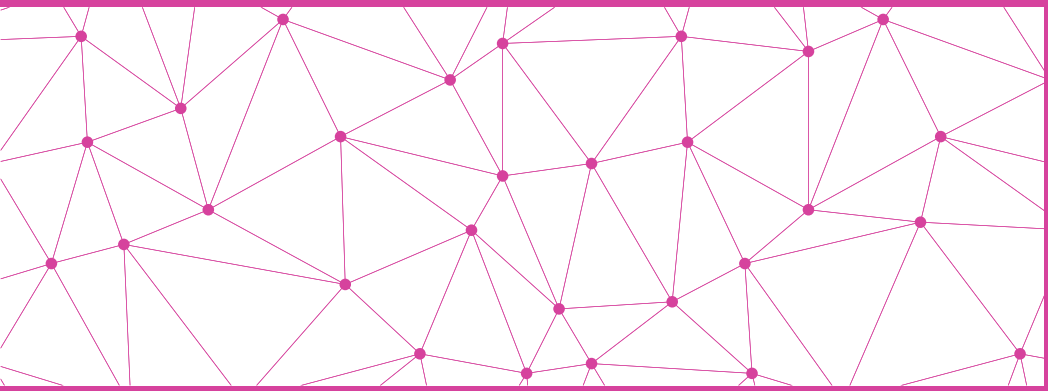
Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berliner Datenschutzgesetz



Berliner Datenschutzgesetz

Berlin 2018

Impressum

Herausgeberin: Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219, 10969 Berlin
Telefon: 030 13889-0
Telefax: 030 2155050
E-Mail: mailbox@datenschutz-berlin.de
Internet: https://www.datenschutz-berlin.de

Auflage: Neudruck September 2018
Gestaltung: april agentur GbR
Druck: ARNOLD group

Vorwort

Seit dem 25. Mai 2018 gilt mit der Datenschutz-Grundverordnung (DS-GVO) in der gesamten Europäischen Union ein einheitliches Datenschutzrecht. Der europäische Gesetzgeber hat sich bei diesem Gesetzgebungsverfahren mit großer Standhaftigkeit und gegen den vehementen Druck von Lobbyisten für die Stärkung des fundamentalen Bürgerrechts auf informationelle Selbstbestimmung stark gemacht. Das Datenschutzrecht ist modernisiert worden, um den Herausforderungen einer flächendeckenden Digitalisierung gewachsen zu sein. Um das zu gewährleisten, regelt die Verordnung umfassend und mit unmittelbarer Geltung in der gesamten Europäischen Union, wie Unternehmen und Behörden mit personenbezogenen Daten umzugehen haben. Sie gibt den Menschen stärkere Rechte und sieht Mechanismen vor, mit denen das Datenschutzrecht wirksam durchgesetzt werden kann.

Zwar gilt die DS-GVO unmittelbar und verbindlich für alle. An einigen Stellen hat der Europäische Gesetzgeber den nationalen Gesetzgebern jedoch Spielräume für Ergänzungen und Konkretisierungen gegeben, um den nationalen Rechtstraditionen gerecht zu werden. Darüber hinaus mussten die bis dato geltenden nationalen Gesetze an die neue Rechtslage angepasst werden.

Am 27. April 2017 hat der Bundesgesetzgeber ein neues Bundesdatenschutzgesetz (BDSG-neu) beschlossen, das wie die DS-GVO am 25. Mai 2018 wirksam wurde und für den privatwirtschaftlichen Bereich auch in Berlin Anwendung findet.

Für den öffentlich-rechtlichen Bereich wurde im Zuge der europäischen Datenschutzreform das Berliner Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG) ebenfalls neu gefasst und vom Berliner Gesetzgeber durch das Berliner Datenschutz-Anpassungs- und -Umsetzungsgesetz am 31. Mai 2018 beschlossen. Wirksam wurde dieses neue Berliner Datenschutzgesetz mit seiner Veröffentlichung im Gesetz- und Verordnungsblatt des Landes Berlin am 13. Juni 2018. Es regelt die Voraussetzungen, unter denen die öffentlichen Stellen des Landes Berlin grundsätzlich personenbezogene Daten verarbeiten dürfen.

Neben der Anpassung des allgemeinen Berliner Datenschutzrechts an die DS-GVO wurde mit diesem Gesetz auch die EU-Datenschutzrichtlinie für Polizei- und Justiz (die sog. JI-Richtlinie EU 2016/680) in nationales Recht umgesetzt und somit die Verarbeitung personenbezogener Daten durch Polizei- und Justizbehörden

neu geregelt (Teil 1 und 3 des Gesetzes). Wie bisher wird das BlnDSG allerdings auch weiterhin durch diverse bereichsspezifische Regelungen in verschiedenen Spezialgesetzen ergänzt.

Damit stehen nunmehr die öffentlichen Stellen des Landes Berlin – einschließlich der Berliner Beauftragten für Datenschutz und Informationsfreiheit – vor der Herausforderung, die neuen Regelungen in der Praxis anzuwenden. Dabei wird sich zeigen, ob und inwieweit sich die unter großem Zeitdruck erarbeiteten Vorschriften bewähren und an welchen Stellen Nachbesserungen notwendig sind. Der Gesetzgeber sicherte im Gesetzgebungsverfahren seine Bereitschaft zu, die neuen Regeln noch in der laufenden Wahlperiode zu evaluieren und bei Bedarf noch einmal anzupassen.

Bei der Neugestaltung des europäischen Datenschutzrechts handelt es sich um ein historisches Mammutprojekt, dessen Ausgestaltung in der Praxis nur bedingt im Vorhinein überblickt werden konnte. Insofern wird es jetzt auf die praktischen Erfahrungen ankommen, um die Tauglichkeit der neuen gesetzlichen Regeln in der täglichen Anwendung zu prüfen. Meine Behörde stellt sich dieser Herausforderung mit großer Einsatzfreude und mit dem Willen, das Beste für die Bürgerinnen und Bürger aus der neuen Rechtslage zu machen.

Weitere Informationen zur Datenschutzreform sowie zu Ihren Rechten und Pflichten nach dem BlnDSG finden Sie auf unserer Webseite unter www.datenschutz-berlin.de

Maja Smoltczyk

Berliner Beauftragte für Datenschutz und Informationsfreiheit

Inhalt

Berliner Datenschutzgesetz

Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG) Vom 13. Juni 2018*

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 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 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).

* Verkündet als Artikel 1 des Gesetzes 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 13. Juni 2018 (GVBl. S. 418)

(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 auf Grund 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 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 Vorschriften 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 nicht-öffentlicher Stellen und öffentlicher Stellen, soweit diese am Wettbewerb teilnehmen.

(3) Die oder der Berliner 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 Artikel 21 des Gesetzes vom 2. Februar 2018 (GVBl. S. 160) 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 Mitteilun-

gen 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 auf Grund 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, auf Grund 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 Zuständigkeitsbeziehungsweise 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 diesen zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden 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 auf Grund 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 Verordnung (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. damit der Verantwortliche oder die betroffene Person die ihm oder ihr aus dem Dienst- und Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen oder ihren diesbezüglichen Pflichten nachkommen kann,
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 Umstände 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 für dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Personen zu personenbezogenen Daten 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 auf Grund 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 Absatzes 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 auf Grund 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 Zwecke 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 auf Grund 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 Ar-

tikel 5 Absatz 1 Buchstabe f sowie Artikel 24 und 32. 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 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 abzustimmendes 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 auf Grund 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 auf Grund 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 in zumutbarer Weise 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.

(4) Der Rechnungshof ist zur Erteilung von Informationen nach Artikel 14 der Verordnung (EU) 2016/679 nicht verpflichtet, soweit er im Rahmen seiner unabhängigen Tätigkeit personenbezogene Daten verarbeitet.

§ 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 Landesfinanzbehörden, 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 Ver-

teidigung 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 5 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.

(8) Der Rechnungshof ist zur Erteilung von Auskünften nach Artikel 15 der Verordnung (EU) 2016/679 nicht verpflichtet, soweit er im Rahmen seiner unabhängigen Tätigkeit personenbezogene Daten verarbeitet.

§ 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 automatisiert erfolgt, 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.

(4) Die Regelungen der Verordnung (EU) 2016/679 werden durch die Absätze 1 bis 3 nicht eingeschränkt.

§ 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 erwor-

benen 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.

(3) Der Verantwortliche ist für die Einhaltung der Absätze 1 und 2 verantwortlich und muss deren Einhaltung nachweisen können. Dies gilt entsprechend für die Regelungen in § 34 und § 35 Absatz 1 bis 3.

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 zu-

geordnet 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 auf Grund 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 darü-

ber 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, bei Übermittlungen an Empfänger in Drittländern oder internationale Organisationen auch Angaben dazu,
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 auf Grund 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 Berich-

tigung 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 Satz 1 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, auf Grund 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 auf Grund 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 sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben, 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 §§ 50 bis 53 und 55 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 Nummer 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 zu-

mindest 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 auf Grund 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, auf Grund 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 personenbezogenen 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 angemessenem 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 personenbe-

zogene 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 den 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 auf Grund 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 nicht-automatisierten 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 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.

www.datenschutz-berlin.de

be Berlin