher die Gerichte der Kontrolle der oder des Berliner Beauftragten nur unterliegen, soweit sie in Verwaltungsangelegenheiten tätig werden, an den Wortlaut der Verordnung (EU) 2016/679 bzw. der Richtlinie (EU) 2016/680 an. Hierdurch wird Artikel 45 Absatz 2 der Richtlinie (EU) 2016/680 umgesetzt; Artikel 55 Absatz 3 der Verordnung (EU) 2016/679 gilt hingegen unmittelbar.
Dies gilt auch für den Rechnungshof im Rahmen seiner unabhängigen Tätigkeit (so auch Körffer in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Auflage 2017, Art. 55 Rn. 8).

Zu § 9 Ernennung und Beendigung des Amtsverhältnisses

§ 9 regelt in Durchführung von Artikel 53 und Artikel 54 Absatz 1 Buchstaben b bis e der Verordnung (EU) 2016/679 und Artikel 43 Absatz 1 sowie Artikel 44 Absatz 2 der Richtlinie (EU) 2016/680 das Verfahren und die Voraussetzungen für die Ernennung, die Amtszeit sowie die Zulässigkeit der Wiederwahl der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit.

Zu Absatz 1
Die in Satz 1 vorgesehenen Modalitäten der Ernennung dienen zugleich der Umsetzung der Regelungsaufträge in Artikel 53 Absatz 1 der Verordnung (EU) 2016/679 und in Artikel 44 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/680.
Gleichzeitig wird in Satz 2 entsprechend § 21 Absatz 1 des bisher geltenden Berliner Datenschutzgesetzes der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit die Aufgabe der oder des Landesbeauftragten für das Recht auf Akteneinsicht übertragen und die Amts- und Funktionsbezeichnung festgelegt.
In Satz 3 werden entsprechend des Regelungsauftrages in Artikel 53 Absatz 2 und in Artikel 54 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/680 die Anforderungen an die Qualifikation der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit festgelegt.

Zu Absatz 2
Die Regelung des § 21 Absatz 2 des bisher geltenden Berliner Datenschutzgesetzes zum Amtseid wurde im Zusammenhang mit den zu regelnden Modalitäten des Ernennungsverfahrens übernommen.

Zu Absatz 3
Die im Wesentlichen aus dem bisherigen § 21 Absatz 3 des bisher geltenden Berliner Datenschutzgesetzes übernommenen Regelungen entsprechen den Vorgaben des Artikels 54 Absatz 1 Buchstabe d, e und f Verordnung (EU) 2016/679. Davon umfasst ist die vorgesehene Pflicht der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit zur Weiterführung des Amtes bis zur Ernennung einer Nachfolgerin oder eines Nachfolgers.
Die in § 21 Absatz 3 Satz 3 des bisher geltenden Berliner Datenschutzgesetzes geregelte Entlassungsmöglichkeit wird an die Regelungen des Artikels 53 Absatz 3 und 4 der Verordnung (EU) 2016/679 angepasst. Nach Artikel 53 Absatz 4 der Verordnung (EU) 2016/679 erfolgt eine Amtsenthebung, wenn ein Mitglied der Aufsichtsbehörde entweder eine schwere Verfehlung begangen hat oder wenn die Voraussetzungen für die Wahrnehmung der Aufgaben nicht mehr erfüllt sind. Wegen der Regelung in Artikel 53 Absatz 4 der Verordnung (EU) 2016/679 und Artikel 43 Absatz 4 der Richtlinie (EU) 2016/680 konnte der bislang in § 21 Absatz 3 Satz 3 des Berliner Datenschutzgesetzes enthaltene ausdrückliche Bezug auf die Entlassungs-

gründe bei einem Richterverhältnis auf Lebenszeit nicht aufrechterhalten werden. Materiellrechtlich dürften die insoweit im Deutschen Richtergesetz vorgesehenen Voraussetzungen regelmäßig eine schwere Verfehlung im Sinne der Regelung darstellen.

Zu § 10 Rechtsstellung

Zu Absatz 1
Die Ausgestaltung als öffentlich-rechtliches Amtsverhältnis sichert die Unabhängigkeit der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit rechtlich ab. Bei der Regelung handelt sich um eine Konkretisierung des nach Artikel 54 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 zu konkretisierenden Amtsverhältnisses. Damit ist verbunden, dass die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit nach § 11 Absatz 1 Nummer 2 Buchstabe b des Strafgesetzbuches Amtsträger im Sinne des Strafrechts ist und deshalb unter anderem die Straftatbestände der §§ 201, 203 Absatz 2, 204, 331, 332, 353b und 355 des Strafgesetzbuches gelten. Zudem unterfällt sie oder er auch dem Beamtenbegriff im haftungsrechtlichen Sinne nach § 839 des Bürgerlichen Gesetzbuchs in Verbindung mit Artikel 34 des Grundgesetzes.

Zu Absatz 2 und 3
Die Regelungen dienen der Umsetzung von Artikel 42 der Richtlinie (EU) 2016/680.

Zu Absatz 4
Absatz 4 enthält ein umfassendes Verbot sämtlicher nicht mit dem Amt zu vereinbarender Handlungen und Tätigkeiten, gleich ob entgeltlich oder unentgeltlich. Die Regelung entspricht § 22 Absatz 3 des bisher geltenden Berliner Datenschutzgesetzes, allerdings nach Maßgabe von Artikel 52 Absatz 3 der Verordnung (EU) 2016/679 als Konkretisierung des allgemeinen Verbots der Ausübung mit dem Amt nicht zu vereinbarender Handlungen und Tätigkeiten. Die Befugnis zur Konkretisierung ergibt sich aus Artikel 54 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679.

Zu Absatz 5
Durch die Regelung wird die Vorgabe in Artikel 54 Absatz 2 der Verordnung (EU) 2016/679 zur Verschwiegenheitspflicht umgesetzt. Die Regelung aus § 23 des bisher geltenden Berliner Datenschutzgesetzes wird inhaltlich ergänzt um die Aussagegenehmigung der oder des amtierenden Berliner Beauftragten für Datenschutz und Informationsfreiheit sowie um die eigenständige Ermessensentscheidung aufgrund der entfallenden Dienstaufsicht durch die Präsidentin oder den Präsidenten des Abgeordnetenhauses. Die Regelungsbefugnis ergibt sich aus Artikel 54 Absatz 2 in Verbindung mit Absatz 1 Buchstabe f der Verordnung (EU) 2016/679.

Zu Absatz 6
Die Rechtsstellung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit soll im Übrigen wie in § 22 Absatz 3 Satz 3 des bisher geltenden Berliner Datenschutzgesetzes durch Vertrag geregelt werden.
Auf das Amtsverhältnis sollen die beamtenrechtlichen Vorschriften des Landes Berlin sinngemäß Anwendung finden. Diese Regelung ist im bisher geltenden Berliner Datenschutzgesetz nicht enthalten, entspricht aber der geltenden Regelungslage. Aus Gründen der Rechtssicherheit und Transparenz soll die sinngemäße Anwendung beamtenrechtlicher Vorschriften nunmehr auch im Gesetz geregelt werden.

Zu § 11 Aufgaben

Zur Umsetzung des Artikels 46 der Richtlinie (EU) 2016/680 werden die in Artikel 57 der Verordnung (EU) 2016/679 enthaltenen Regelungen in das Berliner Recht übernommen.

Zu § 12 Tätigkeitsbericht

Zu Absatz 1
Durch die Regelung wird die Verpflichtung zur Erstellung und Übermittlung eines Tätigkeitsberichts an das Parlament über den Anwendungsbereich des unmittelbar geltenden Artikels 59 der Verordnung (EU) 2016/679 hinaus erstreckt, unter anderem auch zur Umsetzung der gleichlautenden Vorgabe in Artikel 49 der Richtlinie (EU) 2016/680.
Die Regelung entspricht § 29 Absatz 2 Satz 1 des bisher geltenden Berliner Datenschutzgesetzes, jedoch entfällt zukünftig die Vorlagepflicht gegenüber dem Senat, um die Unabhängigkeit der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit zu wahren.

Zu Absatz 2
Die Stellungnahmeverpflichtung des Senats aus § 29 Absatz 2 Satz 2 des bisher geltenden Berliner Datenschutzgesetzes wird übernommen, allerdings wird die bisherige Stellungnahmefrist von drei Monaten auf sechs Monate erhöht. Mit der Verlängerung der Stellungnahmefrist wird der möglichen Erhöhung des Umfangs und der Komplexität des Tätigkeitsberichts, wie sie aufgrund der Zunahme an Aufgaben der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit zu erwarten ist, Rechnung getragen.

Zu § 13 Befugnisse

§ 13 ergänzt die unmittelbar geltenden Befugnisse aus Artikel 58 der Verordnung (EU) 2016/679. Gleichzeitig wird damit die Vorgabe von Artikel 58 Absatz 4 der Verordnung (EU) 2016/679 mitumgesetzt, wonach ein ordnungsgemäßes Verfahren im Einklang mit der Charta festzulegen ist, nach dem die Aufsichtsbehörden ihre Befugnisse gemäß Artikel 58 Verordnung (EU) 2016/679 ausüben können.

Zu Absatz 1
Absatz 1 führt im Anwendungsbereich der Verordnung (EU) 2016/679 die Beanstandungsbefugnis der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit aus § 26 Absatz 1 des bisher geltenden Berliner Datenschutzgesetzes ein. Eine solche ist nach Artikel 58 Absatz 1 bis 3 der Verordnung (EU) 2016/679 nicht vorgesehen, jedoch von der Öffnungsklausel in Artikel 58 Absatz 6 der Verordnung (EU) 2016/679 gedeckt. Danach kann jeder Mitgliedstaat vorsehen, dass die Aufsichtsbehörden neben den in Artikel 58 Absatz 1, 2 und 3 der Verordnung (EU) 2016/679 vorgesehenen Befugnissen über zusätzliche Befugnisse verfügen.
Eine Beanstandung mit der Möglichkeit zur Einholung einer Stellungnahme stellt eine zweckmäßige zusätzliche Befugnis für die oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit dar. Die Einholung einer Stellungnahme soll jedoch nicht – wie bis-

her - verpflichtend vorgeschrieben werden, sondern vielmehr eine zusätzliche Option neben den anderen Befugnissen darstellen. Die Durchführung eines quasi vorgeschalteten Beanstandungsverfahrens eröffnet die ressourcensparende Möglichkeit, dass festgestellte Verstöße gegen die Vorschriften des Datenschutzes der oder dem jeweils zuständigen Verantwortlichen mitgeteilt werden und diese vor der etwaigen Ausübung der Befugnisse nach Artikel 58 Absatz 2 Verordnung (EU) 2016/679 unter Setzung einer angemessenen Frist Gelegenheit zur Stellungnahme erhalten. Die Angemessenheit der Frist für die Stellungnahme ist von den konkreten Umständen des Einzelfalls abhängig, insbesondere davon, ob der Beanstandung zugrundeliegende Verstöße gegen Datenschutzvorschriften weiterhin bestehen oder ob diese bereits beendet sind, von der Komplexität des zugrundeliegenden Sachverhaltes sowie der Art und des Umfanges erforderlicher Ermittlungen des Verantwortlichen.

Zu Absatz 2
Außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 steht der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit das Beanstandungsrecht nach Absatz 2 zur Verfügung. Dies betrifft insbesondere den Anwendungsbereich der Richtlinie (EU) 2016/680, nach deren Artikel 47 Absatz 2 wirksame Abhilfebefugnisse bestehen müssen. Als Beispiel wirksamer Abhilfebefugnisse sieht Artikel 47 Absatz 2 Buchstabe a der Richtlinie (EU) 2016/680 eine mögliche Warnung des Verantwortlichen vor, was einer Beanstandung entspricht. Insbesondere gegenüber öffentlichen Stellen, die einer besonderen Bindung an Recht und Gesetz unterliegen, entfaltet eine Beanstandung, dass eine beabsichtigte oder bisher vorgenommene Verarbeitung gegen Vorschriften der Richtlinie verstoßen könnte oder verstoßen hat, eine ausreichende Wirkung, um bestehende Verstöße abzustellen und zukünftige Verstöße verhindern zu können. Weitergehende Eingriffsbefugnisse der Aufsichtsbehörde im Anwendungsbereich der Richtlinie (EU) 2016/680 würden dazu führen, dass die für den Datenschutz zuständige Aufsichtsbehörde auch in fachliche Maßnahmen der Sicherheitsbehörden eingreifen könnte. Soweit die Einrichtung spezifischer Eingriffsmöglichkeiten erforderlich ist, um einen Ausgleich zwischen der Funktion der Aufsichtsbehörde und den spezifischen Aufgaben im Anwendungsbereich der Richtlinie (EU) 2016/680 zu schaffen, können diese im Fachrecht vorgesehen werden.
Die Angemessenheit der im Rahmen des Beanstandung zu setzenden Frist zur Stellungnahme richtet sich nach den konkreten Umständen des Einzelfalls, insbesondere danach, ob der Beanstandung zugrundeliegende Verstöße gegen Datenschutzvorschriften weiterhin bestehen oder ob diese bereits beendet sind, nach der Komplexität des zugrundeliegenden Sachverhaltes sowie der Art und des Umfanges erforderlicher Ermittlungen des Verantwortlichen.

Zu Absatz 3
In denjenigen Fällen des Absatzes 1 oder 2, in denen die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit eine Beanstandung mit einer Frist zur Stellungnahme innerhalb einer angemessenen Frist verbunden hat, erhält die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit die Möglichkeit, den für die öffentliche Stelle jeweils zuständigen Ausschuss des Abgeordnetenhauses mit der Beanstandung befassen zu können. Eine Aufnahme auf die Tagesordnung des jeweiligen Ausschusses setzt jedoch voraus, dass zuvor zwischen der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit und der jeweiligen öffentlichen Stelle, deren Verarbeitung Gegenstand der Beanstandung ist, der Versuch einer Einigung unternommen wurde. Im Rahmen der Einigung sollen die Rechtsansichten der Beteiligten berücksichtigt und alternative Handlungsmöglichkeiten vorgeschlagen werden. Sofern der Versuch einer Einigung nicht dazu führt, dass die von der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit beanstandeten Verstöße gegen

Datenschutzvorschriften oder Mängel beseitigt werden, erfolgt die Aufnahme auf die Tagesordnung des jeweils zuständigen Fachausschusses des Abgeordnetenhauses auf Antrag der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Sie oder er kann im Rahmen der vom Abgeordnetenhaus vorgegebenen Sitzungstermine den Zeitpunkt wählen, ist dabei aber an die Vorgaben des Abgeordnetenhauses, insbesondere zu Form und Frist der Anmeldung, gebunden.
In den Fällen einer Beanstandung, in denen die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit eine Beanstandung mit einer angemessenen Frist zur Stellungnahme verbunden hat, die Stellungnahme jedoch ohne Zustimmung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit nicht erfolgt, kann eine Aufnahme auf die Tagesordnung des für die öffentliche Stelle jeweils zuständigen Ausschusses auch ohne Versuch einer Einigung erfolgen.
Die Möglichkeit der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit zur Aufnahme auf die Tagesordnung eines Ausschusses des Abgeordnetenhauses stellt eine Erweiterung der in Artikel 58 Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 vorgesehenen Befugnis zur Stellungnahme gegenüber dem Parlament, aufgrund der in Artikel 58 Absatz 6 der Verordnung (EU) 2016/679 enthaltenen Öffnungsklausel, dar.
Im Anwendungsbereich der Richtlinie (EU) 2016/680 stellt die in Absatz 3 vorgesehene Möglichkeit eine wirksame Abhilfebefugnis im Sinne von Artikel 47 Absatz 2 der Richtlinie (EU) 2016/680 dar.

Zu Absatz 4
Die Regelung übernimmt die in § 28 Absatz 1 Satz 2 Nummer 3 des bisher geltenden Berliner Datenschutzgesetzes normierten Zugangsrechte der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Hierdurch wird die gemäß Artikel 58 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 zur Ausübung der Untersuchungsbefugnisse notwendige mitgliedstaatliche Verfahrensvorschrift für die Zugangs- und Betretungsrechte von Diensträumen und Anlagen geschaffen.

Zu Absatz 5
Aufgrund von Artikel 58 Absatz 5 der Verordnung (EU) 2016/679 wird die in § 24 Absatz 5 Satz 4 des bisher geltenden Berliner Datenschutzgesetzes enthaltene Befugnis der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit, einen strafbewehrten Verstoß gegen datenschutzrechtliche Bestimmungen zur Anzeige zu bringen, übernommen.

Zu Absatz 6
Absatz 5 schafft eine eigene Rechtsgrundlage für die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit, um die mit der Wahrnehmung der Befugnisse erforderlichen personenbezogenen Daten, einschließlich besonderer Kategorien, verarbeiten zu können. Satz 3 enthält Regelbeispiele für ein erhebliches öffentliches Interesse im Zusammenhang mit der Verarbeitung besonderer Kategorien personenbezogener Daten.

Zu Absatz 7
Absatz 7 stellt im Einklang mit dem Erwägungsgrund 143 der Verordnung (EU) 2016/679 klar, dass die nach Artikel 263 AEUV vorgesehene Klagemöglichkeit vor dem Europäischen Gerichtshof auch durch die oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit wahrgenommen werden kann.

Zu Absatz 8

Das Berliner Datenschutzgesetz gilt nach § 2 Absatz 2 Satz 1 auch für Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen das Land Berlin mit absoluter Mehrheit der Anteile oder mit absoluter Mehrheit der Stimmen beteiligt ist. Nach § 2 Absatz 2 Satz 2 gilt es zudem, unabhängig von einer Beteiligung öffentlicher Stellen, für nicht-öffentliche Stellen, die hoheitliche Aufgaben wahrnehmen. Da für solche Stellen die Verpflichtung aus Absatz 4 mit einem Eingriff in das Grundrecht aus Artikel 13 Absatz 1 des Grundgesetzes verbunden sein kann, dient Absatz 8 der Erfüllung des Zitiergebotes aus Artikel 19 Absatz 1 Satz 2 des Grundgesetzes.

Zu Teil 2
Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679

Zu Kapitel 1 Grundsätze der Verarbeitung personenbezogener Daten

Zu § 14 Verarbeitung besonderer Kategorien personenbezogener Daten

Artikel 9 der Verordnung (EU) 2016/679 enthält in Absatz 1 ein grundsätzliches Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten und zählt die Kategorien auf, zu denen beispielsweise die ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, die Gewerkschaftszugehörigkeit oder Gesundheitsdaten gehören. In Absatz 2 des Artikels 9 sind in den Buchstaben a, c, d, e und f Ausnahmen von dem Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten enthalten, die unmittelbar gelten. In Artikel 9 Absatz 2 Buchstabe b, g, h und i sind weitere Ausnahmetatbestände enthalten, die jedoch durch europäisches oder nationales Recht zur Geltung gebracht werden müssen. Unter anderem diesem Zweck dient § 14.

Zu Absatz 1
In Absatz 1 Nummer 1 wird von der Möglichkeit in Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 Gebrauch gemacht, durch nationales Recht die Verarbeitung besonderer Kategorien personenbezogener Daten im Hinblick auf das Dienst- und Arbeitsrecht und das Recht der sozialen Sicherheit zu ermöglichen.
Absatz 1 Nummer 2 ermöglicht entsprechend Artikel 9 Absatz 2 Buchstabe h der Verordnung (EU) 2016/679 die Verarbeitung besonderer Kategorien personenbezogener Daten.
Absatz 1 Nummer 3 ermöglicht entsprechend Artikel 9 Absatz 2 Buchstabe i der Verordnung (EU) 2016/679 die Verarbeitung besonderer Kategorien personenbezogener Daten.
Die Regelungen in § 14 Absatz 1 Nummer 2 und 3 sind zum Teil bereits Bestandteil von § 6a Absatz 3 des bisher geltenden Berliner Datenschutzgesetzes.

Zu Absatz 2
Absatz 2 sieht die Verarbeitung besonderer Kategorien personenbezogener Daten in Fällen des Artikels 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 unter den dort genannten besonderen Voraussetzungen vor und bestimmt in den Nummern 1 und 2 das erhebliche öffentliche Interesse näher. Um ein angemessenes Verhältnis zu den in den Nummern 1 und 2 verfolgten Zielen herzustellen, ist eine Verarbeitung besonderer Kategorien personenbezoge-

ner Daten nach Absatz 2 nur zulässig, wenn eine vorzunehmende Interessenabwägung ein Überwiegen der öffentlichen Interessen ergibt.

Zu Absatz 3
Absatz 3 enthält die Verpflichtung zur Einhaltung spezifischer Maßnahmen und geeigneter Garantien zur Wahrung der Grundrechte und Interessen der betroffenen Personen, wie dies in Artikel 9 Absatz 2 Buchstabe b, g und i der Verordnung (EU) 2016/679 vorgesehen ist. Die beispielhafte Aufzählung in Satz 2 ist nicht abschließend und nicht auf die Auswahl einer der genannten Maßnahmen beschränkt.

Zu § 15 Verarbeitung zu anderen Zwecken

Die Verarbeitung personenbezogener Daten, zu einem anderen Zweck, als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, kann gemäß Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 erfolgen, wenn die betroffene Person in die Verarbeitung zu dem geänderten Zweck einwilligt oder aufgrund einer Rechtsvorschrift der Europäischen Union oder der Mitgliedstaaten. § 15 macht von dieser Regelungsbefugnis Gebrauch. Die neben dieser Möglichkeit zur mitgliedstaatlichen Regelung in Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 vorgesehenen und unmittelbar geltenden Möglichkeiten zu einer zweckändernden Verarbeitung (aufgrund einer Einwilligung oder unter den Voraussetzungen der Buchstaben a sowie c bis f des Artikels 6 Absatz 4 der Verordnung (EU) 2016/679) bleiben unberührt.

Zu Absatz 1
Absatz 1 Satz 1 enthält eine abschließende Aufzählung derjenigen Alternativen, nach denen durch mitgliedstaatliches Recht eine zweckändernde Verarbeitung personenbezogener Daten zulässig ist. Die Alternativen berücksichtigen die Vorgabe aus Artikel 6 Absatz 4 der Verordnung (EU) 2016/679, wonach eine mitgliedstaatliche Regelung zugleich eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 genannten Ziele darstellen muss.
Nummer 1, die § 11 Absatz 2 Satz 1 Nummer 1 in Verbindung mit § 6a Absatz 2 des bisher geltenden Berliner Datenschutzgesetzes entspricht, dient dem Schutz der betroffenen Person, der als wichtiges Ziel in Artikel 23 Absatz 1 Buchstabe c und i der Verordnung (EU) 2016/679 enthalten ist.
Nummer 2 schützt das in Artikel 23 Absatz 1 Buchstabe c und d; Nummer 3 das in Artikel 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679 enthaltene Ziel. Die Vorschriften entsprechen im Wesentlichen § 11 Absatz 2 Satz 1 Nummer 2 und 3 des bisher geltenden Berliner Datenschutzgesetzes.
Nummer 4 dient der Möglichkeit einer zweckändernden Verarbeitung personenbezogener Daten, die der Öffentlichkeit bereits zugänglich sind, beziehungsweise welche die Voraussetzungen für eine Zugänglichmachung für die Öffentlichkeit erfüllen. Die zweckändernde Verarbeitung kann verschiedenen der in Artikel 23 Absatz 1 genannten Ziele dienen, beispielsweise der Sicherstellung der öffentlichen Sicherheit oder der Verhütung von Straftaten. Zur Wahrung der Verhältnismäßigkeit müssen vor einer zweckändernden Verarbeitung bereits veröffentlichter oder einer Veröffentlichung zur Verfügung stehender personenbezogener Daten offensichtlich entgegenstehende Interessen der betroffenen Person berücksichtigt werden, welche eine zweckändernde Verarbeitung ausschließen.
Nummer 5 dient den in Artikel 23 Absatz 1 Buchstabe h der Verordnung (EU) 2016/679 genannten Zielen, wobei die Kontroll-, Überwachungs- und Ordnungsfunktionen der beaufsich-

tigenden Stelle insbesondere die Aufrechterhaltung der Funktionsfähigkeit der öffentlichen Verwaltung, als Bestandteil der öffentlichen Sicherheit, gewährleisten sollen. Im zweiten Halbsatz von Nummer 5 werden Anforderungen an die Verhältnismäßigkeit der Erhebung personenbezogener Daten im Zusammenhang mit Kontroll-, Überwachungs- und Ordnungsfunktionen formuliert, so dass die Verarbeitung von nicht zu diesem Zweck bereits verarbeiteter Daten nur dann zulässig ist, wenn die Aufgabe anderenfalls nicht erfüllt werden könnte.
Die in Nummer 6 enthaltene Möglichkeit, personenbezogene Daten auch zu Aus- und Fortbildungszwecken nutzen zu können, soweit schutzwürdige Belange der betroffenen Person nicht entgegenstehen, stellt ein wichtiges Ziel des allgemeinen öffentlichen Interesses im Sinne von Artikel 23 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 dar. Aus- und Fortbildung im Rahmen der Tätigkeiten öffentlicher Stellen dienen unmittelbar der Erfüllung von öffentlichen Aufgaben und sind zudem häufig mit Grundrechtseingriffen verbunden oder dienen der Verwaltung öffentlicher Mittel, deren schonende Verwendung mindestens mittelbar einen Verzicht auf weitere Grundrechtseingriffe bewirkt. An einer möglichst qualitativen Aus- und Fortbildung, wie sie insbesondere durch Lernen an möglichst praxisnahen Fällen erfolgen kann, stellt ein gewichtiges öffentliches Interesse dar.
Durch § 15 Absatz 1 Satz 1 Nummer 5, 6 und Satz 2 sind die Fälle, die bereits in § 11 Absatz 4 und 5 des bisher geltenden Berliner Datenschutzgesetzes geregelt sind, auch nach Inkrafttreten der Verordnung (EU) 2016/679 weiterhin erfasst.

Zu Absatz 2
Wie in § 11 Absatz 3 des bisher geltenden Berliner Datenschutzgesetzes soll eine zweckändernde Verarbeitung nach Absatz 2 Nummer 2 und 3 nicht zulässig sein, wenn die personenbezogenen Daten einem Berufsgeheimnis oder besonderen Amtsgeheimnis unterliegen. Berufsgeheimnisse sind Geheimnisse, die den Angehörigen der in § 203 Absatz 1 des Strafgesetzbuches genannten Berufsgruppen (unter anderem Ärzte, Berufspsychologen, Rechtsanwälte, Ehe-, Erziehungs- oder Jugendberater, Suchtberater, Sozialarbeiter) in Ausübung ihrer Tätigkeit bekannt werden. Dabei stehen den in § 203 Absatz 1 und Satz 1 des Strafgesetzbuches Genannten ihre berufsmäßig tätigen Gehilfinnen und Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Besondere Amtsgeheimnisse sind solche Geheimnisse, die über das im Verwaltungsverfahrensrecht geregelte allgemeine Amtsgeheimnis und die dienst- und arbeitsrechtlichen Verschwiegenheitspflichten hinausgehen, wie zum Beispiel das Steuergeheimnis, das Post- und Fernmeldegeheimnis oder das Statistikgeheimnis.

Zu Absatz 3
Nach Artikel 13 Absatz 3 und Artikel 14 Absatz 4 der Verordnung (EU) 2016/679 treffen den Verantwortlichen Informationspflichten gegenüber der betroffenen Person nicht nur bei der ursprünglichen Datenerhebung, sondern auch im Falle einer Verarbeitung zu einem anderen, als dem ursprünglichen Zweck. In denjenigen Fällen, in denen aufgrund von Artikel 23 der Verordnung (EU) 2016/679 Ausnahmen von der Informationspflicht bei der ursprünglichen Datenerhebung vorgesehen sind, würde es zu einer Regelungslücke führen, wenn die Informationspflicht nicht auch für den Fall einer Zweckänderung bis zu dem Zeitpunkt aufgeschoben würde, in dem durch die Erfüllung der Informationspflicht der Zweck der Verarbeitung nicht mehr gefährdet wird. Von einer Information der betroffenen Person über die Verarbeitung zu einem anderen, als dem ursprünglichen Zweck, kann jedoch nur in den Fällen des Absatzes 1 Satz 1 Nummer 2, 3 und 5 abgesehen werden. Durch die entsprechende Anwendung von § 23 Absatz 3 sind die Informationen im Falle eines vorübergehenden Hinderungsgrundes unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer

angemessenen Frist ab Fortfall des Hinderungsgrundes, spätestens jedoch nach Ablauf von zwei Wochen, zu erteilen.

Zu Absatz 4
Die in § 11 Absatz 3 des bisher geltenden Berliner Datenschutzgesetzes bereits enthaltene Regelung soll auch nach Inkrafttreten der Verordnung (EU) 2016/679 weiterhin anwendbar sein, da sich insbesondere in den Fällen einer aktenmäßigen Verarbeitung personenbezogener Daten nicht immer sicherstellen lässt, dass eine Trennung personenbezogener Daten von weiteren Daten der betroffenen Person oder Dritter nach verschiedenen Zwecken mit vertretbarem Aufwand möglich ist. Nur wenn eine solche Trennung nicht oder nur mit unvertretbar großem Aufwand möglich ist, dürfen ausnahmsweise auch nicht für den konkreten Zweck erforderliche Daten weitergegeben oder übermittelt werden. In diesem Falle unterliegen zum Schutz der Rechte der betroffenen Personen die Daten, die nicht dem Zweck der jeweiligen Verarbeitung dienen, einem Verwertungsverbot.
Die Regelungsbefugnis ergibt sich aus Artikel 6 Absatz 2 und 3 der Verordnung (EU) 2016/679, indem die Voraussetzungen für die Rechtmäßigkeit der Verarbeitung näher spezifiziert werden.

Zu Absatz 5
Absatz 5 ermöglicht in begrenztem Rahmen eine Zweckänderung der Verarbeitung besonderer Kategorien personenbezogener Daten in den Fällen des § 14 Absatz 2. Der Verweis auf den unmittelbar geltenden Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 dient der Wahrung der Kohärenz und Verständlichmachung im Sinne des Erwägungsgrundes 8 der Verordnung (EU) 2016/679.
Auch im Falle einer Verarbeitung besonderer Kategorien personenbezogener Daten zu einem anderen, als dem ursprünglichen Zweck, gelten die Voraussetzungen von § 14 Absatz 3.

Zu § 16 Verantwortlichkeit bei der Übermittlung personenbezogener Daten

Die Übermittlung personenbezogener Daten stellt nach Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 sowohl für die übermittelnde Stelle, als auch für die ersuchende und abrufende Stelle jeweils einen eigenen Verarbeitungsvorgang dar. Beide Stellen können somit Verantwortliche im Sinne von Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 sein.

Zu Absatz 1
§ 16 Absatz 1 Satz 1 und Absatz 2 Satz 1 treffen jeweils eine Regelung im Sinne von Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 über den Zweck der Übermittlung und legen dazu die Verantwortlichkeit fest. Im Falle eines Ersuchens oder eines automatisierten Abrufs durch eine öffentlichen Stelle, die nach Artikel 1 Absatz 2 und Artikel 20 Absatz 3 des Grundgesetzes sowie Artikel 1 Absatz 3 und Artikel 36 Absatz 1 der Verfassung von Berlin einer besonderen Bindung an Recht und Gesetz unterworfen ist, wird die Verantwortlichkeit einseitig der ersuchenden oder abrufenden Stelle zugewiesen.
Im Falle von § 16 Absatz 1 Satz 1 werden die Pflichten der übermittelnden Stelle auf die Prüfung beschränkt, ob das Ermittlungsersuchen in den Aufgabenbereich der ersuchenden Stelle fällt, wobei der Aufgabenbereich regelmäßig gesetzlich festgelegt ist. Hierdurch wird die unabhängige Prüfung der Angaben der ersuchenden Stelle gewährleistet, bei einem gleichzeitig hohen Maß an Zuverlässigkeit für die Richtigkeit des Prüfungsergebnisses. Bei Zweifeln erfolgt keine Zuweisung der Verantwortlichkeit an nur eine Stelle, die Verantwortlichkeit rich-

tet sich dann nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679. In einem solchen Falle ist vor der Übermittlung eine weitergehende Prüfung der Rechtmäßigkeit der Übermittlung erforderlich.
Zweck der Regelung ist die Beschleunigung der Verwaltungstätigkeiten, durch Entlastung der übermittelnden Stelle, wobei die Einhaltung eines hohen Schutzniveaus für die Grundrechte der betroffenen Personen durch die bestehende Bindung der ersuchenden Behörde an Recht und Gesetz und die Prüfung der Aufgabeneinhaltung durch die ersuchte Stelle gewährleistet bleibt.

Zu Absatz 2
Die Regelung in Absatz 2 entspricht § 15 Absatz 5 des bisher geltenden Berliner Datenschutzgesetzes, die ebenfalls zum Zweck der Beschleunigung der Verwaltungstätigkeiten übernommen wird. Anders als in den Fällen des Absatz 1, in denen die übermittelnde Behörde durch das Ersuchen eine Prüfungsmöglichkeit vor der jeweiligen Übermittlung besitzt, besteht eine solche Möglichkeit beim automatisierten Verfahren auf Abruf nicht. Da sich die Regelungen von Absatz 1 Satz1 und Absatz 2 Satz 1 nur dahingehend unterscheiden, dass das Übermittlungsersuchen durch einen automatisierten Abruf ersetzt wird, ansonsten jedoch eine vergleichbare Interessenlage sowohl seitens der übermittelnden und abrufenden/ersuchenden Stellen und der betroffenen Personen besteht, wird durch die Reglung in Absatz 2 Satz 2 und 3 ein vergleichbares Schutzniveau wie in Absatz 1 für die Rechte der betroffenen Personen geschaffen.

Die Zuweisung der Verantwortlichkeit nach § 16 an die ersuchende oder abrufende Stelle erfolgt nur, wenn es sich bei dieser Stelle um eine öffentliche handelt. Bei einer Übermittlung ohne Ersuchen oder bei einer Übermittlung aufgrund eines Ersuchens oder Abrufs einer nichtöffentlichen Stelle richtet sich die Verantwortlichkeit der übermittelnden Stelle nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679.

Zu Kapitel 2 Besondere Verarbeitungssituationen

Zu § 17 Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

§ 17 regelt die Zulässigkeit von der und spezifische Anforderungen an die Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken und enthält Garantien im Sinne des Artikels 89 der Verordnung (EU) 2016/679 für die Rechte und Freiheiten der betroffenen Personen, mit denen insbesondere sichergestellt wird, dass technische und organisatorische Maßnahmen bestehen, mit denen unter anderem die Achtung des Grundsatzes der Datenminimierung (Artikel 5 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679) gewährleistet werden soll.

Zu Absatz 1
In Absatz 1 wird aufgrund von Artikel 6 Absatz 1 Satz 1 Buchstabe e in Verbindung mit Absatz 2 und 3 der Verordnung (EU) 2016/679 die Regelung in § 30 Absatz 1 Satz 1 und Absatz 6 des bisher geltenden Berliner Datenschutzgesetzes beibehalten.
Die Befugnis zur Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken umfasst nach Artikel 5 Absatz 1

Buchstabe b der Verordnung (EU) 2016/679 die Befugnis, ursprünglich zu anderen Zwecken verarbeitete Daten, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken zu verarbeiten. Umgekehrt ist durch die Regelung in Satz 2 jedoch ausgeschlossen, dass zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken verarbeitete personenbezogene Daten einer Zweckänderung unterzogen werden.

Zu Absatz 2
In Absatz 2 werden von Artikel 89 der Verordnung (EU) 2016/679 vorgesehene Garantien durch die Einbeziehung der Regelung des § 30 Absatz 2 des bisher geltenden Berliner Datenschutzgesetzes vorgesehen.

Zu Absatz 3
Die Bestimmung spezifiziert die Verarbeitung (Übermittlung) personenbezogener Daten im Hinblick auf deren Veröffentlichung, indem entsprechend § 30 Absatz 5 des bisher geltenden Berliner Datenschutzgesetzes zum Schutz der Rechte der betroffenen Personen nur im besonderen Ausnahmefall eine personenbezogene Darstellung der Forschungsergebnisse zugelassen wird.

Zu Absatz 4
Artikel 89 Absatz 2 der Verordnung (EU) 2016/679 sieht die Möglichkeit der Mitgliedstaaten vor, Ausnahmen von den Rechten gemäß der Artikel 15, 16, 18 und 21 der Verordnung (EU) 2016/679 zu machen, wovon in Absatz 5 Gebrauch gemacht wird. Ein Beispiel für die ernsthafte Beeinträchtigung der Forschung könnte das Auskunftsrecht der betroffenen Personen darstellen, wenn im Rahmen sozialwissenschaftlicher Forschung große Mengen öffentlich zugänglicher personenbezogener Daten aus sozialen Medien verarbeitet werden, so dass die Bearbeitung der Auskünfte die Kapazitäten der Forschungsstelle übersteigen kann.

Zu § 18 Verarbeitung personenbezogener Beschäftigtendaten

§ 18 macht von der Möglichkeit des Artikels 88 der Verordnung (EU) 2016/679 Gebrauch, spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext zu treffen und erklärt hierzu die Regelungen des auf die Verordnung (EU) 2016/679 abgestimmten Bundesdatenschutzgesetzes (einschließlich des dort in § 26 Absatz 8 näher bestimmten Beschäftigtenbegriffes) für anwendbar. Die Anwendung der Regelungen des Bundesdatenschutzgesetzes auf Beschäftigtendaten ist bereits Bestandteil des bisher geltenden Rechts (§ 2 Absatz 2 des bisher geltenden Berliner Datenschutzgesetzes).

Zu § 19 Verarbeitung personenbezogener Daten zu Zwecken der freien Meinungsäußerung und der Informationsfreiheit

§ 19 dienst der Umsetzung des Regelungsauftrages in Artikel 85 der Verordnung (EU) 2016/679. Der Anwendungsbereich der Norm erfasst nach § 2 Absatz 7 auch nicht-öffentliche Stellen, soweit diese die Daten nicht ausschließlich zu persönlichen oder familiären Zwecken verarbeiten.

Zu Absatz 1
Die Abweichungsbefugnis des Artikels 85 Absatz 1 und 2 der Verordnung (EU) 2016/679 soll für sämtliche Bereiche des Rechts auf freie Meinungsäußerung und Informationszugang zum Tragen kommen. Die Verortung im Berliner Datenschutzgesetz dient dazu, auch diejenigen Handlungen unter Ausübung der genannten Rechte zu erfassen, die (noch) keinem medienbezogenen Fachrecht zugeordnet werden können, weil sie beispielsweise noch nicht bekannt sind.
Durch den Ausschluss der Kapitel II bis VII sowie IX und der bestehenbleibenden Anwendbarkeit von Artikel 5 Absatz 1 Buchstabe f und Artikel 24, 32 und 33 der Verordnung (EU) 2016/679 wird die bisherige Rechtslage des sogenannten Medienprivilegs beibehalten, wonach Presse, Rundfunk und diesen gleichgestellte Medien bei der Ausübung der journalistisch-redaktionellen Tätigkeit lediglich die Vorschriften zum Datengeheimnis und zur Datensicherheit beachten müssen und Schadensersatzansprüchen bei Nichtbeachtung ausgesetzt sind.

Zu Absatz 2
Im Anwendungsbereich des Medienprivilegs würde das Recht auf freie Meinungsäußerung leer laufen, wenn Berichtigungs- und Löschungsansprüche vollumfänglich zur Durchsetzung gelangen würden. So kommt eine Verpflichtung zur Berichtigung oder Löschung bereits veröffentlichter oder zur Veröffentlichung vorgesehener journalistischer Erzeugnisse gemäß den Vorgaben der Verordnung (EU) 2016/679 nicht ohne weiteres in Betracht. Das Recht auf informationelle Selbstbestimmung vermittelt gleichwohl einen Anspruch der betroffenen Personen auf die Gewährleistung von Vollständigkeit und Richtigkeit ihrer personenbezogenen Daten. Ein Ausgleich dieser Interessen wird mit der Verpflichtung zur parallelen Aufbewahrung und Übermittlung erzielt. Das Zustandekommen und die Durchsetzung der Gegendarstellungs- und Unterlassungsansprüche bestimmen sich nach dem jeweiligen Fachrecht.

Zu § 20 Videoüberwachung

Die Regelungen zur Videoüberwachung in § 31b des bislang bisher geltenden Berliner Datenschutzgesetzes wurden im Wesentlichen übernommen. Die Befugnis zur Regelung der Videoüberwachung folgt aus Artikel 6 Absatz 1 Buchstabe e in Verbindung mit den Absätzen 2 und 3 der Verordnung (EU) 2016/679. Die Regelung zur Löschung in § 31b Absatz 5 des bisher geltenden Berliner Datenschutzgesetzes wurde nicht übernommen, da Artikel 17 der Verordnung (EU) 2016/679 eigene und vergleichbare Löschungsverpflichtungen vorsieht.

Zu Absatz 1
Absatz 1 schafft eine Rechtsgrundlage für die Videoüberwachung in öffentlich zugänglichen Räumen, jedoch nur zu den Zwecken der Erfüllung einer im öffentlichen Interesse liegenden Aufgabe oder zur Wahrnehmung des Hausrechts. Die von § 31b Absatz 1 des bisher geltenden Berliner Datenschutzgesetzes abweichende Formulierung in Bezug auf die Aufgabenerfüllung beruht auf Artikel 6 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679.
Der Begriff der Videoüberwachung umfasst alle optisch-elektronischen Einrichtungen, unabhängig davon, ob eine Aufzeichnung erfolgt. Eine unterschiedliche Behandlung von Videobeobachtung und Videoaufzeichnung wird nicht vorgenommen. Der Verarbeitungsbegriff des Absatz 1 umfasst somit insbesondere die Erhebung, das Erfassen und das Speichern personenbezogener Daten. Nicht unter die Norm fallen beispielsweise Beobachtungen mittels eines

Spiegels oder mit Hilfe eines Fernglases, da in diesen Fällen lediglich eine optische, aber keine elektronische Komponente enthalten ist.
Spezifische Regelungen zur Videoüberwachung, beispielsweise aus dem Allgemeinen Sicherheits- und Ordnungsgesetz, gehen gemäß § 2 Absatz 8 der Befugnis zur vor und schließen bei abschließender Regelung die Anwendbarkeit von Absatz 1 aus.

Zu Absatz 2
Absatz 2 enthält eine Verpflichtung zur Erkennbarmachung einer Videoüberwachung zu einem Zeitpunkt, zu dem sich betroffene Personen noch nicht innerhalb des überwachten Bereiches befinden und in dem somit noch keine Verarbeitung personenbezogener Daten erfolgt. Durch die frühzeitige Information soll dem Recht auf informationelle Selbstbestimmung in größtmöglichem Umfang Rechnung getragen werden, so dass betroffene Personen mitentscheiden können, ob sie personenbezogene Daten bereitstellen (vgl. Erwägungsgrund 60 Satz 4 der Verordnung (EU) 2016/679).
Die Informationen nach Absatz 2 können an oder innerhalb des überwachten Bereiches angebracht werden, wenn sie von außerhalb wahrgenommen werden können und somit die Entscheidung zu einem Betreten oder Nichtbetreten ermöglichen.
Die Information können nach dem Erwägungsgrund 60 Satz 5 der Verordnung (EU) 2016/679 auch in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln.
Durch die Regelung des Absatzes 2 werden die Informationspflichten des Artikels 13 der Verordnung (EU) 2016/679 nicht berührt. Nach Artikel 13 der Verordnung (EU) 2016/679 sind die dort genannten Informationen zum Zeitpunkt der Erhebung der Daten zu erteilen.

Zu Absatz 3
Absatz 3 entspricht § 31b Absatz 3 Satz 2 des bisher geltenden Datenschutzgesetzes. Auf die Übernahme des Begriffes der staatlichen Sicherheit wurde verzichtet, da dieser vom Begriff der öffentlichen Sicherheit umfasst ist (vgl. BVerwG, Beschluss vom 19. September 2017 – 1 VR 8/17).

Zu Absatz 4
Absatz 4 entspricht § 31b Absatz 3a des bisher geltenden Berliner Datenschutzgesetzes. Die Regelung der Höchstspeicherfrist erfolgt aufgrund von Artikel 6 Absatz 3 Satz 3 der Verordnung (EU) 2016/679.

Zu Absatz 5
In Absatz 5 wird die Regelung aus § 31b Absatz 5 Alternative 2 des bisher geltenden Berliner Datenschutzgesetzes übernommen. Die Regelung aus § 31b Absatz 5 Alternative 1 des bisher geltenden Berliner Datenschutzgesetzes gilt unmittelbar aufgrund von Artikel 17 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679.
Nach Absatz 1 setzt die Videoüberwachung unter anderem voraus, dass keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen. Absatz 5 regelt den Fall, dass nachträglich schutzwürdige Interessen bekannt werden oder entstehen, oder dass bereits bekannte schutzwürdige Interessen zwar zunächst für die Erhebung nicht überwogen haben, aber für die Frage der weiteren Speicherung abweichend zu beurteilen sind.

Zu § 21 Gemeinsames Verfahren und automatisiertes Verfahren auf Abruf

Zu Absatz 1
Satz 1 entspricht inhaltlich § 15 Absatz 1 des bisher geltenden Berliner Datenschutzgesetzes und wurde an die Begriffe der Verordnung (EU) 2016/679 angepasst.
Nach Artikel 26 Absatz 3 der Verordnung (EU) 2016/679 kann die betroffene Person ihre Rechte gegenüber jedem der Verantwortlichen geltend machen, so dass es keiner gesonderten Regelung wie in § 15 Absatz 3 des bisher geltenden Berliner Datenschutzgesetzes mehr bedarf.
Die Verantwortlichkeit im Rahmen des automatisierten Verfahrens auf Abruf ist in § 15 Absatz 2 geregelt.

Zu Absatz 2
In Absatz 2 wird die Regelung aus § 15 Absatz 2 Satz 1 Nummer 1 des bisher geltenden Berliner Datenschutzgesetzes übernommen, die insoweit über den Anwendungsbereich der Verordnung (EU) 2016/679 hinausgeht, als dass die Vorgaben auch fachliche und technische Vorgaben umfassen, die unabhängig von personenbezogenen Daten sein können. Die weiteren in § 15 Absatz 2 und 3 des bisher geltenden Datenschutzgesetzes getroffenen Regelungen sind von Artikel 26 der Verordnung (EU) 2016/679 erfasst und gelten unmittelbar, was durch die einleitende Formulierung des Absatzes 2 klargestellt wird.

Zu Absatz 3 bis 6
Die Absätze entsprechen § 15 Absatz 6 bis 9 des bisher geltenden Berliner Datenschutzgesetzes.

Zu § 22 Fernmess- und Fernwirkdienste

In § 22 wurde die Regelung aus § 31a des bisher geltenden Berliner Datenschutzgesetzes übernommen. Die Regelung enthält in den Absätzen 1 bis 3 auch Regelungen, die über den Umgang mit personenbezogenen Daten hinausgehen, aber wegen der Besonderheiten von Fernmess- und Fernwirkdiensten, die jederzeit zu einer Verarbeitung personenbezogener Daten führen können, in einem engen Zusammenhang mit der Verarbeitung personenbezogener Daten stehen und deshalb systematisch zusammen geregelt werden.

Zu Absatz 1
Die Regelung bezieht sich auf den Zeitpunkt vor der Erhebung personenbezogener Daten und regelt die Zulässigkeitsvoraussetzungen der Einrichtung eines Fernmess- oder Fernwirkdienstes. Soweit personenbezogene Daten erhoben werden, gelten für die Einwilligung die Artikel 7 und 8 der Verordnung (EU) 2016/679 unmittelbar. Die Einwilligungsregelungen des Absatzes 1 gelten drüber hinaus auch für die sonstigen Daten, die im Rahmen der Fernmess- und Fernwirkdienste erhoben werden. Hierfür ist insbesondere die Vorgabe in Artikel 7 Absatz 2 der Verordnung (EU) 2016/679 zu beachten.

Zu Absatz 2
Die Regelung schützt das Recht auf informationelle Selbstbestimmung, indem der betroffenen Person während des Betriebs eines Fernmess- oder Fernwirkdienstes der Umfang der Messungen oder Einwirkungen erkennbar werden soll, um daraus das Maß der Erhebung personenbezogener Daten erkennen zu können, soweit dies mit dem Vertragszweck vereinbar ist.

Zu Absatz 3
Die Regelung schützt die Freiheit zur Willensentschließung, ob eine Einwilligung abgegeben beziehungsweise widerrufen wird.

Zu Absatz 4
Satz 1 enthält eine Zweckbindungsregelung, die im Falle des Wunsches nach einer Verarbeitung zu anderen Zwecken bei der Auslegung nach Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 zu berücksichtigen ist.
Satz 2 dient der Klarstellung.

Zu Kapitel 3 Rechte der betroffenen Personen

Zu § 23 Informationspflicht bei Erhebung von personenbezogener Daten

Artikel 13 und Artikel 14 der Verordnung (EU) 2016/679 verpflichten den Verantwortlichen, den von der Erhebung personenbezogener Daten betroffenen Personen bestimmte, in Artikel 13 und 14 der Verordnung (EU) 2016/679 näher festgelegte Informationen bereitzustellen, ohne dass es dafür eines gesonderten Antrags bedarf. Ausnahmen von dieser Verpflichtung sind in Artikel 13 Absatz 4 und Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 enthalten. Darüber hinaus können die Mitgliedstaaten nach Artikel 23 der Verordnung (EU) 2016/679 weitere Ausnahmen vorsehen, sofern die Ausnahmen der Erfüllung einer der dort in Absatz 1 genannten Zwecke dienen. § 22 macht von diesem Recht des Artikels 23 der Verordnung (EU) 2016/679 Gebrauch und sieht zusätzliche Ausnahmen von der Informationspflicht vor.
§ 22 gilt sowohl für die Erhebung personenbezogener Daten bei der betroffenen Person, als auch bei der Erhebung personenbezogener Daten über die betroffene Person bei Dritten.

Zu Absatz 1
Die Informationspflichten der Verordnung (EU) 2016/679 stellen ein neues Element im Datenschutzrecht dar. Sie zielen ebenso wie das Auskunftsrecht, welches bereits im bisher geltenden Berliner Datenschutzgesetz enthalten ist, auf eine möglichst umfassende Information der betroffenen Person zur Wahrnehmung ihrer Rechte. Das Auskunftsrecht in § 16 des bisher geltenden Berliner Datenschutzgesetzes ist eingeschränkt, wenn eine Abwägung ergibt, dass ein öffentliches Geheimhaltungsinteresse oder ein überwiegendes Geheimhaltungsinteresse Dritter, das Interesse der betroffenen Person an der Auskunftserteilung überwiegt. Diese Regelung wird aufgrund von Artikel 23 Absatz 1 Buchstaben e und i der Verordnung (EU) 2016/679 in Absatz 1 Satz 1 auch für das Informationsrecht übernommen, da anderenfalls eine mögliche Beschränkung des Auskunftsrechts in Leere laufen würde, wenn die geheimzuhaltenden Informationen im Rahmen des Informationsrechts mitgeteilt werden müssten. Die vorzunehmende Abwägung und die Berücksichtigung des Umfangs der Einschränkung stellen spezifische Vorschriften zum Schutz der Rechte der betroffenen Person im Sinne von Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 dar.
Beim Überwiegen eines öffentlichen oder privaten Geheimhaltungsinteresses ist in jedem Fall zu prüfen, wie weit die Einschränkung des Informationsrechts anhand der konkreten Umstände des Einzelfalles reicht. Je nach Einzelfall kann die Verweigerung der Information nur ganz bestimmte Elemente aus Artikel 13 Absatz 1, 2 oder 3 oder Artikel 14 Absatz 1 oder 2 der Verordnung (EU) 2016/679 umfassen; beispielsweise kann die Abwägung ergeben, dass nur die Information über eine zweckändernde Verarbeitung oder über die Empfänger personenbe-

zogener Daten geheimgehalten werden müssen, während die anderen Informationen mitzuteilen sind. Zudem muss auch anhand des Einzelfalles geprüft werden, für welche Dauer das Informationsrecht entfallen soll. Nach Wegfall des Geheimhaltungsgrundes ist die Information zu erteilen, es sei denn, dass nach der Verordnung (EU) 2016/679 ein Grund für die Nichterteilung der Information besteht.
In Satz 2 werden Beispiele genannt, bei denen typischerweise ein Überwiegen des öffentlichen oder privaten Geheimhaltungsinteresses angenommen werden kann. Auch bei Vorliegen der genannten Gründe muss in jedem Fall geprüft werden, wie weit und wie lange die Einschränkung des Informationsrechtes reicht.

Zu Absatz 2
Im Falle einer mitgliedstaatlichen Einschränkung der Informationspflichten sind nach Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 zum Ausgleich der Nachteile zugleich spezifische Regelungen vorzusehen. Hierfür wird zunächst die Entscheidung über das Absehen von der Information einer zentralen Stelle, entweder der Leitung oder einer von dieser bestimmten Stelle, zugewiesen. Zudem muss die Entscheidung dokumentiert und diese der oder dem behördlichen Datenschutzbeauftragten mitgeteilt werden. Weiterhin wird der Verantwortliche in Absatz 2 verpflichtet, geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person zu treffen. Die konkret zu treffenden Maßnahmen richten sich nach dem Einzelfall und müssen unter anderem die Dauer und den Umfang der Einschränkung berücksichtigen. Als eine mögliche Maßnahme wird die Bereitstellung der nach Artikel 13 Absatz 1 und 2 sowie Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 erforderlichen Informationen für die Öffentlichkeit genannt. Die Veröffentlichung kann beispielsweise auf der allgemein zugänglichen Website des Verantwortlichen erfolgen (Erwägungsgrund 58 der Verordnung (EU) 2016/679). Durch diese Form der Bereitstellung wird betroffenen Personen ein allgemeiner und umfassender Überblick über die Datenverarbeitung beim Verantwortlichen, insbesondere zu deren Rechtsgrundlagen und Zwecken ermöglicht, so dass die Einschränkung der konkreten, speziell auf die betroffene Person bezogenen Informationen auf ein Minimum beschränkt wird.

Zu Absatz 3
Bei Fortfall des Hinderungsgrundes muss die Information nachträglich erteilt werden. Dies gilt jedoch nur insoweit, wie nicht aufgrund der Verordnung (EU) 2016/679 von der Informationserteilung abgesehen werden kann.

Zu § 24 Auskunftsrecht der betroffenen Person
Neben den Informationen, die der Verantwortliche aufgrund von Artikel 13 und 14 der Verordnung (EU) 2016/679 eigeninitiativ zur Verfügung stellen muss, gewährt Artikel 15 der Verordnung (EU) 2016/679 einen antragsgebundenen Anspruch auf Auskunft zu den konkret verarbeiteten Daten. Das Auskunftsrecht kann ebenso wie das Informationsrecht aufgrund von Artikel 23 der Verordnung (EU) 2016/679 durch mitgliedstaatliches Recht eingeschränkt werden. Von dieser Möglichkeit wird in § 24 Gebrauch gemacht.

Zu Absatz 1
Ebenso wie in § 16 Absatz 5 des bisher geltenden Berliner Datenschutzgesetzes wird das Auskunftsrecht der betroffenen Person eingeschränkt, wenn eine Abwägung ergibt, dass ein öffentliches Geheimhaltungsinteresse oder ein überwiegendes Geheimhaltungsinteresse Drit-

ter, das Interesse der betroffenen Person an der Auskunftserteilung überwiegt. Diese Regelung erfolgt aufgrund von Artikel 23 Absatz 1 Buchstaben e und i der Verordnung (EU) 2016/679 in Absatz 1 Satz 1. Die vorzunehmende Abwägung und die Berücksichtigung des Umfangs der Einschränkung stellen spezifische Vorschriften zum Schutz der Rechte der betroffenen Person im Sinne von Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 dar.
Beim Überwiegen eines öffentlichen oder privaten Geheimhaltungsinteresses ist in jedem Fall zu prüfen, wie weit die Einschränkung des Auskunftsrechts anhand der konkreten Umstände des Einzelfalles reicht. Je nach Einzelfall kann die Verweigerung der Auskunft nur ganz bestimmte Elemente aus Artikel 15 Absatz 1 der Verordnung (EU) 2016/679 umfassen; beispielsweise kann die Abwägung ergeben, dass nur die Auskunft über die Herkunft der Daten oder über die Empfänger personenbezogener Daten geheim gehalten werden müssen, während die anderen Auskünfte zu erteilen sind. Zudem muss auch anhand des Einzelfalles geprüft werden, für welche Dauer das Auskunftsrecht entfallen soll. Nach Wegfall des Geheimhaltungsgrundes ist die Auskunft zu erteilen.
In Satz 2 werden Beispiele genannt, bei denen typischerweise ein Überwiegen des öffentlichen oder privaten Geheimhaltungsinteresses angenommen werden kann. Auch bei Vorliegen der genannten Gründe muss in jedem Fall geprüft werden, wie weit und wie lange die Einschränkung des Informationsrechtes reicht.
Das Auskunftsrecht besteht nach Satz 3 nicht für Daten, die zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind und wenn deren Verarbeitung durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. Diese Regelung betrifft Sicherungskopien. Als Sicherungskopien entsprechen diese Daten denjenigen, die aktiv verarbeitet werden und zu denen bereits umfassend Auskunft erteilt werden muss. Die Erstreckung der Auskunft auf die Sicherheitskopien würde seitens der öffentlichen Stellen zu einem unvertretbaren Mehraufwand führen, ohne dass der betroffenen Person zugleich ein wesentlicher Vorteil entstehen würde.

Zu Absatz 2
Ohne Zustimmung der in Absatz 2 genannten Stellen ist eine Auskunftserteilung unzulässig. Die Befugnis für diese Regelung ergibt sich aus Artikel 23 Absatz 1 Buchstaben a bis e der Verordnung (EU) 2016/679.
Die Regelung in Satz 3 wonach die Zustimmung nur zum Schutz einer der in der Verordnung (EU) 2016/679 genannten Gründe versagt werden darf, bindet diejenigen der in Absatz 3 genannten Stellen, die dem Anwendungsbereich des Gesetzes unterfallen.

Zu Absatz 3
Die Regelung in Absatz 3 Satz 1 ist erforderlich, um den Zweck, der einer Auskunft entgegensteht, nicht zu gefährden. Die Entscheidung, ob und inwieweit eine Begründung der Auskunftsverweigerung erfolgen kann, ist gesondert zu treffen. Die Entscheidung obliegt der jeweiligen Behördenleiterin oder dem jeweiligen Behördenleiter (bzw. der Leitung der jeweiligen öffentlichen Stelle) und kann auf die Leiterin oder den Leiter der nächst darunterliegenden Organisationsebene delegiert werden. Eine Delegation auf weitere oder andere Organisationebenen ist nicht möglich. Insbesondere bei Kollegialorganen als Behördenleitung kommt eine Delegation auf die jeweiligen Mitglieder des Kollegialorgans in Betracht. Eine Delegation berührt jedoch nicht die weiterhin bestehende Verantwortlichkeit der Leitung.
In jedem Fall sind die Gründe aktenkundig zu machen, da dies Voraussetzung der Prüfung der Einhaltung der gesetzlichen Vorschriften durch die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit ist. Zudem ist die betroffene Person in

jedem Fall auf ihr Recht zur Überprüfung durch die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit hinzuweisen. Diese Regelung stellt zugleich eine spezifische Regelung im Sinne von Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 dar und ist bereits in § 16 Absatz 5 des bisher geltenden Berliner Datenschutzgesetzes enthalten.

Zu Absatz 4
Im Falle eines vorübergehenden Hinderungsgrundes ist die zunächst unterbliebene Auskunft unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist ab Wegfall des Hinderungsgrundes, spätestens jedoch nach Ablauf von zwei Wochen, nachzuholen.

Zu Absatz 5
Artikel 15 Absatz 1 der Verordnung (EU) 2016/679 sieht nicht nur ein Recht der betroffenen Person vor, Auskunft verlangen zu können, welche personenbezogenen Daten bei dem jeweiligen Verantwortlichen verarbeitet werden, sondern insbesondere auch, ob überhaupt personenbezogene Daten verarbeitet werden. Das Auskunftsrecht besteht demnach grundsätzlich, ohne dass die betroffene Person an dem Auffinden der Daten mitwirken muss. Die Verweigerung der Auskunft aufgrund fehlender Hinweise zum Auffinden kann nach Artikel 23 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 zum Schutz sonstiger wichtiger Ziele eines Mitgliedstaates erfolgen. Die Vermeidung eines unverhältnismäßigen Verwaltungsaufwands durch die aufwendige Suche in einer Vielzahl von Akten nach personenbezogenen Daten der antragstellenden Person stellt ein wichtiges wirtschaftliches und finanzielles Interesse dar. Ein unverhältnismäßiger Aufwand kann in Fällen der nicht-automatisierten Verarbeitung personenbezogener Daten entstehen, insbesondere wenn Akten nicht zu der betroffenen Person geführt werden. In diesen Fällen sind oftmals Hinweise der betroffenen Person erforderlich, um die Akten, in denen sich die personenbezogenen Daten befinden, eingrenzen und auffinden zu können. Die Hinweise können beispielsweise thematische aber auch örtliche oder zeitliche Eingrenzungen betreffen.

Zu Absatz 6
Zusätzlich zu dem Auskunftsrecht der Verordnung (EU) 2016/679 wird in Absatz 5 das bereits in § 16 Absatz 4 des bisher geltenden Berliner Datenschutzgesetzes vorgesehene Akteneinsichtsrecht übernommen. Das Akteneinsichtsrecht des Absatzes 5 betrifft vorrangig die dort vorhandenen personenbezogenen Daten, kann jedoch auch auf weitere Daten erstreckt werden. Die Erstreckung auf weitere Daten ist jedoch unzulässig, wenn es sich um personenbezogene Daten Dritter oder geheimhaltungsbedürftige sonstige Daten handelt. Sind solche Daten mit personenbezogenen Daten der anspruchsberechtigten Person verbunden, muss zunächst geprüft werden, ob eine Trennung möglich ist (z.B. auch durch Herstellung einer Kopie mit Schwärzungen). Ist eine solche Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich, kann die Akteneinsicht versagt werden.
In Satz 4 wird die entsprechende Geltung der Absätze 1 bis 4 angeordnet, um einen Gleichklang der Regelungen zu Auskunft und Akteneinsicht herzustellen.

Zu Absatz 7
Die Vorschrift enthält eine Verpflichtung des Senats zur Vorlage eines Berichts, insbesondere zu Anzahl und Gründen, sowie kompensierender Maßnahmen, für die Fälle, in denen Auskunftsersuchen nicht oder nicht vollständig beantwortet wurden.

Zu § 25 Recht auf Löschung

Artikel 17 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 sieht das grundsätzliche Recht der betroffenen Person vor, die Löschung personenbezogener Daten verlangen zu können, sofern diese für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr erforderlich sind. Dieses Recht gilt jedoch nach Artikel 17 Absatz 3 Buchstabe d der Verordnung (EU) 2016/679 nicht, soweit die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke erforderlich ist und das Recht auf Löschung voraussichtlich die Verwirklichung dieser Ziele unmöglich macht oder ernsthaft beeinträchtigt.
Durch § 25 wird aufgrund der Regelungskompetenz in Artikel 6 Absatz 1 Satz 1 Buchstabe e in Verbindung mit Absatz 2 und 3 der Verordnung (EU) 2016/679 ein Ausgleich zwischen den im öffentlichen Interesse liegenden Archivzwecken und dem Recht der betroffenen Person auf Löschung der personenbezogenen Daten geschaffen, indem die datenverarbeitende Stelle zunächst verpflichtet wird, eine frühzeitige (unverzügliche) Entscheidung über die Archivwürdigkeit herbeizuführen, sobald bei der datenverarbeitenden Stelle die Voraussetzungen zur Löschung eintreten und nach Ablauf der in § 7 Absatz 1 Satz 2 des Archivgesetzes des Landes Berlin bestimmten Frist die Löschungsverpflichtung eintritt.
Die Verpflichtungen des öffentlichen Archivs zum Umgang mit den personenbezogenen Daten ergeben sich aus dem Fachrecht.

Zu Kapitel 4 Pflichten der Verantwortlichen und Auftragsverarbeiter

Zu § 26 Spezifische technische und organisatorische Maßnahmen zur Gewährleistung einer rechtmäßigen Verarbeitung

Artikel 24 und 25 der Verordnung (EU) 2016/679 verpflichten den Verantwortlichen zur Umsetzung von technischen und organisatorischen Maßnahmen, um sicherzustellen und nachweisen zu können, dass die Vorgaben der Verordnung (EU) 2016/679 umgesetzt werden.
Sofern der Verantwortliche mit einem Auftragsverarbeiter zusammenarbeiten will, darf er nach Artikel 28 Absatz 1 der Verordnung (EU) 2016/679 nur solche Auftragsverarbeiter auswählen, die ihrerseits hinreichende Garantien für geeignete technische und organisatorische Maßnahmen zur Umsetzung der Vorschriften der Verordnung (EU) 2016/679 bieten. Die spezifischen Maßnahmen in § 26, die den Verantwortlichen treffen, sind auch dann einzuhalten, wenn sich der Verantwortliche der Dienste eines Auftragsverarbeiters bedient.
Die Vorschrift gilt für alle automatisierten Verarbeitungen personenbezogener Daten. Sie gilt jedoch nicht für die automatisierte Verarbeitung personenbezogener Daten, soweit diese aufgrund von Bundesrecht erfolgt.

Zu Absatz 1
Absatz 1 spezifiziert die Anforderungen an die technischen und organisatorischen Maßnahmen des Verantwortlichen über die Vorgaben hinaus, die bereits in den Artikeln 25, 32, 35 und 36 der Verordnung (EU) 2016/679 enthalten sind und die zum Teil Regelungen des bisher geltenden Berliner Datenschutzgesetzes ablösen. Zur Regelung weitergehender Pflichten wird von der Möglichkeit in Artikel 6 Absatz 2 und 3 der Verordnung (EU) 2016/679 Gebrauch gemacht, spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschrif-

ten der Verordnung (EU) 2016/679 in den Fällen des Artikels 6 Absatz 1 Satz 1 Buchstabe c und e, beibehalten oder einführen zu können.
Die Nummern 1 bis 3 entsprechen § 5 Absatz 2 Nummern 4 bis 6 des bisher geltenden Berliner Datenschutzgesetzes.

Zu Absatz 2
Ebenso wie in Absatz 1, werden auf der Grundlage von Artikel 6 Absatz 2 und 3 der Verordnung (EU) 2016/679 spezifischere Bestimmungen vorgesehen, die im Wesentlichen § 5 Absatz 3 Satz 1 des bisher geltenden Berliner Datenschutzgesetzes entsprechen. Durch die Verpflichtung zur Risikoanalyse und Dokumentation in einem Datenschutzkonzept wird klargestellt, dass alle technischen und organisatorischen Maßnahmen, nicht nur wie bisher die Sicherheitsmaßnahmen, in einem Konzept zusammenzufassen sind. Die systematische Ermittlung und Darstellung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung kann nach wie vor in der gewohnten Form eines (Informations-)Sicherheitskonzepts erfolgen, auf das im Datenschutzkonzept verwiesen wird, sofern beachtet wird, dass das Sicherheitskonzept die Risiken für die Rechte und Freiheiten der betroffenen Personen vorrangig zu berücksichtigen hat.
Das Datenschutzkonzept bildet eine Grundlage für die Entscheidung, ob eine Datenschutzfolgeabschätzung nach Artikel 35 Absatz 1 der Verordnung (EU) 2016/679 erforderlich ist.

Zu Absatz 3
Absatz 3 enthält auf der Grundlage von Artikel 6 Absatz 2 und 3 der Verordnung (EU) 2016/679 spezifische Bestimmungen zur Wartung von Datenverarbeitungssystemen, in denen Teile von § 3a des bisher geltenden Berliner Datenschutzgesetzes übernommen werden. Besteht bei einer Wartung die Möglichkeit, dass Stellen außerhalb des Geltungsbereiches der Verordnung (EU) 2016/67, dazu zählen nach § 2 Absatz 10 auch die dort genannten Staaten, Kenntnis personenbezogener Daten erlangen können, müssen die Voraussetzungen der Artikel 45 und 46 der Verordnung (EU) 2016/679 vorliegen. Zudem darf eine Wartung, bei der die Möglichkeit einer Kenntniserlangung personenbezogener Daten außerhalb der genannten Staaten besteht, nur erfolgen, wenn es erforderlich ist. Dies ist der Fall, wenn die Wartung nicht auf eine andere Weise, bei der keine oder zumindest eine weniger beeinträchtigende Möglichkeit der Kenntniserlangung personenbezogener Daten außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 und der in § 2 Absatz 10 genannten Staaten, besteht.

Zu § 27 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

Artikel 34 der Verordnung (EU) 2016/679 sieht in seinem Absatz 1 eine Verpflichtung des Verantwortlichen vor, betroffene Personen zu benachrichtigen, wenn der Schutz deren personenbezogener Daten verletzt wurde. In Artikel 34 Absatz 3 der Verordnung (EU) 2016/679 sind Ausnahmen von der Benachrichtigungspflicht vorgesehen. Darüber hinaus können nach Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 weitere Ausnahmen durch die Mitgliedstaaten vorgesehen werden. Von dieser Möglichkeit wird in § 27 Gebrauch gemacht.
Durch § 27 soll sichergestellt werden, dass keine Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen erfolgt, wenn ein öffentliches Geheimhaltungsinteresse oder ein Geheimhaltungsinteresse Dritter besteht und dieses das Interesse der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person überwiegt.

Durch eine entsprechende Anwendung von § 23 Absatz 1 kann einerseits ein Gleichklang hergestellt werden, zwischen den Gründen, aus denen die Auskunft verweigert werden kann und den Gründen, aus denen die Benachrichtigung unterbleiben kann. Andererseits können durch die entsprechende Anwendung von § 23 Absatz 1 aber auch die konkreten Umstände des Einzelfalles, insbesondere die Tatsache der Verletzung des Schutzes personenbezogener Daten, die Art und die Anzahl der betroffenen Daten, die Maßnahmen des Verantwortlichen zur Beseitigung oder Begrenzung der Folgen und die Risiken für die betroffenen Personen, im Rahmen der in § 23 Absatz 1 vorgesehenen Abwägung berücksichtigt werden.

Zu Kapitel 5 Sanktionen

Zu § 28 Geldbußen

Artikel 83 der Verordnung (EU) 2016/679 sieht für dort näher bestimmte Verstöße gegen Datenschutzvorschriften die Verhängung von Geldbußen durch die Aufsichtsbehörde vor. In Artikel 83 Absatz 7 der Verordnung (EU) 2016/679 wird den Mitgliedstaaten die Möglichkeit eingeräumt, durch eigenes Recht Ausnahmen von der Möglichkeit zur Verhängung von Geldbußen vorzusehen, soweit diese gegen Behörden und öffentliche Stellen verhängt werden können. § 28 macht von dieser Möglichkeit Gebrauch, soweit die Geldbußen öffentliche Stellen (§ 2 Absatz 1 und 2) und die nicht legislative Tätigkeit des Abgeordnetenhauses betreffen würden. Dies gilt nicht, soweit öffentliche Stellen am Wettbewerb teilnehmen. Durch die Beschränkung der Möglichkeit zur Verhängung von Geldbußen gegen nicht am Wettbewerb teilnehmende öffentliche Stellen soll eine Verringerung des Verwaltungsaufwandes bei der Aufsichtsbehörde, bei der vom Bußgeld betroffenen öffentlichen Stelle und bei den Gerichten erreicht werden. Wegen der Finanzierung der nicht am Wettbewerb teilnehmenden öffentlichen Stellen aus öffentlichen Mitteln wäre der Sanktionscharakter eines Bußgeldes geringer und stünde zu den damit verbundenen Rechtsverfolgungskosten, die ebenfalls öffentliche Mittel binden, in keinem angemessenen Verhältnis. Für öffentliche Stellen, die am Wettbewerb teilnehmen und damit zumindest teilweise eigene Mittel erwirtschaften, ist jedoch der Sanktionscharakter eines Bußgeldes nicht in gleichem Maße eingeschränkt. Zudem soll die Möglichkeit zur Verhängung eines Bußgeldes die Entstehung eines möglichen Wettbewerbsvorteils gegenüber nicht-öffentlichen Wettbewerbern verhindert werden.
Wird nur ein Teil der Tätigkeit der öffentlichen Stelle im Wettbewerb ausgeübt, unterfällt auch nur dieser Teil der Bemessung der Höhe einer möglichen Geldbuße.

Zu § 29 Ordnungswidrigkeiten, Strafvorschriften

Artikel 84 Absatz 1 der Verordnung (EU) 2016/679 berechtigt und verpflichtet die Mitgliedstaaten, andere, als in der Verordnung selber festgelegte Sanktionen für Verstöße gegen die Verordnung festzulegen, die wirksam, verhältnismäßig und abschreckend sein müssen. Aufgrund dieser Vorschrift übernimmt § 29 Regelungen aus § 32 des bisher geltenden Berliner

Datenschutzgesetzes, jedoch erfolgt eine Differenzierung zwischen Ordnungswidrigkeiten und Straftaten.

Zu Absatz 1
Die bisher als Straftatbestand vorgesehenen Handlungsalternativen werden zu Ordnungswidrigkeiten. Die Begehungsformen sind jedoch nicht mehr wie in § 32 Absatz 1 des bisher geltenden Berliner Datenschutzgesetzes auf die Übermittlung, Veränderung, den Abruf oder das Verschaffen aus verschlossenen Behältnissen beschränkt, sondern umfassen alle Modalitäten einer unbefugten Verarbeitung, namentlich auch die unbefugte Erhebung personenbezogener Daten.
Die Möglichkeit zur Schaffung einer Ordnungswidrigkeitenvorschrift besteht nach Artikel 84 Absatz 1 der Verordnung (EU) 2016/679. Danach können die Mitgliedstaaten andere Sanktionen für Verstöße gegen die Verordnung (EU) 2016/679 festlegen, insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 unterliegen. Absatz 1 stellt eine andere Sanktion, als die in Artikel 83 der Verordnung (EU) 2016/679 vorgesehenen dar, weil sie sich nicht an den Verantwortlichen oder Auftragsverarbeiter richtet, sondern an jede Person, insbesondere an dem Verantwortlichen unterstellte Personen, die gemäß Artikel 29 der Verordnung (EU) 2016/679 zur rechtmäßigen Verarbeitung personenbezogener Daten verpflichtet sind.

Zu Absatz 2
Die in § 32 Absatz 2 des bisher geltenden Berliner Datenschutzgesetzes enthaltenen Qualifikationsmerkmale wurden übernommen und führen nun in Verbindung mit dem objektiven Tatbestand des Absatz 1 zur Strafbarkeit. Durch die Verbindung mit Absatz 1 wird die Strafbarkeit ebenfalls auf die weiteren Modalitäten einer unbefugten Verarbeitung erweitert.

Zu Absatz 3
Die Antragsbefugnis für die Verfolgung der Straftat nach Absatz 2 wurde aus § 32 Absatz 3 des bisher geltenden Berliner Datenschutzgesetzes übernommen und um die Antragsbefugnis des Verantwortlichen ergänzt.

Zu Absatz 4
Die Regelung dient dem verfassungsrechtlichen Verbot einer Selbstbezichtigung. Zudem soll die Motivation zur Meldung einer Verletzung des Schutzes personenbezogener Daten nicht dadurch verringert werden, dass die durch die Meldung verfügbar werdenden Informationen zur Einleitung eines Straf- oder Bußgeldverfahrens führen können.

Zu Teil 3
Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680

Teil 3 dient der Umsetzung der Richtlinie (EU) 2016/680 in das Berliner Landesrecht.

Zu Kapitel 1 Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Zu § 30 Anwendungsbereich

§ 30 legt den Anwendungsbereich gemäß Artikel 2 Absatz 1 der Richtlinie (EU) 2016/680 für die Erfüllung der in Artikel 1 Absatz 1 der Richtlinie genannten Zwecke fest.

Zu den Absätzen 1 und 2
Der Anwendungsbereich von Teil 3 ist eröffnet, soweit öffentliche Stellen personenbezogene Daten zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten verarbeiten. Diese Zwecke schließen die Vollstreckung ein, ebenso den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit.
Teil 3 gilt für alle öffentlichen Stellen, die Daten zu den genannten Zwecken verarbeiten. Dies sind insbesondere Der Polizeipräsident in Berlin, die Amts- und Staatsanwaltschaft, aber auch die Ordnungsbehörden.
Für Behörden, die personenbezogene Daten auch in anderem Zusammenhang als mit Straftaten oder Ordnungswidrigkeiten verarbeiten (insbesondere die Ordnungsbehörden), ist der Anwendungsbereich von Teil 3 nur unter den folgenden Voraussetzungen eröffnet:

1. Die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten, einschließlich der damit verbundenen Vollstreckung und Gefahrenverhütung oder Gefahrenabwehr muss zu den gesetzlichen Aufgaben der datenverarbeitenden Behörde gehören und in deren Zuständigkeit fallen.
So ist beispielsweise im Bereich des ASOG die Aufgabe der Verhütung von Straftaten und die Vorsorge für die Verfolgung von Straftaten ausschließlich der Polizei zugewiesen (§ 1 Absatz 3 ASOG). Die Verarbeitung personenbezogener Daten durch eine Ordnungsbehörde zu diesen Zwecken könnte nur dann in den Anwendungsbereich des Teils 3 fallen, wenn spezialgesetzlich eine von § 1 Absatz 3 ASOG abweichende Aufgabenzuweisung besteht.

2. Soweit die gesetzlichen Aufgaben und Zuständigkeiten einer öffentlichen Stelle auch andere Zwecke als die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten, einschließlich der damit verbundenen Vollstreckung und Gefahrenverhütung oder Gefahrenabwehr umfassen, fallen nur solche Verarbeitungen personenbezogener Daten in den Anwendungsbereich des Teils 3, die einen konkreten Bezug zu Straftaten oder Ordnungswidrigkeiten aufweisen. Dies ergibt sich aus dem Erwägungsgrund 12 Satz 4 der Richtlinie (EU) 2016/680.
Beispielsweise fallen die Tätigkeiten des Verkehrsüberwachungsdienstes der bezirklichen Ordnungsämter in den Anwendungsbereich des Teils 3, weil die Verkehrsüberwachung von Beginn an zum Zweck der Ermittlung, Aufdeckung und Verfolgung von Ordnungswidrigkeiten erfolgt. Der Straßenverkehrsbehörde im Ordnungsamt sind hingegen Aufgaben wie zum Beispiel die Anordnung von Halteverboten zugewiesen, die nicht vordergründig die Ermittlung, Aufdeckung und Verfolgung von Ordnungswidrigkeiten bezwecken. Die Verarbeitung personenbezogener Daten zur Erfüllung dieser Aufgaben unterfällt nicht dem Teil 3, sondern der Verordnung (EU) 2016/679 und ergänzend dem Teil 1 und 2, sowie gegebenenfalls bereichsspezifischem Recht. Erst wenn ein solches Verwaltungsverfahren in ein konkretes Ordnungswidrigkeitenverfahren übergeht, ist der Anwendungsbereich von Teil 3 eröffnet.

3. Soweit die Verarbeitung personenbezogener Daten zum Schutze vor oder zur Abwehr von Gefahren für die öffentliche Sicherheit erfolgt, muss sich die Gefahr auf konkrete Straftaten oder Ordnungswidrigkeiten beziehen. Der Begriff der Gefahr für die öffentliche Sicherheit ist aufgrund der Gestaltung des Anwendungsbereichs der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 nicht deckungsgleich mit dem nationalen polizeirechtlichen Gefahrenbegriff, welcher auch die Wahrscheinlichkeit einer Rechtsgutbeeinträchtigung umfassen

kann, die nicht straf- oder bußgeldbewehrt ist. Aus den Erwägungsgründen 5 ff., insbesondere aus dem Erwägungsgrund 12 der Richtlinie (EU) 2016/680 kann abgeleitet werden, dass der Anwendungsbereich im Wesentlichen auf die Tätigkeiten von Strafverfolgungsbehörden, zu denen der europäische Gesetzgeber insbesondere die Polizei zählt, ausgerichtet ist. Für solche Strafverfolgungsbehörden können auch Tätigkeiten im Vorfeld konkreter Straftaten der Richtlinie und damit dem Teil 3 des Gesetzes unterfallen, wenn damit strafrechtlich abgesicherte Interessen der Gesellschaft geschützt werden. Für andere als originäre Strafverfolgungsbehörden ergibt sich jedoch aus Satz 4 des Erwägungsgrundes 12 der Richtlinie (EU) 2016/680, dass für die Verarbeitung personenbezogener Daten für solche Behörden eine genaue Trennung nach den Aufgaben erforderlich ist und Aufgaben, die nicht im Zusammenhang mit konkreten Strafverfahren stehen, der Verordnung (EU) 2016/679 unterfallen sollen.

In den Anwendungsbereich des Teils 3 fallen sowohl Tätigkeiten im Zusammenhang mit Straftaten, als auch Tätigkeiten im Zusammenhang mit Ordnungswidrigkeiten. Der Begriff der Straftat im Sinne der Richtlinie (EU) 2016/680 unterliegt nach dem Erwägungsgrund 13 der Richtlinie (EU) 2016/680 einem eigenständigen unionsrechtlichen Verständnis. Das System der Unterscheidung zwischen Straftaten und Ordnungswidrigkeiten existiert nicht in allen Mitgliedsstaaten, was zur Folge hätte, dass Handlungen, die in der Bundesrepublik Deutschland Ordnungswidrigkeiten darstellen, in anderen Mitgliedstaaten aber als Straftaten behandelt würden, unterschiedlichen Datenschutzregimen unterfallen würden. Dies würde der in Erwägungsgrund 7 der Richtlinie (EU) 2016/680 zum Ausdruck kommenden Intention widersprechen, die von europaweit einheitlichen und gleichwertigen Vorschriften ausgeht. Auch aus dem Erwägungsgrund 12 der Richtlinie (EU) 2016/680 ergibt sich, dass die Verarbeitung personenbezogener Daten durch die Strafverfolgungsbehörden umfassend nach den Regeln der Richtlinie erfolgen soll. Dem würde es widersprechen, wenn bei einem möglichen Wechsel zwischen Straf- und Bußgeldverfahren unterschiedliche Regelungen anzuwenden wären.

Zu Absatz 3
Öffentliche oder nicht-öffentliche Auftragsverarbeiter, denen durch Rechtsvorschriften keine eigenen der in § 30 genannten Aufgaben übertragen wurden, unterfallen nur denjenigen Regelungen des Teils 3, in denen Auftragsverarbeiter gesondert adressiert sind.

Zu § 31 Begriffsbestimmungen

Die Begriffsbestimmungen in § 31 wurden zum Zweck der Umsetzung von Artikel 3 der Richtlinie (EU) 2016/680 aufgenommen. Zur besseren Übersicht wurden die in Artikel 10 der Richtlinie (EU) 2016/680 genannten besonderen Kategorien personenbezogener Daten in Nummer 14 aufgenommen. Der Begriff der Einwilligung in Nummer 17 entspricht dem Begriff aus Artikel 4 Nummer 11 der Verordnung (EU) 2016/679.

Zu § 32 Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Die Vorschrift dient der Umsetzung von Artikel 4 Absatz 1 der Richtlinie (EU) 2016/680.

Zu Kapitel 2 Rechtsgrundlagen der Verarbeitung

Zu § 33 Verarbeitung besonderer Kategorien personenbezogener Daten

Die Vorschrift dient der Umsetzung von Artikel 10 der Richtlinie (EU) 2016/680.

Zu Absatz 1
Absatz 1 schafft eine eigene Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten. Die in Absatz 1 Nummer 1 genannten Aufgaben werden durch gesonderte Rechtsvorschrift übertragen.

Zu Absatz 2
Nach Absatz 2 sind bei der Verarbeitung besonderer Kategorien personenbezogener Daten immer auch geeignete Garantien vorzusehen, die dem besonderen Interesse der betroffenen Personen an einem möglichst hohen Schutzniveau für diese Daten entsprechen. Die beispielhafte Aufzählung möglicher Garantien in Absatz 2 Satz 2 ist nicht abschließend. Die Geeignetheit der Auswahl einer oder mehrerer der genannten Maßnahmen oder weiterer Maßnahmen richtet sich nach den konkreten Umständen des Einzelfalles.

Zu § 34 Verarbeitung zu anderen Zwecken

Die Vorschrift dient der Umsetzung von Artikel 4 Absatz 2 der Richtlinie (EU) 2016/680. Satz 1 stellt klar, dass unter den Voraussetzungen von § 30 der Verantwortliche nicht auf einen der dort genannten Zwecke beschränkt ist, solange auch die Voraussetzungen für die Verarbeitung zu einem anderen der dort genannten Zwecke vorliegen. Zusätzliche Anforderungen an eine Zweckänderung innerhalb der in § 30 genannten Zwecke (so etwa der Grundsatz der hypothetischen Datenneuerhebung, vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 und 1 BvR 1140/06) werden in den Fachgesetzen umgesetzt.

Zu § 35 Verarbeitung zu wissenschaftlichen, historischen, archivarischen und statistischen Zwecken

§ 35 dient der Umsetzung von Artikel 4 Absatz 3 der Richtlinie (EU) 2016/680.

Zu Absatz 1
Absatz 1 enthält die Befugnis zu einer Verarbeitung personenbezogener Daten zu den genannten Zwecken. Die Verarbeitung ist jedoch nicht zu jedem wissenschaftlichen, historischen, archivarischen oder statistischen Zweck zulässig, sondern die Zwecke müssen zur Erfüllung einer der in § 30 Absatz 1 oder 2 genannten Aufgaben erfolgen. Somit könnte beispielsweise die Verarbeitung personenbezogener Daten für ein Forschungsvorhaben zur Ermittlung der Auswirkungen konkreter Strafmaßnahmen auf die Verhütung weiterer Taten unter die Norm fallen, wohingegen Grundlagenforschung nicht der Norm unterfällt.

Zu Absatz 2
In Absatz 2 wird die Vorgabe aus Artikel 4 Absatz 3 der Richtlinie (EU) 2016/680 zur Einrichtung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person umsetzt und hierfür die Regelung aus § 30 Absatz 1 Satz 2 des bisher geltenden Berliner Datenschutzgesetzes übernommen. Als Mindestvorgabe muss eine frühestmögliche Anonymisierung der personenbezogenen Daten erfolgen. Die Anforderungen an eine Anonymisierung ergeben sich

aus der Definition desweniger weit reichenden Begriffs der Pseudonymisierung in § 31 Nummer 5. Während das Merkmal einer Pseudonymisierung die reversible Trennung personenbezogener Daten zu einer bestimmten Person umfasst, liegt eine Anonymisierung bei einer endgültigen Trennung vor, wenn auch trotz Hinzuziehung zusätzlicher Informationen die personenbezogenen Daten keiner spezifischen Person mehr zugeordnet werden können.
Satz 2 sieht in jedem Fall zumindest eine Pseudonymisierung vor und gestattet eine Aufhebung der Trennung der personenbezogenen Daten zu einer spezifischen Person nur, wenn dies für den jeweiligen Zweck erforderlich ist.
Im Falle der Verarbeitung besonderer Kategorien personenbezogener Daten ist zudem § 33 Absatz 2 zu beachten, der ebenfalls die Einhaltung geeigneter Garantien vorschreibt und Beispiele dafür nennt.
Die weitergehende Konkretisierung geeigneter Garantien erfolgt im bereichsspezifischen Recht.

Zu Absatz 3
Absatz 3 enthält unter engen Voraussetzungen Beschränkungen der Rechte der betroffenen Person. Die Beschränkungen gelten nur für Forschungs- und Statistikzwecke und auch nur, soweit und solange diese Zwecke durch die Wahrnehmung der Rechte unmöglich gemacht oder ernsthaft beeinträchtigt werden würden. Das Auskunftsrecht nach § 43 ist darüber hinaus auch eingeschränkt, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

Zu Absatz 4
§ 35 tritt am 30. September 2025 außer Kraft.

Zu § 36 Einwilligung

Durch die Vorschrift werden Regelungen aus Artikel 7 der Verordnung (EU) 2016/679 und aus § 6 des bisher geltenden Berliner Datenschutzgesetz in den Anwendungsbereich der Richtlinie (EU) 2016/680 übernommen.

Zu Absatz 1
Absatz 1 entspricht Artikel 7 Absatz 1 der Verordnung (EU) 2016/679.

Zu Absatz 2
Absatz 2 entspricht Artikel 7 Absatz 2 Satz 1 der Verordnung (EU) 2016/679.

Zu Absatz 3
Absatz 3 entspricht Artikel 7 Absatz 3 Sätze 1, 2 und 3 der Verordnung (EU) 2016/679.

Zu Absatz 4
Absatz 4 Satz 1 entspricht § 6 Absatz 5 Satz 1 des bisher geltenden Berliner Datenschutzgesetzes. § 6 Absatz 5 Satz 2 des bisher geltenden Berliner Datenschutzgesetzes, wonach die die Einwilligung insbesondere unwirksam ist, wenn sie durch Androhung ungesetzlicher Nachteile oder durch fehlende Aufklärung bewirkt wurde, nennt zwei Beispiele, die von der Formulierung in Absatz 4 Satz 1 bereits erfasst sind. Absatz 4 Satz 3 entspricht § 6 Absatz 3 Satz 1; Absatz 4 Satz 4 entspricht § 6 Absatz 3 Satz 3 des bisher geltenden Berliner Datenschutzgesetzes.

Zu Absatz 5
Absatz 5 entspricht § 6 Absatz 5 Satz 3 des bisher geltenden Berliner Datenschutzgesetzes.

Zu § 37 Verarbeitung auf Weisung des Verantwortlichen

Die Vorschrift dient der Umsetzung von Artikel 23 der Richtlinie (EU) 2016/680.

Zu § 38 Datengeheimnis

Durch die Vorschrift wird die bereits in § 8 des bisher geltenden Berliner Datenschutzgesetzes enthaltene Regelung in den Anwendungsbereich der Richtlinie übernommen.

Zu § 39 Automatisierte Einzelentscheidung

Die Vorschrift, die vergleichbar bereits in § 15a des bisher geltenden Berliner Datenschutzgesetzes enthalten ist, dient der Umsetzung von Artikel 11 der Richtlinie (EU) 2016/680.
Eine Entscheidung ist mit einer nachteiligen Rechtsfolge für die betroffene oder einer erheblichen Beeinträchtigung der betroffenen Person verbunden, wenn die Entscheidung Außenwirkung besitzt. Hierunter fallen insbesondere Verwaltungsakte gegenüber der betroffenen Person. Interne Zwischenfestlegungen oder -auswertungen, die Ausfluss automatisierter Prozesse sind, fallen nicht darunter.
Als geeignete Garantien zum Schutz der betroffenen Person kommen nach dem Erwägungsgrund 38 Satz 2 der Richtlinie (EU) 2016/680 die spezifische Unterrichtung der betroffenen Person und die Unterrichtung über das Recht, das Eingreifen einer Person zu erwirken, den eigenen Standpunkt darzulegen, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung oder auf Anfechtung der Entscheidung, in Frage.

Zu § 40 Gemeinsames Verfahren und automatisiertes Verfahren auf Abruf

Zur einheitlichen Anwendbarkeit der Regelungen über gemeinsame Verfahren und automatisierte Verfahren auf Abruf, unabhängig davon, ob diese Verfahren zu Zecken, die in den Anwendungsbereichs der Verordnung (EU) 2016/679 oder der Richtlinie(EU) 2016/680 fallen, verarbeitet werden, werden die Regelungen aus § 21 und die hierzu gehörende Regelung aus § 16 Absatz 2 auch in den Anwendungsbereich der Richtlinie (EU) 2016/680 übernommen.

Zu Kapitel 3 Rechte der betroffenen Person

Zu § 41 Allgemeine Informationen zu Datenverarbeitungen

Die Vorschrift dient der Umsetzung von Artikel 13 Absatz 1 der Richtlinie (EU) 2016/680.
Die Informationspflichten, die unabhängig von eventuell geltend gemachten Auskunftsrechten der betroffenen Personen bestehen, können nach dem Erwägungsgrund 42 der Richtlinie

(EU) 2016/680 beispielsweise durch Veröffentlichung der Informationen auf der Website der zuständigen Behörde erfüllt werden. Durch die Bereitstellung der in § 41 genannten Informationen in allgemeiner Form sollen sich betroffene Personen unabhängig von konkreten Datenverarbeitungen einen Überblick über die Zwecke der beim Verantwortlichen vorgenommenen Verarbeitungen und über bestehende Betroffenenrechte sowie Möglichkeiten zur Wahrnehmung dieser Rechte verschaffen können. Die nach § 41 zu erteilenden Informationen stellen eine Mindestvorgabe dar und können um weitere Informationen ergänzt werden.

Zu § 42 Benachrichtigung betroffener Personen

Zu Absatz 1
Absatz 1 dient der Umsetzung von Artikel 13 Absatz 2 der Richtlinie (EU) 2016/680 und betrifft Informationen, die unabhängig von einem Antrag der betroffenen Person bereitzustellen sind. Die gemäß Absatz 1 Nummer 4 mitzuteilenden Informationen über Kategorien von Empfängern müssen erkennen lassen, wenn es sich um Empfänger in Drittländern oder internationalen Organisationen handelt.

Zu Absatz 2
Durch Absatz 2 wird von den Möglichkeiten des Artikel 13 Absatz 3 der Richtlinie (EU) 2016/680 Gebrauch gemacht, in bestimmten Fällen eine Benachrichtigung der betroffenen Person aufschieben, einschränken oder unterlassen zu können.

Zu Absatz 3
Das Erfordernis der Zustimmung der in Absatz 3 genannten Stellen berücksichtigt, dass bei diesen Stellen zusätzliche Erkenntnisse zu einem Ablehnungsgrund nach Absatz 2 vorhanden sein können.

Zu Absatz 4
Im Falle der Einschränkung einer Benachrichtigung hat die betroffene Person das Recht, die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit anzurufen und die Entscheidung des Verantwortlichen überprüfen zu lassen. Über diese Möglichkeiten hat der Verantwortliche die betroffene Person hinzuweisen. Die Hinweispflicht gilt nicht, wenn wegen des Vorliegens der Voraussetzungen des Absatzes 2 gar keine Benachrichtigung erfolgen kann, diese also entweder aufgeschoben oder unterlassen wird.

Zu § 43 Auskunftsrecht

Durch § 43 wird Artikel 14 der Richtlinie (EU) 2016/680 umgesetzt und zugleich mit den nach Artikel 15 der Richtlinie (EU) 2016/680 möglichen Ausnahmen verbunden.

Zu Absatz 1
Der Umfang der zu erteilenden Auskunft wird in Absatz 1 festgelegt. Nummer 9 enthält über die Vorgaben des Artikels 14 der Richtlinie (EU) 2016/680 hinaus eine Regelung aus Artikel 15 Absatz 1 Buchstabe h der Verordnung (EU) 2016/679, die wesentliche Elemente der Regelung in § 16 Absatz 1 Nummer 4 des bisher geltenden Berliner Datenschutzgesetz enthält. Die Informationen über das Bestehen einer automatisierten Entscheidungsfindung und Informati-

onen über die involvierte Logik stellen nach dem Erwägungsgrund 38 Satz 2 der Richtlinie eine geeignete Garantie im Sinne von Artikel 11 Absatz 1 der Richtlinie (EU) 2016/680 dar.

Zu Absatz 2
Die Regelung dient dem Ausgleich zwischen den Rechten der betroffenen Person und einer möglichst effizienten Verwaltungstätigkeit. Den in Absatz 2 genannten Fallgruppen ist gemein, dass die personenbezogenen Daten zwar bei der öffentlichen Stelle noch vorliegen, jedoch nicht mehr aktiv genutzt werden und genutzt werden können und in denen die Daten auch sonst nicht zur Grundlage von Entscheidungen gegenüber der betroffenen Person gemacht werden. In diesen Fällen liegt keine maßgebliche Beeinträchtigung von Rechten, einschließlich des Rechts auf informationelle Selbstbestimmung, der betroffenen Person vor, so dass die Interessen der öffentlichen Stelle an einer effizienten Verwaltungstätigkeit in den Vordergrund rücken.

Zu Absatz 3
Als Beispiel für einen Fall, der unter die Regelung des Absatzes 3 fällt, können ins Unreine geschriebene handschriftliche Aufzeichnungen von Polizeibediensteten im Rahmen einer Anzeigenaufnahme dienen. Im Rahmen eines späteren Auskunftsbegehrens ist es nicht unverhältnismäßig, die Auskunft nur dann auf solche Aufzeichnungen zu erstrecken, wenn die betroffene Person auf die handschriftlichen Aufzeichnungen hingewiesen hat und wenn die Aufzeichnungen auch noch vorhanden sind. Die Verpflichtungen der Beschäftigten zum datenschutzgerechten Umgang mit handschriftlichen Aufzeichnungen werden durch die Vorschrift nicht berührt.

Zu Absatz 4
Das Auskunftsrecht aufgrund von Artikel 15 der Richtlinie (EU) 2016/680 wird gleichermaßen wie das Benachrichtigungsrecht nach § 42 beschränkt, um in den genannten Fällen die Aufgabenerfüllung nicht durch eine frühzeitige Kenntnis der betroffenen Person zu gefährden. Ebenso wie in § 42 Absatz 2 hat der Verantwortliche eine Interessenabwägung durchzuführen und dabei auch zu berücksichtigen, ob das Auskunftsrecht nicht zumindest teilweise besteht. Die Auskunft ist zu erteilen, sobald die Gründe für die Verweigerung nicht mehr bestehen.

Zu Absatz 5
Das Erfordernis der Zustimmung der in Absatz 5 genannten Stellen berücksichtigt, dass bei diesen Stellen zusätzliche Erkenntnisse zu einem Ablehnungsgrund nach § 42 Absatz 2 vorhanden sein können.

Zu Absatz 6
Durch die Regelung wird Artikel 15 Absatz 3 der Richtlinie (EU) 2016/680 umgesetzt.

Zu Absatz 7
Absatz 7 dient der Umsetzung von Artikel 17 der Richtlinie (EU) 2016/680 und enthält neben der Wiederholung des in § 46 enthaltenen Rechts zur Anrufung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit Regelungen für einen Ausgleich zwischen den Rechten der betroffenen Person und den öffentlichen Interessen.

Zu Absatz 8
In Absatz 8 wird Artikel 15 Absatz 4 der Richtlinie (EU) 2016/680 umgesetzt.

Zu § 44 Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

Artikel 16 der Richtlinie (EU) 2016/680 sieht in den Fällen der unrichtigen, unvollständigen oder unrechtmäßigen Verarbeitung personenbezogener Daten vor, dass sowohl der betroffenen Person Rechte auf Berichtigung, Vervollständigung, Löschung oder Einschränkung der Verarbeitung zustehen sollen, als auch, dass dem Verantwortlichen damit korrespondierende Pflichten auferlegt werden sollen. Während die Pflichten des Verantwortlichen in § 61 geregelt werden, dient § 44 der Umsetzung der Rechte der betroffenen Person aus Artikel 16 der Richtlinie (EU) 2016/680.

Zu Absatz 1
Die Vorschrift sieht ein Recht zur Berichtigung unrichtiger personenbezogener Daten vor, stellt in Satz 2 allerdings klar, dass die Änderung einer Aussage oder Beurteilung nicht aufgrund dieser Vorschrift beansprucht werden können soll. Dies entspricht dem Erwägungsgrund 47 der Richtlinie (EU) 2016/680, der von einem Berichtigungsrecht nur bezüglich der personenbezogenen Daten ausgeht. Beispielhaft wird dort der Inhalt von Zeugenaussagen genannt, die nicht dem Berichtigungsrecht unterfallen sollen. Ausgehend von diesen Erwägungen sind demnach insbesondere persönliche Eindrücke und Meinungen von dem Recht auf Berichtigung ausgenommen. Dies gilt auch für polizeifachliche Bewertungen.
Im Falle des Bestreitens der Richtigkeit und deren Nichterweislichkeit ist in Satz 3 eine Einschränkung der Verarbeitung vorgesehen. Die Regelung entspricht § 17 Absatz 2 Satz 2 des bisher geltenden Berliner Datenschutzgesetzes.
Das in Absatz 1 Satz 5 geregelte Recht auf Vervollständigung umfasst auch eine ergänzende Erklärung der betroffenen Person.

Zu Absatz 2 und 3
Während Absatz 2 diejenigen Fälle regelt, in denen grundsätzlich ein Recht der betroffenen Person besteht, die Löschung der personenbezogenen Daten verlangen zu können, regelt Absatz 3 die Ausnahmen davon und modifiziert das Recht auf Löschung, indem der Verantwortliche nicht zur Löschung, sondern zur Einschränkung der Verarbeitung verpflichtet wird. Die Gründe in Absatz 3 Satz 1 Nummer 1 und 2 entsprechen dem Erwägungsgrund 47 Satz 4 und Artikel 16 Absatz 3 Satz 1 Buchstabe b der Richtlinie (EU) 2016/680. Die unter Nummer 3 vorgesehene Möglichkeit, die an eine Regelung in § 48 des ASOG angelehnt ist, wegen unverhältnismäßigen Aufwandes von einer Löschung absehen zu können, ist auf enge Ausnahmefälle außerhalb einer IT-gestützten Datenverarbeitung beschränkt. Absatz 3 Satz 2 führt im Ergebnis zu einem Verarbeitungsverbot der eingeschränkten Daten, außer zu dem Zweck, der Grund für das Unterbleiben der Löschung war. Dies ergibt sich als notwendige Konsequenz aus Satz 4 des Erwägungsgrundes 47 und aus Artikel 16 Absatz 3 Satz 1 Buchstabe b der Richtlinie (EU) 2016/680, weil ohne Nutzungsmöglichkeit der eingeschränkten Daten zu dem Zweck, welcher der Löschung entgegenstand, die genannten Regelungen der Richtlinie eine Löschung vorsehen müssten.

Zu Absatz 6 und 7
Absatz 6 sieht in Satz 1 als Regelfall eine Unterrichtung der betroffenen Person vor, wenn deren Verlangen nicht in vollem Umfang nachgekommen wurde. In anderen Vorschriften enthaltene Verpflichtungen, die eine Benachrichtigung auch für die Fälle vorsehen, in denen dem Verlangen der betroffenen Person vollständig nachgekommen wurde, bleiben von der Regelung unberührt. Abweichend von dem Regelfall in Absatz 6 Satz 1 sind in Satz 2 und 3

aufgrund von Artikel 16 Absatz 4 Satz 2 der Richtlinie (EU) 2016/680, Einschränkungen von der Unterrichtungspflicht vorgesehen. Zum Ausgleich der Einschränkungen wird der betroffenen Person die Ausübung ihrer Rechte über die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit eingeräumt.

Zu § 45 Verfahren für die Ausübung der Rechte der betroffenen Person

§ 45 dient der Umsetzung von Artikel 12 der Richtlinie (EU) 2016/680.

Zu § 46 Anrufung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit

§ 46 dient der Umsetzung von Artikel 52 der Richtlinie (EU) 2016/680.

Zu § 47 Rechtsschutz gegen Entscheidungen oder bei Untätigkeit der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit

Die Vorschrift dient der Umsetzung von Artikel 53 der Richtlinie (EU) 2016/680 und ermöglicht gerichtlichen Rechtsschutz gegen rechtsverbindliche Entscheidungen der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Unverbindliche Entscheidungen, wie Stellungnahmen oder Empfehlungen, werden von der Vorschrift nicht erfasst.

Zu Kapitel 4 Pflichten der Verantwortlichen und Auftragsverarbeiter

Zu § 48 Auftragsverarbeitung

§ 48 dient der Umsetzung von Artikel 22 der Richtlinie (EU) 2016/680.

Zu Absatz 1 und 8
Absatz 1 und Absatz 8 regeln die Verantwortlichkeit. Danach liegt als Regelfall die Verantwortlichkeit bei den Beauftragenden. Diese sollen betroffenen Personen als alleinige Ansprechpersonen dienen. Eine solche Regelung ist in all denjenigen Fällen zur Vereinfachung des Verfahrens für alle Beteiligten sinnvoll, in denen der Auftragsverarbeiter nicht von den Weisungen des Auftraggebers abweicht. In den Fällen, in denen der Auftragsverarbeiter weisungswidrig eine Verarbeitung vornimmt, ist nach Absatz 8 in Umsetzung von Artikel 22 Absatz 5 der Richtlinie (EU) 2016/680 der Auftragsverarbeiter Verantwortlicher.

Zu Absatz 2
Absatz 2 dient der Umsetzung von Artikel 22 Absatz 1 der Richtlinie (EU) 2016/680.

Zu Absatz 3
Absatz 3 dient der Umsetzung von Artikel 22 Absatz 2 der Richtlinie (EU) 2016/680.

Zu Absatz 4

In Absatz 4 wird die Regelung aus Artikel 28 Absatz 4 der Verordnung (EU) 2016/679 in den Anwendungsbereich der Richtlinie (EU) 2016/680 übernommen.

Zu Absatz 5
Absatz 5 verbindet die Vorgaben in Artikel 22 Absatz 3 der Richtlinie (EU) 2016/680 mit den in § 3 Absatz 1 des bisher geltenden Berliner Datenschutzgesetzes enthaltenen Vorgaben an den Inhalt der zwischen dem Verantwortlichen und dem Auftragsverarbeiter abzuschließenden Vereinbarung.

Zu Absatz 6
Die in Absatz 6 vorgesehenen Anforderungen an die Form des Vertrages dienen der Umsetzung von Artikel 22 Absatz 4 der Richtlinie (EU) 2016/680.

Zu Absatz 7
Die Regelung betrifft Fälle, in denen eine Wartung der technischen Systeme durch einen Dritten erfolgt und in denen der Dritte keinen Zugang zu personenbezogenen Daten erhalten soll. Kann die Zugriffsmöglichkeit nicht ausgeschlossen werden, sollen die Vorgaben der Absätze 1 bis 6 für einen möglichst lückenlosen Schutz der personenbezogenen Daten entsprechend angewendet werden.

Zu § 49 Gemeinsam Verantwortliche

Die Vorschrift dient der Umsetzung von Artikel 21 der Richtlinie (EU) 2016/680.

Zu § 50 Anforderungen an die Sicherheit der Datenverarbeitung

Zu Absatz 1
Die Vorschrift dient der Umsetzung von Artikel 29 Absatz 1 der Richtlinie (EU) 2016/680. Die im Rahmen der Abwägung zu berücksichtigenden technisch-organisatorischen Maßnahmen umfassen auch die einschlägigen Standards und Empfehlungen, insbesondere technische Richtlinien, des Bundesamts für Sicherheit in der Informationstechnik.

Zu Absatz 2
In Absatz 2 werden Regelungen aus Artikel 32 Absatz 1 Buchstaben a bis c der Verordnung (EU) 2016/679 in den Umsetzungsbereich der Richtlinie (EU) 2016/680 übernommen.

Zu Absatz 3
Absatz 3 übernimmt eine Regelung aus § 9 und dem Anhang zu § 9 Satz 1 des Bundesdatenschutzgesetzes.

Zu § 51 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit

Die Vorschrift dient der Umsetzung von Artikel 30 der Richtlinie (EU) 2016/680.

Anknüpfungspunkt einer Meldung nach § 51 sind entsprechend der systematischen Stellung der Vorschrift im Zusammenhang mit der Sicherheit der Verarbeitung Vorfälle, wie beispielsweise Datenabflüsse.
Die Dokumentation nach Absatz 5 muss qualitativ und quantitativ so beschaffen sein, dass der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit eine Überprüfung der Einhaltung der gesetzlichen Vorschriften ermöglicht wird.

Zu § 52 Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

§ 52 dient der Umsetzung von Artikel 31 der Richtlinie (EU) 2016/680.

Zu § 53 Durchführung einer Datenschutz-Folgenabschätzung

§ 53 dient der Umsetzung von Artikel 27 der Richtlinie (EU) 2016/680.
Zur Umsetzung der Vorgaben in Artikel 27 Absatz 2 der Richtlinie (EU) 2016/680 wurden Regelungen des Artikels 35 der Verordnung (EU) 2016/679 in den Anwendungsbereich der Richtlinie (EU) 2016/680 übernommen.

Zu Absatz 1
In Absatz 1 wurde die Regelung aus Artikel 35 Absatz 1 Satz 1 der Verordnung (EU) 2016/679 übernommen.

Zu Absatz 2
In Absatz 2 wurde die Regelung aus Artikel 35 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 übernommen.

Zu Absatz 3
Absatz 3 enthält eine Regelung aus Artikel 35 Absatz 2 der Verordnung (EU) 2016/679.

Zu Absatz 4
Der Mindestinhalt der Datenschutz-Folgenabschätzung entspricht Artikel 35 Absatz 7 der Verordnung (EU) 2016/679.

Zu Absatz 5
Die Verpflichtung des Verantwortlichen zur Überprüfung der Einhaltung der sich aus der Datenschutz-Folgenabschätzung ergebenden Maßgaben entspricht Artikel 35 Absatz 11 der Verordnung (EU) 2016/679. Die Erforderlichkeit einer Überprüfung kann sich insbesondere aus einer Änderung des Risikos für die Rechte und Freiheiten der betroffenen Personen aufgrund einer Veränderung der Verarbeitungsvorgänge ergeben.

Zu § 54 Zusammenarbeit mit der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit

Die Vorschrift dient der Umsetzung von Artikel 26 der Richtlinie (EU) 2016/680 und fasst die sich auch aus anderen Vorschriften ergebenden Kooperationsverpflichtungen und Kooperati-

onsbeziehungen zwischen dem Verantwortlichen und der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit zusammen.

Zu § 55 Anhörung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit

Die Vorschrift dient der Umsetzung von Artikel 28 der Richtlinie (EU) 2016/680.

Zu Absatz 2
In Absatz 2 werden Vorgaben aus Artikel 28 Absatz 4 der Richtlinie (EU) 2016/680 und Artikel 36 Absatz 3 der Verordnung (EU) 2016/679 zusammengeführt.

Zu § 56 Verzeichnis von Verarbeitungstätigkeiten

Zu Absatz 1
§ 56 dient der Umsetzung von Artikel 24 der Richtlinie (EU) 2016/680. Die in Artikel 24 Absatz 1 der Richtlinie (EU) 2016/680 vorgesehenen Angaben des Verzeichnisses wurden um weitere Angaben aus § 19 Absatz 2 Nummern 5, 6 und 8 des bisher geltenden Berliner Datenschutzgesetzes ergänzt und entsprechen so insgesamt denjenigen Angaben, die bereits nach geltendem Recht, allerdings nur für automatisierte Verarbeitungen, in die Dateibeschreibung aufzunehmen sind. Verantwortliche, die personenbezogene Daten sowohl nach der Verordnung (EU) 2016/679, als auch nach Teil 3 des Gesetzes verarbeiten, können ein einheitliches Verzeichnis, welches sowohl die Anforderungen des Artikels 30 der Verordnung (EU) 2016/679, als auch die Anforderungen des § 56 erfüllt, erstellen. Aus dem Erwägungsgrund 82 der Verordnung (EU) 2016/679 folgt, dass der Zweck des Verzeichnisses der Verarbeitungstätigkeiten nach der Verordnung (EU) 2016/679 darin besteht, die Einhaltung der Vorgaben der Verordnung nachweisen zu können. Die Aufnahme weitergehender Angaben in das Verzeichnis steht diesem Zweck nicht entgegen.

Das Verzeichnis soll „Kategorien von Tätigkeiten der Verarbeitung personenbezogener Daten“ enthalten, so dass nicht einzelne Datenverarbeitungsvorgänge Bestandteil des Verzeichnisses sind, sondern gleichartige Datenverarbeitungsvorgänge, die sinnvoll zu abgrenzbaren Kategorien zusammengefasst werden. Auch für die Inhalte des Verzeichnisses sind die Empfänger personenbezogener Daten, betroffene Personen und personenbezogene Daten, Übermittlungen personenbezogener Daten an Drittstaaten oder internationale Organisationen, Lösch- und Überprüfungsfristen und zugriffsberechtigte Personen oder Personengruppen zu Kategorien zusammenzufassen.

Zu Absatz 2
Absatz 2 setzt Artikel 24 Absatz 2 der Richtlinie (EU) 2016/680 um. Danach haben auch Auftragsverarbeiter ein Verzeichnis der Kategorien der jeweils für einen Verantwortlichen durchgeführten Auftragsverarbeitungen mit dem in Absatz 2 bestimmten Inhalt zu führen.

Zu Absatz 3 und 4
Die Regelungen dienen der Umsetzung von Artikel 24 Absatz 3 der Richtlinie (EU) 2016/680.

Zu § 57 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

§ 57 dient der Umsetzung von Artikel 20 der Richtlinie (EU) 2016/680 und betrifft die datenschutzfreundliche Gestaltung von Datenverarbeitungssystemen (Privacy by Design) und die Implementierung datenschutzfreundlicher Grundeinstellungen (Privacy by Default).

Zu § 58 Unterscheidung zwischen verschiedenen Kategorien personenbezogener Daten

§ 58 dient der Umsetzung von Artikel 6 der Richtlinie (EU) 2016/680. Die Rechtsfolgen der Unterscheidung, beispielsweise die Einrichtung unterschiedlicher Aussonderungsprüffristen, Rechte- oder Rollenkonzepte oder besondere Maßnahmen der Datensicherheit werden im Fachrecht geregelt.

Zu § 59 Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen

§ 59 dient der Umsetzung von Artikel 7 Absatz 1 der Richtlinie (EU) 2016/680. Die Rechtsfolgen aus der Unterscheidung, beispielsweise die Einrichtung unterschiedlicher Aussonderungsprüffristen, Rechte- oder Rollenkonzepte oder besondere Maßnahmen der Datensicherheit werden im Fachrecht geregelt.

Zu § 60 Verfahren bei Übermittlungen

Zu Absatz 1
Absatz 1 dient der Umsetzung von Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680.
Die Richtlinie sieht neben den Gründen der Unrichtigkeit oder fehlenden Aktualität auch vor, dass unvollständige Daten nicht übermittelt oder bereitgestellt werden sollen. Die Übernahme dieser Regelung würde jedoch ausschließen, dass eine Datenübermittlung gerade zu dem Zweck der Vervollständigung unvollständiger Daten erfolgt, so dass darauf verzichtet wurde. Die Begriffe *unrichtig* und *nicht mehr aktuell* sind zudem anhand des konkreten Verarbeitungszwecks der personenbezogenen Daten auszulegen. So können beispielsweise Adressen einer betroffenen Person, an der diese nicht mehr wohnhaft ist, veraltet sein, wenn es auf die aktuelle Adresse ankommt; sie können aber auch noch aktuell sein, wenn es auf den früheren Wohnort ankommt.

Zu Absatz 2
Absatz 2 dient der Umsetzung von Artikel 9 Absatz 3 der Richtlinie (EU) 2016/680. Die besonderen Bedingungen werden im Fachrecht geregelt und können beispielsweise Zweckbindungsregelungen bei der Weiterverarbeitung durch den Empfänger, das Verbot der Weiterübermittlung ohne Genehmigung oder Konsultationserfordernisse vor der Auskunftserteilung an die betroffene Person durch den Empfänger sein.

Zu Absatz 3
Absatz 3 dient der Umsetzung von Artikel 9 Absatz 4 der Richtlinie (EU) 2016/680.

Zu § 61 Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung

Spiegelbildlich zu § 44, welcher die Rechte der betroffenen Person auf Berichtigung, Vervollständigung und Löschung personenbezogener Daten regelt, enthält § 61 die Verpflichtung des Verantwortlichen, die Berichtigung, Vervollständigung oder Löschung beziehungsweise Einschränkung der Verarbeitung vorzunehmen. Ebenso wie § 44 dient § 61 der Umsetzung von Artikel 16 der Richtlinie (EU) 2016/680.

Zu Absatz 1 bis 3
Für die Absätze 1 bis 3 gelten die Ausführungen zu § 44 entsprechend.

Zu Absatz 4
Absatz 4 dient der Umsetzung von Artikel 5 der Richtlinie (EU) 2016/680.

Zu § 62 Protokollierung

§ 62 dient der Umsetzung von Artikel 25 der Richtlinie (EU) 2016/680.
Die in Absatz 2 vorgesehene Möglichkeit, die Protokolle für Strafverfahren verwenden zu können, ist nicht auf Straftaten im Zusammenhang mit Verstößen gegen Datenschutzvorschriften beschränkt.

Zu § 63 Vertrauliche Meldung von Verstößen

§ 63 dient der Umsetzung von Artikel 48 der Richtlinie (EU) 2016/680 und betrifft sowohl interne, als auch externe Hinweise auf Verstöße. Als Kontakt- und Beratungsstelle kann beispielsweise die oder der Datenschutzbeauftragte in Betracht kommen.

Zu Kapitel 5 Datenübermittlungen an Drittstaaten und an internationale Organisationen

Zu § 64 Allgemeine Voraussetzungen

Die Vorschrift dient der Umsetzung von Artikel 35 der Richtlinie (EU) 2016/680.
§ 64 enthält die Voraussetzungen, die regelmäßig bei einer Datenübermittlung an einen Drittstaat oder an eine internationale Organisation (§ 31 Nummer 17) vorliegen müssen.

Zu Absatz 1
Die Voraussetzungen der Nummern 1 und 2 müssen kumulativ vorliegen. Sofern kein Angemessenheitsbeschluss vorliegt, können die Voraussetzungen der Nummer 2 durch die spezielleren Vorgaben in den §§ 65 bis 67 ersetzt werden.

Zu Absatz 2

Zur Wahrung der Grundrechte darf selbst bei Vorliegen eines Angemessenheitsbeschlusses, der für ein Gebiet oder mehrere Sektoren in einem Drittland ein angemessenes Schutzniveau feststellt, keine Übermittlung erfolgen, wenn im Einzelfall Anlass zur Besorgnis besteht, dass ein elementaren rechtsstaatlichen Grundsätzen genügender Umgang mit den übermittelten personenbezogenen Daten nicht gewährleistet ist und wenn diese Besorgnis auch nach einer Prüfung durch den Verantwortlichen nicht beseitigt werden kann (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 und 1 BvR 1140/06). Die Regelung gilt auch in den Fällen der §§ 65 bis 67.

Zu § 65 Datenübermittlung bei geeigneten Garantien

§ 65 dient der Umsetzung von Artikel 37 der Richtlinie (EU) 2016/680.

Zu Absatz 1
Bei Vorliegen der Voraussetzungen kann eine Datenübermittlung an einen Drittstaat oder an eine internationale Organisation erfolgen, auch wenn kein Angemessenheitsbeschluss im Sinne von § 64 Absatz 1 Nummer 2 vorliegt. Bei Vorliegen der Voraussetzungen von § 64 Absatz 2 darf keine Übermittlung erfolgen.

Zu § 66 Datenübermittlung ohne geeignete Garantien

Die Vorschrift dient der Umsetzung von Artikel 38 der Richtlinie (EU) 2016/680.

Zu § 67 Sonstige Datenübermittlung an Empfänger in Drittstaaten

§ 67 dient der Umsetzung von Artikel 39 der Richtlinie (EU) 2016/680 und kann alle Stellen in Drittstaaten betreffen, die dem Verantwortlichen bei der Erfüllung seiner Aufgaben nach § 30 behilflich sein können, zum Beispiel Ersuchen an Finanzinstitutionen oder Telekommunikationsdienstleister, die notwendigerweise mit der Übermittlung personenbezogener Daten verbunden sind.

Zu Kapitel 6 Zusammenarbeit der Aufsichtsbehörden

Zu § 68 Gegenseitige Amtshilfe

Die Vorschrift dient der Umsetzung von Artikel 50 der Richtlinie (EU) 2016/680.

Zu Kapitel 7 Haftung und Sanktionen

Zu § 69 Schadensersatz und Entschädigung

Die Vorschrift dient der Umsetzung von Artikel 56 der Richtlinie (EU) 2016/680.

Zu § 70 Ordnungswidrigkeiten, Strafvorschriften

§ 70 dient der Umsetzung von Artikel 57 der Richtlinie (EU) 2016/680. Durch den Verweis auf § 29 besteht ein einheitlicher Maßstab für die unbefugte Verarbeitung personenbezogener Daten.

Zu Teil 4
Besondere Verarbeitungssituationen außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680

§ 71 Öffentliche Auszeichnungen und Ehrungen

Die Vorschrift regelt die Verarbeitung personenbezogener Daten für Zwecke der Vergabe staatlicher Auszeichnungen und Ehrungen.
Eine solche Regelung war in dem bisher geltenden Berliner Datenschutzgesetz nicht enthalten. Die Vergabe einer öffentlichen Auszeichnung oder Ehrung vollzieht sich ohne Begründungszwang und Überprüfbarkeit in einem rechtlich nur wenig reglementierten Raum. Dieser besondere Charakter der Vergabe öffentlicher Auszeichnungen und Ehrungen berührt besonders sensible Bereiche, so dass mit der Vorschrift für die Verarbeitung personenbezogener Daten spezielle datenschutzrechtliche Regelungen geschaffen werden.
Die Vergabe öffentlicher Auszeichnungen und Ehrungen ist eine Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt. Die Vergabe einer staatlichen Auszeichnung oder Ehrung ist ein außergerichtlicher Gunstbeweis, den die öffentliche Stelle der- oder demjenigen gewährt, die oder den sie für auszeichnungswürdig hält.
Die Verordnung (EU) 2016/679 ist daher nach deren Artikel 2 Absatz 2 Buchstabe a für die Verarbeitung personenbezogener Daten im Rahmen dieser Tätigkeiten nicht anwendbar. Für diese Fälle finden gemäß § 2 Absatz 9 des Berliner Datenschutzgesetzes die Verordnung (EU) 2016/679 und die Teile 1 und 2 des Berliner Datenschutzgesetzes entsprechende Anwendung, soweit nicht Abweichendes geregelt ist.

Zu Absatz 1
Absatz 1 regelt die Verarbeitungsbefugnis der für die Auszeichnung oder Ehrung zuständigen Stelle im Hinblick auf die zur Vorbereitung und Durchführung der Entscheidung erforderlichen Daten und bestimmt zum Schutz der Rechte der betroffenen Personen eine strenge Zweckbindung. Mit Satz 1 wird die Rechtsgrundlage für die Verarbeitung der Daten zu den genannten Zwecken geschaffen. Zur Vorbereitung der Entscheidung sind alle Daten erforderlich, die zur Beurteilung einer in sachlicher und persönlicher Hinsicht bestehenden (Auszeichnungs- oder Ehr-) Würdigkeit der betroffenen Person benötigt werden. Grundsätzlich zulässig ist auch die Verarbeitung besonderer Kategorien personenbezogener Daten entsprechend Artikel 9 Absatz 1 der Verordnung (EU) 2016/679, soweit spezialgesetzliches Recht dem nicht entgegensteht. Die Regelung wurde um den Begriff „Ehrungen“ erweitert, um klarzustellen, dass zum Beispiel auch solche Fälle erfasst werden, in denen ausgewählte Bürgerinnen und Bürger zu staatlichen Empfängen o.ä. geladen werden.
Die Datenverarbeitung unterliegt nach Satz 2 dem Zweckbindungsgrundsatz für die in dieser Regelung genannten Zwecke der öffentlichen Auszeichnungen und Ehrungen, es sei denn, die

betroffene Person willigt – nach der Maßnahme – in die Weiterverarbeitung ein. Damit wird klargestellt, dass eine zweckändernde Weiterverarbeitung nur aufgrund einer Einwilligung entsprechend Artikel 6 Absatz 4 Alternative 1 der Verordnung (EU) 2016/679 erfolgen darf.

Zu Absatz 2
Absatz 2 regelt, dass öffentliche Stellen auf Anforderung der in Absatz 1 genannten Stellen die erforderlichen Daten übermitteln dürfen. Dabei dürfte es sich regelmäßig um eine Zweckänderung handeln. Diese Norm regelt insoweit eine Zweckänderung im Sinne von Artikel 6 Absatz 4 i. V. m. Artikel 23 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679. Die Gewährleistung, dass nur sowohl in sachlicher als auch in persönlicher Hinsicht würdige Personen durch staatliche Stellen ausgezeichnet oder geehrt werden, ist ein wichtiges öffentliches Interesse, das durch die Norm sichergestellt werden soll. Eine Information der betroffenen Person durch die übermittelnde Stelle erfolgt nicht, da die Datenübermittlung auf der Grundlage einer Rechtsvorschrift im Sinne von Artikel 14 Absatz 5 Buchstabe c der Verordnung (EU) 2016/679 erfolgt und in diesen Fällen eine Information der betroffenen Person nicht vorgesehen ist.
Die Feststellung der Ehrwürdigkeit der betroffenen Person erfordert eine möglichst umfassende Heranziehung entscheidungsrelevanter Daten, und zwar gerade solcher, die ursprünglich für andere Zwecke erhoben bzw. gespeichert worden sind.

Absatz 3
Absatz 3 durchbricht den in § 2 Absatz 9 vorgesehenen Grundsatz der entsprechenden Anwendbarkeit der Verordnung (EU) 2016/679 vor und sieht eine Ausnahme vom Auskunftsrecht entsprechend Artikel 15 der Verordnung (EU) 2016/679 vor. Erweitert wird diese Regelung um Ausnahmen von der Mitteilungspflicht entsprechend Artikel 19 der Verordnung (EU) 2016/679 und Ausnahmen von der Informationspflicht entsprechend Artikel 13 und 14 der Verordnung (EU) 2016/679, wobei der Fall des Artikel 13 der Verordnung (EU) 2016/679 in der Regel ohnehin kaum einschlägig sein dürfte, da eine Erhebung bei der betroffenen Person selten vorkommen dürfte. Verfahren zur Vergabe öffentlicher Auszeichnungen und Ehrungen sind in ihrer Gesamtheit zum Schutz öffentlicher und im Verfahren bekannt werdender persönlicher Interessen vertraulich, gerade auch gegenüber der betroffenen Person. Informations- und Mitteilungspflichten oder Auskunftsrechte würden dem Wesen öffentlicher Ehrerweisungen widersprechen. Die Ausnahmen sind mit dem wichtigen öffentlichen Interesse an einer tragfähigen Auswahlentscheidung begründet, die eine vollumfängliche – auch die persönliche Integrität der möglicherweise auszuzeichnenden oder zu ehrenden Personen umfassenden – Würdigung voraussetzt.

Zu Teil 4 Schlussvorschrift

Zu § 72 Übergangsvorschriften

Zu Absatz 1

In Absatz 1 wird von der in Artikel 63 Absatz 2 der Richtlinie (EU) 2016/680 vorgesehenen Möglichkeit Gebrauch gemacht, wonach in Ausnahmefällen, in denen dies für die vor dem 6. Mai 2016 eingerichteten automatisierten Verarbeitungssysteme mit einem unverhältnismäßigen Aufwand verbunden ist, diese bis zum 6. Mai 2023 mit § 62 Absatz 1 und 2, mit dem Artikel 25 Absatz 1 der Richtlinie (EU) 2016/680 umgesetzt wird, in Einklang gebracht werden müssen.

Zu Absatz 2
§ 71 schafft eine Übergangsregelung für die im Amt befindliche Berliner Beauftragte oder den im Amt befindlichen Berliner Beauftragten für Datenschutz und Informationsfreiheit zum Zeitpunkt des Inkrafttretens des Gesetzes. Die oder der beim Inkrafttreten dieses Gesetzes im Amt befindliche Berliner Beauftragte für Datenschutz und Informationsfreiheit wird zu diesem Zeitpunkt von Gesetzes wegen in den Status nach § 9 Absatz 1 übergeleitet.

Zu Artikel 2
Gesetz über den Verfassungsschutz in Berlin (VSG Bln)

Zu Inhaltsverzeichnis (Nummer 1)

Es handelt sich um eine Folgeänderung zur Einführung des § 32a.

Zu Erster Abschnitt

Zu § 2 Absatz 2 (Nummer 2)

Bei dieser Änderung handelt es sich um eine Folgeänderung aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes.

Zu § 8 Absatz 1 Satz 1 (Nummer 3)

§ 8 Absatz 1 Satz 1 wird um einen Halbsatz ergänzt, der die Verarbeitung personenbezogener Daten aufgrund der Einwilligung des Betroffenen regelt. Dadurch wird dem schon in § 6 Absatz 1 Nummer 3 des Berliner Datenschutzgesetzes a.F. verankerten fundamentalen Grundsatz des Datenschutzes Rechnung getragen, der nunmehr auch auf europäischer Ebene seinen Niederschlag in Artikel 6 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 gefunden hat. Die Voraussetzungen der Einwilligung sind in § 36 des Berliner Datenschutzgesetzes geregelt, der aufgrund der Verweisung in § 38 Nummer 2 entsprechende Anwendung findet (ohne § 36 Absatz 5 des Berliner Datenschutzgesetzes, der bereichsspezifisch nicht passt, weil der Umgang mit solchen Daten für die Verfassungsschutzbehörde geradezu aufgabentypisch ist).

Zu § 8 Absatz 1 Satz 2 Nummer 10 (Nummer 4)

Es handelt sich um eine Folgeänderung aufgrund der Änderung des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10). Die Verweisung wird an die aktuelle Gesetzesfassung angepasst.

Zu § 11 (Nummer 5)

Bei der Änderung in § 11 Absatz 1 handelt es sich um eine Folgeänderung aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes.

Zu § 12 (Nummer 6 a und b)

Bei diesen Änderungen handelt es sich um Folgeänderungen aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes.

Zu § 14 (Nummer 7 a bis e)

Bei der Änderungen Nummer a bis e handelt es sich um Folgeänderungen aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes.

Zu § 15 (Nummer 8 a bis)

Bei den Änderungen a bis c handelt es sich um Folgeänderungen aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes.

Zu § 16 (Nummer 9)

Die Ergänzung greift die in § 56 des Berliner Datenschutzgesetzes verankerte Regelung bereichsspezifisch im Verfassungsschutzgesetz auf und sorgt so auch für einen Gleichklang mit der Regelung auf Bundesebene.

Zu § 18 (Nummer 10)

Bei dieser Änderung handelt es sich um eine Folgeänderung aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes.

Zu § 22 (Nummer 11 a und b)

Bei diesen Änderungen handelt es sich um Folgeänderungen aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes.

Zu § 23 (Nummer 12 a bis c)

Bei diesen Änderungen handelt es sich um Folgeänderungen aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes.

Zu § 24 (Nummer 13)

Bei dieser Änderung handelt es sich um eine Folgeänderung aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes.

Zu § 25 (Nummer 14 a und b)

Bei diesen Änderungen handelt es sich um Folgeänderungen aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes.

Zu § 26 (Nummer 15)

Bei dieser Änderung handelt es sich um eine Folgeänderung aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes.

Zu § 27 (Nummer 16)

Bei dieser Änderung handelt es sich um eine Folgeänderung aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes.

Zu § 31 Absatz 4 (Nummer 17)

Bei den Änderungen handelt sich um Folgeänderungen des neuen § 32a (Nummer 18).

Zu § 32a (Nummer 18)

Der neue § 32a übernimmt inhaltlich unverändert die bisherige Regelung des § 31 Absatz 4 Satz 4 und führt diese an einem neuen Regelungsstandort mit weiteren Regelungen betreffend die Ausgestaltung der unabhängigen Datenschutzkontrolle zusammen. In Übereinstimmung mit der verabschiedeten Neuregelung im Bund wird in Absatz 2 Satz 2 redaktionell klargestellt, dass Kontrollgegenstand nicht die personenbezogenen Daten, sondern der Umgang der Verwaltung mit ihnen ist.

Zu § 38 (Nummer 19)

Die Neufassung des § 38 ist eine Folgeänderung der Neugestaltung des Regelungssystems des Berliner Datenschutzgesetzes. Danach finden die Teile 1 und 4 auch außerhalb der Geltung des Gemeinschaftsrechts Anwendung, während der Teil 2 Durchführungsbestimmungen der Verordnung (EU) 2016/679 enthält und der Teil 3 die Richtlinie (EU) 2016/680 umsetzt.
Die in § 38 vorgenommene Differenzierung passt sich dem neuen Konstrukt des Berliner Datenschutzgesetzes an, in dem es in § 38 Nummer 1, wie bisher, Anwendungsausschlüsse für den Verfassungsschutz bestimmt, soweit das VSG Bln bereichsspezifische Sonderregelungen vorsieht. Für die in § 13 Absatz 4 des Berliner Datenschutzgesetzes normierten Befugnisse trifft das VSG Bln mit § 32a eine bereichsspezifische Regelung. Dies ist unionsrechtskonform möglich, da die Verordnung (EU) 2016/679 nur im Kompetenzrahmen der Europäischen Union gilt, die gemäß Artikel 4 Absatz 2 Satz 3 EUV keine Regelungskompetenz zum Bereich des Verfassungsschutzes besitzt. § 13 Absatz 1 ist wegen seines Regelungsgehalts auf den Anwendungsbereich der Verordnung (EU) 2016/679 beschränkt und damit hier nicht anwendbar. Er wird gleichwohl zur Vermeidung von Missverständnissen aufgeführt. Abschließend wird klargestellt, dass § 2 Absatz 9 des Berliner Datenschutzgesetzes für den Verfassungsschutz keine Anwendung findet, da das VSG Bln ein bereichsspezifisches und abschließendes Datenschutzvollsystem für die Aufgabenwahrnehmung gemäß § 5 VSG bildet, das keinen Anwendungsspielraum für Teil 2 des Berliner Datenschutzgesetzes lässt. Der Anwendungsausschluss des § 2 Absatz 9 des Berliner Datenschutzgesetzes lässt die grundsätzliche

Anwendbarkeit des Teils 1 des Berliner Datenschutzgesetzes unberührt. Die nicht in § 38 Nummer 1 aufgeführten Regelungen des Teils 1 sind also anwendbar.
Teil 3 des Berliner Datenschutzgesetzes ist zwar auf den Anwendungsbereich der Verordnung (EU) 2016/679 bzw. der Richtlinie (EU) 2016/680 beschränkt, doch sind einige Vorschriften auch im Bereich des Verfassungsschutzes angemessen und finden durch den Verweis in Nummer 2 entsprechende Anwendung. Die Einbeziehung des § 31 des Berliner Datenschutzgesetzes dient der Vereinheitlichung der Datenschutzterminologie und lässt für den Rechtsanwender keinen Interpretationsspielraum zu.

Zu Artikel 3

Änderung des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen im Land Berlin (BSÜG)

Zum Inhaltsverzeichnis (Nummer 1 a bis c)

Bei Nummer 1 a handelt es sich um eine Folgeänderung aufgrund der neuen Begriffsdefinitionen nach § 31 des Berliner Datenschutzgesetzes. Nummer 1 b und c sind Folgeänderungen aufgrund der Neueinführung der §§ 33a und b.

Zu § 23 (Nummer 2)

Bei dieser Änderung handelt es sich um eine Folgeänderung aufgrund der neuen Begriffsdefinitionen nach § 31 BlnDSG.

Zu § 24 (Nummer 3 a bis c)

Nummer 3 a ist eine Folgeänderung aufgrund der sprachlichen Anpassung.
Nummer 3 b enthält eine sprachliche Anpassung an die aktuelle Bezeichnung und sorgt im Übrigen für einen Gleichklang mit der Parallelregelung des Verfassungsschutzgesetzes Berlin.
Die Änderung in Nummer 3c ist eine Folgeänderung der Anpassung des Bundesdatenschutzgesetzes.

Zu § 33a (Nummer 4)

Es handelt sich um eine Folgeregelung zur Neufassung des Berliner Datenschutzgesetzes und soll einen einheitlichen datenschutzrechtlichen Standard auch im Berliner Sicherheitsüberprüfungsgesetz gewährleisten.
Teil 1 des Berliner Datenschutzgesetzes gilt ohne Beschränkung auch im Bereich des Gemeinschaftsrechts. § 33a Nummer 1 normiert folglich Anwendungsausschlüsse, soweit das Berliner Sicherheitsüberprüfungsgesetz bereichsspezifische Sonderregelungen enthält, die somit abschließend im Sinne des § 2 Absatz 8 sind.
Teile 2 und 3 des Berliner Datenschutzgesetzes sind bereits nach dem Sinn und Zweck sowie dem Regelungsgehalt auf den Anwendungsbereich der Verordnung (EU) 2016/679 bzw. der Richtlinie (EU) 2016/680 beschränkt. Manche der dort getroffenen Regelungen sind aber

auch im Anwendungsbereich des Berliner Sicherheitsüberprüfungsgesetzes angemessen und finden gemäß der Verweisung in Nummer 2 entsprechend Anwendung.

Zu §§ 33b (Nummer 5)

Der neue § 33a dient der Harmonisierung des Datenschutzrechts auf Landesebene und soll die bisher in § 24 Absatz 5 bis 7 statuierten Rechte der Betroffenen stärken. In Übereinstimmung mit der verabschiedeten Neuregelung im Bund und im neuen § 32a des Verfassungsschutzgesetzes Berlin wird in Absatz 2 Satz 2 redaktionell klargestellt, dass Kontrollgegenstand nicht die personenbezogenen Daten, sondern der Umgang der Verwaltung mit ihnen ist.

Zu Artikel 4
Inkrafttreten, Außerkrafttreten

Die Regelungen des Gesetzes sollen zeitgleich mit der der Verordnung (EU) 2016/679 am 25. Mai 2018 in Kraft treten.

Berlin, d. 08. Mai 2018

Saleh Kohlmeier
und die übrigen Mitglieder der Fraktion
der SPD

Bluhm U. Wolf Schrader
und die übrigen Mitglieder der Fraktion
Die Linke

Kapek Gebel Ziller
und die übrigen Mitglieder der Fraktion
Bündnis 90/Die Grünen