Deutscher Bundestag **Drucksache 18/11325**

18. Wahlperiode 24.02.2017

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

A. Problem und Ziel

Am 25. Mai 2018 wird die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union sein. Ziel der Verordnung (EU) 2016/679 ist ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten in allen Mitgliedstaaten (Erwägungsgrund 10). Der Unionsgesetzgeber hat sich für die Handlungsform einer Verordnung entschieden, damit innerhalb der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist (Erwägungsgrund 13). Die Verordnung (EU) 2016/679 sieht eine Reihe von Öffnungsklauseln für den nationalen Gesetzgeber vor. Zugleich enthält die Verordnung (EU) 2016/679 konkrete, an die Mitgliedstaaten gerichtete Regelungsaufträge. Daraus ergibt sich gesetzlicher Anpassungsbedarf im nationalen Datenschutzrecht.

Darüber hinaus dient der vorliegende Gesetzentwurf der Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89), soweit die der Richtlinie unterfallenden Staaten nach deren Artikel 63 verpflichtet sind, bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften zu erlassen, die erforderlich sind, um dieser Richtlinie nachzukommen. Die Umsetzung der Richtlinie (EU) 2016/680 wird über die im vorliegenden Gesetzentwurf enthaltenen relevanten Regelungen hinaus auch noch gesondert im Fachrecht erfolgen.

Um ein reibungsloses Zusammenspiel der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 mit dem stark ausdifferenzierten deutschen Datenschutzrecht sicherzustellen, ist es erforderlich, das bisherige Bundesdatenschutzgesetz (BDSG) durch ein neues Bundesdatenschutzgesetz abzulösen. Weiterer ge-

setzlicher Anpassungsbedarf ergibt sich hinsichtlich der bestehenden bereichsspezifischen Datenschutzregelungen des Bundes infolge der Änderungen im allgemeinen Datenschutzrecht durch die Verordnung (EU) 2016/679 und das sie ergänzende neu gefasste BDSG.

Im Interesse einer homogenen Entwicklung des allgemeinen Datenschutzrechts soll das neu gefasste Bundesdatenschutzgesetz, soweit nicht dieses selbst oder bereichsspezifische Gesetze abweichende Regelungen treffen, auch für die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten öffentlicher Stellen des Bundes Anwendung finden, die außerhalb des Anwendungsbereichs des Unionsrechts liegen, wie etwa die Datenverarbeitung durch das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst oder im Bereich des Sicherheitsüberprüfungsgesetzes. Dies geht einher mit zusätzlichem gesetzlichen Änderungsbedarf in den jeweiligen bereichsspezifischen Gesetzen.

B. Lösung

Der Gesetzentwurf sieht folgende Gesetzesänderungen vor:

1. Neufassung des BDSG (Artikel 1), das für öffentliche Stellen des Bundes und der Länder (soweit nicht landesrechtliche Regelungen greifen) sowie für nichtöffentliche Stellen gilt, bestehend aus vier Teilen:

   a. Gemeinsame Bestimmungen mit folgenden Regelungsschwerpunkten:

      - Schaffung allgemeiner Rechtsgrundlagen für die Datenverarbeitung durch öffentliche Stellen und für die Videoüberwachung (§§ 3, 4 BDSG);
      - Regelungen zu Datenschutzbeauftragten öffentlicher Stellen (§§ 5 bis 7 BDSG);
      - Ausgestaltung des Amtes, der Aufgaben und Befugnisse der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit der unabhängigen Datenschutzaufsichtsbehörden (§§ 8 bis 16 BDSG);
      - Festlegung der deutschen Vertretung im Europäischen Datenschutzausschuss; gemeinsamer Vertreter im Ausschuss ist die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit; als Stellvertreterin oder Stellvertreter wählt der Bundesrat die Leiterin oder den Leiter einer Aufsichtsbehörde eines Landes (§§ 17 bis 19 BDSG);
      - Rechtsbehelfe (§§ 20, 21 BDSG).

   Die gemeinsamen Bestimmungen finden keine Anwendung, soweit das Recht der Europäischen Union unmittelbar gilt, insbesondere die Verordnung (EU) 2016/679. Sie finden Anwendung im Anwendungsbereich der Richtlinie (EU) 2016/680 sowie für die Bereiche, die außerhalb des Unionsrechts liegen.

   b. Bestimmungen zur Ausgestaltung der Verordnung (EU) 2016/679 mit folgenden Regelungsschwerpunkten:

      - Schaffung einer Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten (§ 22 BDSG);

- Festlegung der Zulässigkeitsvoraussetzungen für Verarbeitungen zu anderen Zwecken durch öffentliche Stellen (§ 23 BDSG) und durch nichtöffentliche Stellen (§ 24 BDSG) sowie für Datenübermittlungen durch öffentliche Stellen (§ 25 BDSG);
- Regelung weiterer besonderer Verarbeitungssituationen (§§ 26 bis 31 BDSG);
- Regelungen zu den Betroffenenrechten (§§ 32 bis 37 BDSG);
- Verhängung von Geldbußen bei Verstößen gegen die Verordnung (EU) 2016/679 (§§ 41, 43 BDSG).

c. Bestimmungen zur Umsetzung der Richtlinie EU 2016/680 mit folgenden Regelungsschwerpunkten:

- Aussagen zu Rechtsgrundlagen der Verarbeitung, Zweckbindung und -änderung (§§ 47 bis 51 BDSG);
- Ausformung der Betroffenenrechte (§§ 55 bis 61 BDSG);
- Festlegung unterschiedlich akzentuierter Pflichten der Verantwortlichen
  - Anforderungen an Auftragsverarbeitungsverhältnisse (§ 62 BDSG);
  - Datensicherheit und Meldungen von Verletzungen des Schutzes personenbezogener Daten (§§ 64 bis 66 BDSG);
  - Instrumente zur Berücksichtigung des Datenschutzes (Datenschutz-Folgenabschätzung, Anhörung der oder des Bundesbeauftragten, Verzeichnis von Verarbeitungstätigkeiten, Protokollierung, §§ 67 bis 70 und 76 BDSG);
  - Berichtigungs- und Löschungspflichten (§ 75 BDSG);
- Datenübermittlungen an Stellen in Drittstaaten und an internationale Organisationen (§§ 78 bis 81 BDSG).

d. Besondere Bestimmungen für Datenverarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten.

2. Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes und des Sicherheitsüberprüfungsgesetzes (Artikel 2 bis 6) infolge der Ablösung des bisherigen Bundesdatenschutzgesetzes, die den Erfordernissen der außerhalb des Anwendungsbereichs des Unionsrechts fallenden Datenverarbeitungen im Bereich der nationalen Sicherheit Rechnung tragen.

3. Änderung des geltenden Bundesdatenschutzgesetzes (Artikel 7), die sicherstellt, dass das in § 21 BDSG geschaffene Antragsrecht gegen Beschlüsse der Europäischen Kommission bereits vor Geltung der Verordnung (EU) 2016/679 zur Verfügung steht.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

Die gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG L 281 vom 23.11.1995, S. 31) bereits bestehenden Betroffenenrechte, wie etwa Informations- und Auskunftsrechte gegenüber der betroffenen Person, das Recht auf Berichtigung und Löschung, das Recht auf Einschränkung der Verarbeitung sowie das Widerspruchsrecht, werden durch die Verordnung (EU) 2016/679 gestärkt. Dadurch entsteht zusätzlicher Erfüllungsaufwand für die Bürgerinnen und Bürger, die Wirtschaft und die Verwaltung, der aber durch die Verordnung (EU) 2016/679 und nicht durch dieses Gesetz verursacht wird.

Das neu gefasste BDSG schränkt zugleich in dem durch Artikel 23 der Verordnung (EU) 2016/679 eröffneten Rahmen einzelne Betroffenenrechte ein. Dies führt bei den Unternehmen zu einer Reduzierung von Pflichten und einer Verringerung des Erfüllungsaufwandes. Die im BDSG zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen als Ausgleich für die Einschränkung der Betroffenenrechte von dem Verantwortlichen zu ergreifenden Schutzmaßnahmen, wie etwa das Nachholen einer Informationspflicht oder die Dokumentation, aus welchen Gründen von einer Information abgesehen wird, löst unmittelbaren Erfüllungsaufwand aus. Ohne diese beiden zusammenhängenden Maßnahmen wäre der durch die Verordnung (EU) 2016/679 ausgelöste Aufwand für die Wirtschaft deutlich höher.

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein neuer Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Das Gesetz verpflichtet die Wirtschaft, im Rahmen der Verarbeitung personenbezogener Daten Maßnahmen zum Schutz der betroffenen Person in den Fällen zu ergreifen, in denen sie davon absehen will, die betroffene Person nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679 zu informieren. Dazu gehört etwa das Nachholen der Informationspflicht durch Bereitstellen der Information auf einer allgemein zugänglichen Webseite. Darüber hinaus hat der Verantwortliche zu dokumentieren, aus welchen Gründen von einer Information abgesehen werden soll.

Durch diese als Gegenmaßnahme für die Einschränkung der korrespondierenden Betroffenenrechte eingeführten neuen Pflichten entstehen für die Wirtschaft jährliche Bürokratiekosten aus Informationspflichten in Höhe von rund 17,2 Millionen Euro. Darüber hinaus fällt einmaliger Erfüllungsaufwand in Höhe von rund 58,9 Millionen Euro an.

Die Belastungen sind nicht im Rahmen der „One in, one out“-Regel der Bundesregierung zu kompensieren, da diese Änderungen aus einer 1:1-Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 resultieren.

E.3 Erfüllungsaufwand der Verwaltung

Für die Verwaltung des Bundes entstehen im Bereich der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach derzeitiger Schätzung insgesamt jährlicher Erfüllungsaufwand in Höhe von rund 940.000 Euro sowie einmalige Umsetzungskosten in Höhe von rund 74.000 Euro. Diese Kosten resultieren im Wesentlichen aus der Wahrnehmung der Funktion des gemeinsamen Vertreters im Europäischen Datenschutzausschuss durch die oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie durch die bei der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit angesiedelte Einrichtung der zentralen Anlaufstelle. Dies konnte im Haushalt 2017 nicht berücksichtigt werden, weil der Gesetzentwurf bei Verabschiedung des Haushalts noch nicht etatreif war.

Weiterer neuer Erfüllungsaufwand für die Verwaltung entsteht durch Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 nicht. Die bestehenden allgemeinen wie bereichsspezifischen Regelungen im Datenschutzrecht, die öffentliche Stellen betreffen, können durch Ausnutzung der in der Verordnung (EU) 2016/679 enthaltenen Öffnungsklauseln fortbestehen.

Die im neu gefassten Bundesdatenschutzgesetz zur Umsetzung der Richtlinie (EU) 2016/680 geschaffenen Regelungen schaffen in Teilen gegenüber dem bestehenden Recht und der bestehenden Verwaltungspraxis neue Pflichten für die Verwaltung. Hiervon betroffen sind im Bereich des Bundes das Zollkriminalamt, die Zollverwaltung, die Bundespolizei, das Bundeskriminalamt, der Generalbundesanwalt und die Bundesgerichte. Diesen Pflichten stehen nach derzeitiger Schätzung ein jährlicher Erfüllungsaufwand in Höhe von rund 562.000 Euro sowie einmalige Umsetzungskosten in Höhe von rund 60.000 Euro gegenüber. Die Kosten entstehen im Wesentlichen im Zusammenhang mit Anforderungen an die Durchführung von Datenschutz-Folgenabschätzungen sowie durch Softwareanpassungen zur Protokollierung von Datenverarbeitungen.

Etwaiger Mehrbedarf an Sach- und Personalmitteln soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

Für die Länder entsteht jährlicher Erfüllungsaufwand durch die Tätigkeit als Stellvertreter des gemeinsamen Vertreters im Europäischen Datenschutzausschuss und die Teilnahme am Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Höhe von insgesamt rund 1,98 Millionen Euro.

F. Weitere Kosten

Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

BUNDESREPUBLIK DEUTSCHLAND
DIE BUNDESKANZLERIN

Berlin, 24. Februar 2017

An den
Präsidenten des
Deutschen Bundestages
Herrn Prof. Dr. Norbert Lammert
Platz der Republik 1
11011 Berlin

Sehr geehrter Herr Präsident,

hiermit übersende ich den von der Bundesregierung beschlossenen

> Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium des Innern.

Die Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Absatz 1 NKRG ist als Anlage 2 beigefügt.

Der Gesetzentwurf ist dem Bundesrat am 2. Februar 2017 als besonders eilbedürftig zugeleitet worden.

Die Stellungnahme des Bundesrates zu dem Gesetzentwurf sowie die Auffassung der Bundesregierung zu der Stellungnahme des Bundesrates werden unverzüglich nachgereicht.

Mit freundlichen Grüßen

Dr. Angela Merkel

Anlage 1

Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680

(Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

Vom ….

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

Artikel 1

Bundesdatenschutzgesetz

(BDSG)

Inhaltsübersicht

Kapitel 4

Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Kapitel 5

Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle, Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union

Kapitel 6

Rechtsbehelfe

Teil 2

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

Kapitel 1

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Abschnitt 1

Verarbeitung besonderer Kategorien personenbezogener Daten und Verarbeitung zu anderen Zwecken

Kapitel 4

Pflichten der Verantwortlichen und Auftragsverarbeiter

Kapitel 5

Datenübermittlungen an Drittstaaten und an internationale Organisationen

Kapitel 6

Zusammenarbeit der Aufsichtsbehörden

Kapitel 7

Haftung und Sanktionen

Teil 4

Besondere Bestimmungen für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten

Teil 1

Gemeinsame Bestimmungen

Kapitel 1

Anwendungsbereich und Begriffsbestimmungen

§ 1

Anwendungsbereich des Gesetzes

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
   a) Bundesrecht ausführen oder
   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

Für nichtöffentliche Stellen gilt dieses Gesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

(2) Andere Rechtsvorschriften des Bundes über den Datenschutz gehen den Vorschriften dieses Gesetzes vor. Regeln sie einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften dieses Gesetzes Anwendung. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(3) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(4) Dieses Gesetz findet Anwendung auf öffentliche Stellen. Auf nichtöffentliche Stellen findet es Anwendung, sofern

1. der Verantwortliche oder Auftragsverarbeiter personenbezogene Daten im Inland verarbeitet,
2. die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer inländischen Niederlassung des Verantwortlichen oder Auftragsverarbeiters erfolgt oder
3. der Verantwortliche oder Auftragsverarbeiter zwar keine Niederlassung in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum hat, er aber in den Anwendungsbereich 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) fällt.

Sofern dieses Gesetz nicht gemäß Satz 2 Anwendung findet, gelten für den Verantwortlichen oder Auftragsverarbeiter nur die §§ 8 bis 21, 39 bis 44.

(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) 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 Mitgliedstaaten der Europäischen Union gleich. Andere Staaten gelten insoweit als Drittstaaten.

(7) Bei Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89) 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.

(8) Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten finden die Verordnung (EU) 2016/679 und die Teile 1 und 2 dieses Gesetzes entsprechend Anwendung, soweit nicht in diesem Gesetz oder einem anderen Gesetz Abweichendes geregelt ist.

§ 2

Begriffsbestimmungen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, der Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes oder sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nichtöffentlicher Stellen als öffentliche Stellen des Bundes, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nichtöffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nichtöffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

(5) Öffentliche Stellen des Bundes gelten als nichtöffentliche Stellen im Sinne dieses Gesetzes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Als nichtöffentliche Stellen im Sinne dieses Gesetzes gelten auch öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

Kapitel 2

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 3

Verarbeitung personenbezogener Daten durch öffentliche Stellen

Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle 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.

§ 4

Videoüberwachung öffentlich zugänglicher Räume

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bei der Videoüberwachung von

1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder
2. Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs

gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.

(2) Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

(3) Die Speicherung oder Verwendung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Absatz 1 Satz 2 gilt entsprechend. Für einen anderen Zweck dürfen sie nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, so besteht die Pflicht zur Information der betroffenen Person über die Verarbeitung gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679. § 32 gilt entsprechend.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Kapitel 3
Datenschutzbeauftragte öffentlicher Stellen

§ 5
Benennung

(1) Öffentliche Stellen benennen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten. Dies gilt auch für öffentliche Stellen nach § 2 Absatz 5, 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) Die oder der Datenschutzbeauftragte wird auf der Grundlage ihrer oder seiner beruflichen Qualifikation und insbesondere ihres oder seines 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 § 7 genannten Aufgaben.

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

(5) Die öffentliche Stelle veröffentlicht die Kontaktdaten der oder des Datenschutzbeauftragten und teilt diese Daten der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit.

§ 6
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 § 7, 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 Person sowie über Umstände, die Rückschlüsse auf die betroffene Personen zulassen, verpflichtet, soweit sie oder er nicht davon durch die betroffene Person 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 Schriftstücke einem Beschlagnahmeverbot.

§ 7

Aufgaben

(1) Der oder dem Datenschutzbeauftragten obliegen neben den in der Verordnung (EU) 2016/679 genannten Aufgaben 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 § 67 dieses Gesetzes;
4. Zusammenarbeit mit der Aufsichtsbehörde;
5. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß § 69 dieses Gesetzes, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Im Fall einer oder eines bei einem Gericht bestellten Datenschutzbeauftragten beziehen sich diese Aufgaben nicht auf das Handeln des Gerichts im Rahmen seiner justiziellen Tätigkeit.

(2) 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.

(3) 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

Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

§ 8

Errichtung

(1) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Bundesbeauftragte) ist eine oberste Bundesbehörde. Der Dienstsitz ist Bonn.

(2) Die Beamtinnen und Beamten der oder des Bundesbeauftragten sind Beamtinnen und Beamte des Bundes.

(3) Die oder der Bundesbeauftragte kann Aufgaben der Personalverwaltung und Personalwirtschaft auf andere Stellen des Bundes übertragen, soweit hierdurch die Unabhängigkeit der oder des Bundesbeauftragten nicht beeinträchtigt wird. Diesen Stellen dürfen personenbezogene Daten der Beschäftigten übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

§ 9

Zuständigkeit

(1) Die oder der Bundesbeauftragte ist zuständig für die Aufsicht über die öffentlichen Stellen des Bundes, auch soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Die Vorschriften dieses Kapitels gelten auch für Auftragsverarbeiter, soweit sie nichtöffentliche Stellen sind, bei denen dem Bund die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle des Bundes ist.

(2) Die oder der Bundesbeauftragte ist nicht zuständig für die Aufsicht über die von den Bundesgerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

§ 10

Unabhängigkeit

(1) Die oder der Bundesbeauftragte 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.

(2) Die oder der Bundesbeauftragte unterliegt der Rechnungsprüfung durch den Bundesrechnungshof, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

§ 11

Ernennung und Amtszeit

(1) Der Deutsche Bundestag wählt ohne Aussprache auf Vorschlag der Bundesregierung die Bundesbeauftragte oder den Bundesbeauftragten mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Die oder der Gewählte ist von der Bundespräsidentin oder dem Bundespräsidenten zu ernennen. Die oder der Bundesbeauftragte muss bei ihrer oder seiner Wahl das 35. Lebensjahr vollendet haben. Sie oder er muss über die für die Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Insbesondere muss die oder der Bundesbeauftragte über durch einschlägige Berufserfahrung erworbene Kenntnisse des Datenschutzrechts verfügen und die Befähigung zum Richteramt oder höheren Verwaltungsdienst haben.

(2) Die oder der Bundesbeauftragte leistet vor der Bundespräsidentin oder dem Bundespräsidenten folgenden Eid: „Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe.“ Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit der oder des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.

§ 12

Amtsverhältnis

(1) Die oder der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis.

(2) Das Amtsverhältnis beginnt mit der Aushändigung der Ernennungsurkunde. Es endet mit dem Ablauf der Amtszeit oder mit dem Rücktritt. Die Bundespräsidentin oder der Bundespräsident enthebt auf Vorschlag der Präsidentin oder des Präsidenten des Bundestages die Bundesbeauftragte ihres oder den Bundesbeauftragten seines Amtes, wenn die oder der Bundesbeauftragte eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt. Im Fall der Beendigung des Amtsverhältnisses oder der Amtsenthebung erhält die oder der Bundesbeauftragte eine von der Bundespräsidentin oder dem Bundespräsidenten vollzogene Urkunde. Eine Amtsenthebung wird mit der Aushändigung der Urkunde wirksam. Endet das Amtsverhältnis mit Ablauf der Amtszeit, ist die oder der Bundesbeauftragte verpflichtet, auf Ersuchen der Präsidentin oder des Präsidenten des Bundestages die Geschäfte bis zur Ernennung einer Nachfolgerin oder eines Nachfolgers für die Dauer von höchstens sechs Monaten weiterzuführen.

(3) Die Leitende Beamtin oder der Leitende Beamte nimmt die Rechte der oder des Bundesbeauftragten wahr, wenn die oder der Bundesbeauftragte an der Ausübung ihres oder seines Amtes verhindert ist oder wenn ihr oder sein Amtsverhältnis endet und sie oder er nicht zur Weiterführung der Geschäfte verpflichtet ist. § 10 Absatz 1 ist entsprechend anzuwenden.

(4) Die oder der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Kalendermonats, in dem das Amtsverhältnis endet, im Fall des Absatzes 2 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der Besoldungsgruppe B 11 sowie den Familienzuschlag entsprechend Anlage V des Bundesbesoldungsgesetzes. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im Übrigen sind § 12 Absatz 6 sowie die §§ 13 bis 20 und 21a Absatz 5 des Bundesministergesetzes mit den Maßgaben anzuwenden, dass an die Stelle der vierjährigen Amtszeit in § 15 Absatz 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 und 21a Absatz 5 des Bundesministergesetzes berechnet sich das Ruhegehalt der oder des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und die oder der Bundesbeauftragte sich unmittelbar vor ihrer oder seiner Wahl zur oder zum Bundesbeauftragten als Beamtin oder Beamter oder als Richterin oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 11 zu durchlaufenden Amt befunden hat.

§ 13

Rechte und Pflichten

(1) Die oder der Bundesbeauftragte sieht von allen mit den Aufgaben ihres oder seines Amtes nicht zu vereinbarenden Handlungen ab und übt während ihrer oder seiner Amtszeit keine andere mit ihrem oder seinem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus. Insbesondere darf die oder der Bundesbeauftragte neben ihrem oder seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder 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.

(2) Die oder der Bundesbeauftragte hat der Präsidentin oder dem Präsidenten des Bundestages Mitteilung über Geschenke zu machen, die sie oder er in Bezug auf das Amt erhält. Die Präsidentin oder der Präsident des Bundestages entscheidet über die Verwendung der Geschenke. Sie oder er kann Verfahrensvorschriften erlassen.

(3) Die oder der Bundesbeauftragte ist berechtigt, über Personen, die ihr oder ihm in ihrer oder seiner Eigenschaft als Bundesbeauftragte oder Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen

selbst das Zeugnis zu verweigern. Dies gilt auch für die Mitarbeiterinnen und Mitarbeiter der oder des Bundesbeauftragten mit der Maßgabe, dass über die Ausübung dieses Rechts die oder der Bundesbeauftragte entscheidet. Soweit das Zeugnisverweigerungsrecht der oder des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihr oder ihm nicht gefordert werden.

(4) Die oder der Bundesbeauftragte ist, auch nach Beendigung ihres oder seines Amtsverhältnisses, verpflichtet, über die ihr oder ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Die oder der Bundesbeauftragte 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 Bundesbeauftragten erforderlich. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei einer Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten. Für die Bundesbeauftragte oder den Bundesbeauftragten und ihre oder seine Mitarbeiterinnen und Mitarbeiter gelten die §§ 93, 97 und 105 Absatz 1, § 111 Absatz 5 in Verbindung mit § 105 Absatz 1 sowie § 116 Absatz 1 der Abgabenordnung nicht. Satz 5 findet keine Anwendung, soweit die Finanzbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um vorsätzlich falsche Angaben der oder des Auskunftspflichtigen oder der für sie oder ihn tätigen Personen handelt. Stellt die oder der Bundesbeauftragte einen Datenschutzverstoß fest, ist sie oder er befugt, diesen anzuzeigen und die betroffene Person hierüber zu informieren.

(5) Die oder der Bundesbeauftragte darf als Zeugin oder Zeuge aussagen, es sei denn, die Aussage würde

1. dem Wohl des Bundes oder eines Landes Nachteile bereiten, insbesondere Nachteile für die Sicherheit der Bundesrepublik Deutschland oder ihre Beziehungen zu anderen Staaten, oder
2. Grundrechte verletzen.

Betrifft die Aussage laufende oder abgeschlossene Vorgänge, die dem Kernbereich exekutiver Eigenverantwortung der Bundesregierung zuzurechnen sind oder sein könnten, darf die oder der Bundesbeauftragte nur im Benehmen mit der Bundesregierung aussagen. § 28 des Bundesverfassungsgerichtsgesetzes bleibt unberührt.

(6) Die Absätze 3 und 4 Satz 5 bis 7 gelten entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 14

Aufgaben

(1) Die oder der Bundesbeauftragte hat neben den 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. den Deutschen Bundestag und den Bundesrat, die Bundesregierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten,
4. die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich den zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, entstehenden Pflichten zu sensibilisieren,
5. auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU)

2016/680 erlassenen Rechtsvorschriften, zur Verfügung zu stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten 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 Beschwerdeführer 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 § 69 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 Bundesbeauftragte zudem die Aufgabe nach § 60 wahr.

(2) Zur Erfüllung der in Absatz 1 Satz 1 Nummer 3 genannten Aufgabe kann die oder der Bundesbeauftragte zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an den Deutschen Bundestag oder einen seiner Ausschüsse, den Bundesrat, die Bundesregierung, sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit richten. Auf Ersuchen des Deutschen Bundestages, eines seiner Ausschüsse oder der Bundesregierung geht die oder der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach.

(3) Die oder der Bundesbeauftragte 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 Bundesbeauftragten ist für die betroffene Person unentgeltlich. Bei offenkundig unbegründeten oder, insbesondere im Fall von häufiger Wiederholung, exzessiven Anfragen kann die oder der Bundesbeauftragte eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In diesem Fall trägt die oder der Bundesbeauftragte die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

§ 15

Tätigkeitsbericht

Die oder der Bundesbeauftragte 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 Bundesbeauftragte übermittelt den Bericht dem Deutschen Bundestag, dem Bundesrat und der Bundesregierung und macht ihn der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich.

§ 16

Befugnisse

(1) Die oder der Bundesbeauftragte nimmt im Anwendungsbereich der Verordnung (EU) 2016/679 die Befugnisse gemäß Artikel 58 der Verordnung (EU) 2016/679 wahr. Kommt die oder der Bundesbeauftragte zu dem Ergebnis, dass Verstöße gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, teilt sie oder er dies der zuständigen Rechts- oder Fachaufsichtsbehörde mit und gibt dieser vor der Ausübung der Befugnisse des Artikels 58 Absatz 2 Buchstabe b bis g, i und j der Verordnung (EU) 2016/679 gegenüber dem Verantwortlichen Gelegenheit zur Stellungnahme innerhalb einer angemessenen Frist. Von der Einräumung der Gelegenheit zur Stellungnahme kann abgesehen werden, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der oder des Bundesbeauftragten getroffen worden sind.

(2) Stellt die oder der Bundesbeauftragte bei Datenverarbeitungen durch öffentliche Stellen des Bundes 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 der zuständigen obersten Bundesbehörde und fordert diese zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden Frist auf. Die oder der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Bundesbeauftragten getroffen worden sind. Die oder der Bundesbeauftragte 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) Die Befugnisse der oder des Bundesbeauftragten erstrecken sich auch auf

1. von öffentlichen Stellen des Bundes erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs und
2. personenbezogene Daten, die einem besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen.

Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, der oder dem Bundesbeauftragten und ihren oder seinen Beauftragten

1. jederzeit Zugang zu den Grundstücken und Diensträumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer oder seiner Aufgaben notwendig sind, zu gewähren und
2. alle Informationen, die für die Erfüllung ihrer oder seiner Aufgaben erforderlich sind, bereitzustellen.

(5) Die oder der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 40 hin. § 40 Absatz 2 Satz 1 zweiter Halbsatz gilt entsprechend.

Kapitel 5

Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle, Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union

§ 17

Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle

(1) Gemeinsamer Vertreter im Europäischen Datenschutzausschuss und zentrale Anlaufstelle ist die oder der Bundesbeauftragte (gemeinsamer Vertreter). Als Stellvertreterin oder Stellvertreter des gemeinsamen Vertreters wählt der Bundesrat eine Leiterin oder einen Leiter der Aufsichtsbehörde eines Landes (Stellvertreter). Die Wahl erfolgt für fünf Jahre. Mit dem Ausscheiden aus dem Amt als Leiterin oder Leiter der Aufsichtsbehörde eines Landes endet zugleich die Funktion als Stellvertreter. Wiederwahl ist zulässig.

(2) Der gemeinsame Vertreter überträgt in Angelegenheiten, die die Wahrnehmung einer Aufgabe betreffen, für welche die Länder allein das Recht zur Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, dem Stellvertreter auf dessen Verlangen die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss.

§ 18

Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder

(1) Die oder der Bundesbeauftragte und die Aufsichtsbehörden der Länder (Aufsichtsbehörden des Bundes und der Länder) arbeiten in Angelegenheiten der Europäischen Union mit dem Ziel einer einheitlichen Anwendung der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 zusammen. Vor der Übermittlung eines gemeinsamen Standpunktes an die Aufsichtsbehörden der anderen Mitgliedstaaten, die Europäische Kommission oder den Europäischen Datenschutzausschuss geben sich die Aufsichtsbehörden des Bundes und der Länder frühzeitig Gelegenheit zur Stellungnahme. Zu diesem Zweck tauschen sie untereinander alle zweckdienlichen Informationen aus. Die Aufsichtsbehörden des Bundes und der Länder beteiligen die nach den Artikeln 85 und 91 der Verordnung (EU) 2016/679 eingerichteten spezifischen Aufsichtsbehörden, sofern diese von der Angelegenheit betroffen sind.

(2) Soweit die Aufsichtsbehörden des Bundes und der Länder kein Einvernehmen über den gemeinsamen Standpunkt erzielen, legen die federführende Behörde oder in Ermangelung einer solchen der gemeinsame Vertreter und sein Stellvertreter einen Vorschlag für einen gemeinsamen Standpunkt vor. Einigen sich der gemeinsame Vertreter und sein Stellvertreter nicht auf einen Vorschlag für einen gemeinsamen Standpunkt, legt in Angelegenheiten, die die Wahrnehmung von Aufgaben betreffen, für welche die Länder allein das Recht der Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, der Stellvertreter den Vorschlag für einen gemeinsamen Standpunkt fest. In den übrigen Fällen fehlenden Einvernehmens nach Satz 2 legt der gemeinsame Vertreter den Standpunkt fest. Der nach den Sätzen 1 bis 3 vorgeschlagene Standpunkt ist den Verhandlungen zu Grunde zu legen, wenn nicht die Aufsichtsbehörden von Bund und Ländern einen anderen Standpunkt mit einfacher Mehrheit beschließen. Der Bund und jedes Land haben jeweils eine Stimme. Enthaltungen werden nicht gezählt.

(3) Der gemeinsame Vertreter und dessen Stellvertreter sind an den gemeinsamen Standpunkt nach den Absätzen 1 und 2 gebunden und legen unter Beachtung dieses Standpunktes einvernehmlich die jeweilige Verhandlungsführung fest. Sollte ein Einvernehmen nicht erreicht werden, entscheidet in den in § 18 Absatz 2 Satz 2 genannten Angelegenheiten der Stellvertreter über die weitere Verhandlungsführung. In den übrigen Fällen gibt die Stimme des gemeinsamen Vertreters den Ausschlag.

§ 19

Zuständigkeiten

(1) Federführende Aufsichtsbehörde eines Landes im Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII der Verordnung (EU) 2016/679 ist die Aufsichtsbehörde des Landes, in dem der Verantwortliche oder der Auftragsverarbeiter seine Hauptniederlassung im Sinne des Artikels 4 Nummer 16 der Verordnung (EU) 2016/679 oder seine einzige Niederlassung in der Europäischen Union im Sinne des Artikels 56 Absatz 1 der Verordnung (EU) 2016/679 hat. Im Zuständigkeitsbereich der oder des Bundesbeauftragten gilt Artikel 56 Absatz 1 in Verbindung mit Artikel 4 Nummer 16 der Verordnung (EU) 2016/679 entsprechend. Besteht über die Federführung kein Einvernehmen, findet für die Festlegung der federführenden Aufsichtsbehörde das Verfahren des § 18 Absatz 2 entsprechende Anwendung.

(2) Die Aufsichtsbehörde, bei der eine betroffene Person Beschwerde eingereicht hat, gibt die Beschwerde an die federführende Aufsichtsbehörde nach Absatz 1, in Ermangelung einer solchen an die Aufsichtsbehörde eines Landes ab, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wird eine Beschwerde bei einer sachlich unzuständigen Aufsichtsbehörde eingereicht, gibt diese, sofern eine Abgabe nach Satz 1 nicht in Betracht kommt, die Beschwerde an die Aufsichtsbehörde am Wohnsitz des Beschwerdeführers ab. Die empfangende Aufsichtsbehörde gilt als die Aufsichtsbehörde nach Maßgabe des Kapitels VII der Verordnung (EU) 2016/679, bei der die Beschwerde eingereicht worden ist, und kommt den Verpflichtungen aus Artikel 60 Absatz 7 bis 9 und Artikel 65 Absatz 6 der Verordnung (EU) 2016/679 nach.

Kapitel 6

Rechtsbehelfe

§ 20

Gerichtlicher Rechtsschutz

(1) Für Streitigkeiten zwischen einer natürlichen oder einer juristischen Person und einer Aufsichtsbehörde des Bundes oder eines Landes über Rechte gemäß Artikel 78 Absatz 1 und 2 der Verordnung (EU) 2016/679 sowie § 61 ist der Verwaltungsrechtsweg gegeben. Satz 1 gilt nicht für Bußgeldverfahren.

(2) Die Verwaltungsgerichtsordnung ist nach Maßgabe der Absätze 3 bis 7 anzuwenden.

(3) Für Verfahren nach Absatz 1 Satz 1 ist das Verwaltungsgericht örtlich zuständig, in dessen Bezirk die Aufsichtsbehörde ihren Sitz hat.

(4) In Verfahren nach Absatz 1 Satz 1 ist die Aufsichtsbehörde beteiligungsfähig.

(5) Beteiligte eines Verfahrens nach Absatz 1 Satz 1 sind

1. die natürliche oder juristische Person als Klägerin oder Antragstellerin und
2. die Aufsichtsbehörde als Beklagte oder Antragsgegnerin.

§ 63 Nummer 3 und 4 der Verwaltungsgerichtsordnung bleibt unberührt.

(6) Ein Vorverfahren findet nicht statt.

(7) Die Aufsichtsbehörde darf gegenüber einer Behörde oder deren Rechtsträger nicht die sofortige Vollziehung gemäß § 80 Absatz 2 Satz 1 Nummer 4 der Verwaltungsgerichtsordnung anordnen.

§ 21

Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Rechtswidrigkeit eines Beschlusses der Europäischen Kommission

(1) Hält eine Aufsichtsbehörde einen Angemessenheitsbeschluss der Europäischen Kommission, einen Beschluss über die Anerkennung von Standardschutzklauseln oder über die Allgemeingültigkeit von genehmigten Verhaltensregeln, auf dessen Gültigkeit es für eine Entscheidung der Aufsichtsbehörde ankommt, für rechtswidrig, so hat die Aufsichtsbehörde ihr Verfahren auszusetzen und einen Antrag auf gerichtliche Entscheidung zu stellen.

(2) Für Verfahren nach Absatz 1 ist der Verwaltungsrechtsweg gegeben. Die Verwaltungsgerichtsordnung ist nach Maßgabe der Absätze 3 bis 6 anzuwenden.

(3) Über einen Antrag der Aufsichtsbehörde nach Absatz 1 entscheidet im ersten und letzten Rechtszug das Bundesverwaltungsgericht.

(4) In Verfahren nach Absatz 1 ist die Aufsichtsbehörde beteiligungsfähig. An einem Verfahren nach Absatz 1 ist die Aufsichtsbehörde als Antragstellerin beteiligt; § 63 Nummer 3 und 4 der Verwaltungsgerichtsordnung bleibt unberührt. Das Bundesverwaltungsgericht kann der Europäischen Kommission Gelegenheit zur Äußerung binnen einer zu bestimmenden Frist geben.

(5) Ist ein Verfahren zur Überprüfung der Gültigkeit eines Beschlusses der Europäischen Kommission nach Absatz 1 bei dem Gerichtshof der Europäischen Union anhängig, so kann das Bundesverwaltungsgericht anordnen, dass die Verhandlung bis zur Erledigung des Verfahrens vor dem Gerichtshof der Europäischen Union auszusetzen sei.

(6) In Verfahren nach Absatz 1 ist § 47 Absatz 5 Satz 1 und Absatz 6 der Verwaltungsgerichtsordnung entsprechend anzuwenden. Kommt das Bundesverwaltungsgericht zu der Überzeugung, dass der Beschluss der Europäischen Kommission nach Absatz 1 gültig ist, so stellt es dies in seiner Entscheidung fest. Andernfalls legt es die Frage nach der Gültigkeit des Beschlusses gemäß Artikel 267 des Vertrags über die Arbeitsweise der Europäischen Union dem Gerichtshof der Europäischen Union zur Entscheidung vor.

Teil 2

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

Kapitel 1

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Abschnitt 1

Verarbeitung besonderer Kategorien personenbezogener Daten und Verarbeitung zu anderen Zwecken

§ 22

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig

1. durch öffentliche und nichtöffentliche Stellen, wenn sie

   a) erforderlich ist, um die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte auszuüben und den diesbezüglichen Pflichten nachzukommen,

   b) zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden, oder

   c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist; ergänzend zu den in Absatz 2 genannten Maßnahmen sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten,

2. durch öffentliche Stellen, wenn sie

   a) aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist,

   b) zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,

   c) zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist oder

   d) aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist

   und soweit die Interessen des Verantwortlichen an der Datenverarbeitung in den Fällen der Nummer 2 die Interessen der betroffenen Person überwiegen.

(2) In den Fällen des Absatzes 1 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. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt,
2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. Benennung einer oder eines Datenschutzbeauftragten,
5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
6. Pseudonymisierung personenbezogener Daten,
7. Verschlüsselung personenbezogener Daten,

8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder
10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.

Die Sätze 1 und 2 finden in den Fällen des Absatzes 1 Nummer 1 Buchstabe b keine Anwendung.

§ 23

Verarbeitung zu anderen Zwecken durch öffentliche Stellen

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn

1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,
2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
3. die Daten allgemein zugänglich sind oder der Verantwortliche sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Weiterverarbeitung offensichtlich überwiegt,
4. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist,
5. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,
6. sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
7. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.

(2) 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 des Absatzes 1 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 vorliegen.

§ 24

Verarbeitung zu anderen Zwecken durch nichtöffentliche Stellen

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nichtöffentliche Stellen ist zulässig, wenn

1. sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder
2. sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist,

sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.

(2) 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 des Absatzes 1 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 vorliegen.

§ 25

Datenübermittlungen durch öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 23 zulassen würden. Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist unter den Voraussetzungen des § 23 zulässig.

(2) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an nichtöffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 23 zulassen würden,
2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat oder
3. es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist

und der Dritte sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Satz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

(3) Die Übermittlung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 ist zulässig, wenn die Voraussetzungen des Absatzes 1 oder 2 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 vorliegen.

Abschnitt 2

Besondere Verarbeitungssituationen

§ 26

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn

zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

(3) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Absatz 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. § 22 Absatz 2 gilt entsprechend.

(4) Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten.

(5) Der Verantwortliche muss geeignete Maßnahmen ergreifen, um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

(6) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

(7) Die Absätze 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(8) Beschäftigte im Sinne dieses Gesetzes sind:

1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
2. zu ihrer Berufsbildung Beschäftigte,
3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte.

§ 27

Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

(2) Die in den Artikeln 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 beinträchtigen 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.

(3) Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis dahin 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.

(4) Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 28

Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken

(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

(2) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.

(3) Das Recht auf Berichtigung der betroffenen Person gemäß Artikel 16 der Verordnung (EU) 2016/679 besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.

(4) Die in Artikel 18 Absatz 1 Buchstabe a, b und d, den Artikeln 20 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte bestehen nicht, soweit diese Rechte voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

§ 29

Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1 bis 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Die Pflicht zur Benachrichtigung gemäß Artikel 34 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 34 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahme nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Abweichend von der Ausnahme nach Satz 3 ist die betroffene Person nach Artikel 34 der Verordnung (EU) 2016/679 zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

(2) Werden Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Berufsgeheimnisträger übermittelt, so besteht die Pflicht der übermittelnden Stelle zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 nicht, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt.

(3) Gegenüber den in § 203 Absatz 1, 2a und 3 des Strafgesetzbuchs genannten Personen oder deren Auftragsverarbeitern bestehen die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht im Sinne des Satzes 1 unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.

§ 30

Verbraucherkredite

(1) Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, hat Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union genauso zu behandeln wie Auskunftsverlangen inländischer Darlehensgeber.

(2) Wer den Abschluss eines Verbraucherdarlehensvertrags oder eines Vertrags über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft einer Stelle im Sinne des Absatzes 1 ablehnt, hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten. Die Unterrichtung unterbleibt, soweit hierdurch die öffentliche Sicherheit oder Ordnung gefährdet würde. § 37 bleibt unberührt.

§ 31

Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften

(1) Die Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person (Scoring) ist nur zulässig, soweit

1. die Vorschriften des Datenschutzrechts eingehalten wurden,

2. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,
3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt wurden und
4. im Fall der Nutzung von Anschriftendaten die betroffene Person vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

(2) Die Verwendung eines von Auskunfteien ermittelten Wahrscheinlichkeitswerts über die Zahlungsfähig- und Zahlungswilligkeit einer natürlichen Person ist im Fall der Einbeziehung von Informationen über Forderungen nur zulässig, soweit die Voraussetzungen nach Absatz 1 vorliegen und nur solche Forderungen über eine geschuldete Leistung, die trotz Fälligkeit nicht erbracht worden ist, berücksichtigt werden,

1. die durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden sind oder für die ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,
2. die nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden sind,
3. die der Schuldner ausdrücklich anerkannt hat,
4. bei denen
   a) der Schuldner nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,
   b) die erste Mahnung mindestens vier Wochen zurückliegt,
   c) der Gläubiger den Schuldner zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet hat und
   d) der Schuldner die Forderung nicht bestritten hat oder
5. deren zugrunde liegendes Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und bei denen der Gläubiger den Schuldner zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet hat.

Die Zulässigkeit der Verarbeitung, einschließlich der Ermittlung von Wahrscheinlichkeitswerten, von anderen bonitätsrelevanten Daten nach allgemeinem Datenschutzrecht bleibt unberührt.

Kapitel 2

Rechte der betroffenen Person

§ 32

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 13 Absatz 4 der Verordnung (EU) 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung

1. einen unverhältnismäßigen Aufwand erfordern würde und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere wegen des Zusammenhangs, in dem die Daten erhoben wurden, als gering anzusehen ist,

2. im Fall einer öffentlichen Stelle die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Artikels 23 Absatz 1 Buchstabe a bis e der Verordnung (EU) 2016/679 gefährden würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen,
3. die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen,
4. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen oder
5. eine vertrauliche Übermittlung von Daten an öffentliche Stellen gefährden würde.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 13 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. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat. Die Sätze 1 und 2 finden in den Fällen des Absatzes 1 Nummer 4 und 5 keine Anwendung.

(3) Unterbleibt die Benachrichtigung 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 nach Fortfall des Hinderungsgrundes, spätestens jedoch innerhalb von zwei Wochen, nach.

§ 33

Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1, 2 und 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 und der in § 29 Absatz 1 Satz 1 genannten Ausnahme nicht, wenn die Erteilung der Information

1. im Fall einer öffentlichen Stelle
   a) die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Artikels 23 Absatz 1 Buchstabe a bis e der Verordnung (EU) 2016/679 gefährden würde oder
   b) die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde

und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss,

2. im Fall einer nichtöffentlichen Stelle
   a) allgemein anerkannte Geschäftszwecke des Verantwortlichen erheblich gefährden würde, es sei denn, dass das Interesse der betroffenen Person an der Informationserteilung überwiegt, oder
   b) die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in 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. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat.

(3) Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten durch öffentliche Stellen 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.

§ 34

Auskunftsrecht der betroffenen Person

(1) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht ergänzend zu den in § 27 Absatz 2, § 28 Absatz 2 und § 29 Absatz 1 Satz 2 genannten Ausnahmen nicht, wenn

1. die betroffene Person nach § 33 Absatz 1 und 3 nicht zu informieren ist oder
2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsgemäßer oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(2) Die Gründe der Auskunftsverweigerung sind zu dokumentieren. Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Die zum Zweck der Auskunftserteilung an die betroffene Person und zu deren Vorbereitung gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verarbeitet werden; für andere Zwecke ist die Verarbeitung nach Maßgabe des Artikels 18 der Verordnung (EU) 2016/679 einzuschränken.

(3) Wird der betroffenen Person durch eine öffentliche Stelle des Bundes keine Auskunft erteilt, so ist sie auf ihr Verlangen der oder dem Bundesbeauftragten zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung der oder des Bundesbeauftragten an die betroffene Person über das Ergebnis der datenschutzrechtlichen Prüfung darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Auskunft zustimmt.

(4) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die durch eine öffentliche Stelle weder automatisiert verarbeitet noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert 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.

§ 35

Recht auf Löschung

(1) Ist eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

(2) Ergänzend zu Artikel 18 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 gilt Absatz 1 Satz 1 und 2 entsprechend im Fall des Artikels 17 Absatz 1 Buchstabe a und d der Verordnung (EU) 2016/679, solange und soweit der Verantwortliche Grund zu der Annahme hat, dass durch eine Löschung schutzwürdige

Interessen der betroffenen Person beeinträchtigt würden. Der Verantwortliche unterrichtet die betroffene Person über die Einschränkung der Verarbeitung, sofern sich die Unterrichtung nicht als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.

(3) Ergänzend zu Artikel 17 Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 gilt Absatz 1 entsprechend im Fall des Artikels 17 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679, wenn einer Löschung satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen.

§ 36

Widerspruchsrecht

Das Recht auf Widerspruch gemäß Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 gegenüber einer öffentlichen Stelle besteht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

§ 37

Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Das Recht gemäß Artikel 22 Absatz 1 der Verordnung (EU) 2016/679, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, besteht über die in Artikel 22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 genannten Ausnahmen hinaus nicht, wenn die Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht und

1. dem Begehren der betroffenen Person stattgegeben wurde oder
2. die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht und der Verantwortliche für den Fall, dass dem Antrag nicht vollumfänglich stattgegeben wird, angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung zählt; der Verantwortliche informiert die betroffene Person über diese Rechte spätestens im Zeitpunkt der Mitteilung, aus der sich ergibt, dass dem Antrag der betroffenen Person nicht vollumfänglich stattgegeben wird.

(2) Entscheidungen nach Absatz 1 dürfen auf der Verarbeitung von Gesundheitsdaten im Sinne des Artikels 4 Nummer 15 der Verordnung (EU) 2016/679 beruhen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

Kapitel 3

Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 38

Datenschutzbeauftragte nichtöffentlicher Stellen

(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder

für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

(2) § 6 Absatz 4, 5 Satz 2 und Absatz 6 finden Anwendung, § 6 Absatz 4 jedoch nur, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.

§ 39

Akkreditierung

Die Erteilung der Befugnis, als Zertifizierungsstelle gemäß Artikel 43 Absatz 1 Satz 1 der Verordnung (EU) 2016/679 tätig zu werden, erfolgt durch die für die datenschutzrechtliche Aufsicht über die Zertifizierungsstelle zuständige Aufsichtsbehörde des Bundes oder der Länder auf der Grundlage einer Akkreditierung durch die Deutsche Akkreditierungsstelle. § 2 Absatz 3 Satz 2, § 4 Absatz 3 und § 10 Absatz 1 Satz 1 Nummer 3 des Akkreditierungsstellengesetzes finden mit der Maßgabe Anwendung, dass der Datenschutz als ein dem Anwendungsbereich des § 1 Absatz 2 Satz 2 unterfallender Bereich gilt.

Kapitel 4

Aufsichtsbehörde für die Datenverarbeitung durch nichtöffentliche Stellen

§ 40

Aufsichtsbehörden der Länder

(1) Die nach Landesrecht zuständigen Behörden überwachen im Anwendungsbereich der Verordnung (EU) 2016/679 bei den nichtöffentlichen Stellen die Anwendung der Vorschriften über den Datenschutz.

(2) Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten; hierbei darf sie Daten an andere Aufsichtsbehörden übermitteln. Eine Verarbeitung zu einem anderen Zweck ist über Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 hinaus zulässig, wenn

1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,
2. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist oder
3. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist.

Stellt die Aufsichtsbehörde einen Verstoß gegen die Vorschriften über den Datenschutz fest, so ist sie befugt, die betroffenen Personen hierüber zu unterrichten, den Verstoß anderen für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten. § 13 Absatz 4 Satz 4 bis 7 gilt entsprechend.

(3) Die der Aufsicht unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben einer Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Absatz 1 Nummer 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

(4) Die von einer Aufsichtsbehörde mit der Überwachung der Einhaltung der Vorschriften über den Datenschutz beauftragten Personen sind befugt, zur Erfüllung ihrer Aufgaben Grundstücke und Geschäftsräume der Stelle zu betreten und Zugang zu allen Datenverarbeitungsanlagen und -geräten zu erhalten. Die Stelle ist insoweit zur Duldung verpflichtet. § 16 Absatz 4 gilt entsprechend.

(5) Die Aufsichtsbehörden beraten und unterstützen die Datenschutzbeauftragten mit Rücksicht auf deren typische Bedürfnisse. Sie können die Abberufung der oder des Datenschutzbeauftragten verlangen, wenn sie oder er die zur Erfüllung ihrer oder seiner Aufgaben erforderliche Fachkunde nicht besitzt oder im Fall des Artikels 38 Absatz 6 der Verordnung (EU) 2016/679 ein schwerwiegender Interessenkonflikt vorliegt.

(6) Die Anwendung der Gewerbeordnung bleibt unberührt.

Kapitel 5

Sanktionen

§ 41

Anwendung der Vorschriften über das Bußgeld- und Strafverfahren

(1) Für Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß. Die §§ 17, 35 und 36 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung.

(2) Für Verfahren wegen eines Verstoßes nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten und der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung und des Gerichtsverfassungsgesetzes, entsprechend. Die §§ 56 bis 58, 87, 88, 99 und 100 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung. § 69 Absatz 4 Satz 2 des Gesetzes über Ordnungswidrigkeiten findet mit der Maßgabe Anwendung, dass die Staatsanwaltschaft das Verfahren nur mit Zustimmung der Aufsichtsbehörde, die den Bußgeldbescheid erlassen hat, einstellen kann.

§ 42

Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 und eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 dürfen in einem Strafverfahren gegen die meldepflichtige Person oder einen ihrer in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung verwendet werden.

§ 43

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder
2. entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

(4) Eine Meldung, die der Meldepflichtige nach Artikel 33 der Verordnung (EU) 2016/679 erteilt hat, oder eine nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 erfolgte Benachrichtigung darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder in § 52 Absatz 1 der Strafprozessordnung bezeichnete Angehörige des Meldepflichtigen oder Benachrichtigenden nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

Kapitel 6

Rechtsbehelfe

§ 44

Klagen gegen den Verantwortlichen oder Auftragsverarbeiter

(1) Klagen der betroffenen Person gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Anwendungsbereich der Verordnung (EU) 2016/679 oder der darin enthaltenen Rechte der betroffenen Person können bei dem Gericht des Ortes erhoben werden, an dem sich eine Niederlassung des Verantwortlichen oder Auftragsverarbeiters befindet. Klagen nach Satz 1 können auch bei dem Gericht des Ortes erhoben werden, an dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat.

(2) Absatz 1 gilt nicht für Klagen gegen Behörden, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden sind.

(3) Hat der Verantwortliche oder Auftragsverarbeiter einen Vertreter nach Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 benannt, gilt dieser auch als bevollmächtigt, Zustellungen in zivilgerichtlichen Verfahren nach Absatz 1 entgegenzunehmen. § 184 der Zivilprozessordnung bleibt unberührt.

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

§ 45

Anwendungsbereich

Die Vorschriften dieses Teils gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche. Die Verhütung von Straftaten im Sinne des Satzes 1 umfasst den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit. Die Sätze 1 und 2 finden zudem Anwendung auf diejenigen öffentlichen Stellen, die für die Vollstreckung von Strafen von Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs, von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes und von Geldbußen zuständig sind. Soweit dieser Teil Vorschriften für Auftragsverarbeiter enthält, gilt er auch für diese.

§ 46

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

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

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

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

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

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

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

14. „besondere Kategorien personenbezogener Daten“

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

    b) genetische Daten,

    c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,

    d) Gesundheitsdaten und

    e) Daten zum Sexualleben oder zur sexuellen Orientierung;

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

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

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

§ 47

Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen

1. auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,
2. für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,
3. dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sein,
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,
5. 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, und
6. 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.

Kapitel 2

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 48

Verarbeitung besonderer Kategorien personenbezogener Daten

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

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

1. spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle,
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.

§ 49

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 § 45 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 § 45 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

§ 50

Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken

Personenbezogene Daten dürfen im Rahmen der in § 45 genannten Zwecke in archivarischer, wissenschaftlicher oder statistischer Form verarbeitet werden, wenn hieran ein öffentliches Interesse besteht und geeignete Garantien für die Rechtsgüter der betroffenen Personen vorgesehen werden. Solche Garantien können in einer so zeitnah wie möglich erfolgenden Anonymisierung der personenbezogenen Daten, in Vorkehrungen gegen ihre unbefugte Kenntnisnahme durch Dritte oder in ihrer räumlich und organisatorisch von den sonstigen Fachaufgaben getrennten Verarbeitung bestehen.

§ 51

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 eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

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

(4) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden. Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

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

§ 52

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.

§ 53

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.

§ 54

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.

(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.

Kapitel 3

Rechte der betroffenen Person

§ 55

Allgemeine Informationen zu Datenverarbeitungen

Der Verantwortliche hat in allgemeiner Form und für jedermann zugänglich 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 oder den Bundesbeauftragten anzurufen, und
5. die Erreichbarkeit der oder des Bundesbeauftragten.

§ 56

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 § 55 genannten Angaben,
2. die Rechtsgrundlage der Verarbeitung,
3. die Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Fristen,
4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten 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 § 45 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 § 57 Absatz 7 entsprechend.

§ 57

Auskunftsrecht

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

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und die Kategorie, zu der sie gehören,
2. die verfügbaren Informationen über die Herkunft der Daten,
3. die Zwecke der Verarbeitung und deren Rechtsgrundlage,
4. die Empfänger oder die Kategorien von Empfängern, gegenüber denen die Daten offengelegt worden sind, insbesondere bei Empfängern in Drittstaaten oder bei internationalen Organisationen,
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 § 60, die oder den Bundesbeauftragten anzurufen, sowie
8. Angaben zur Erreichbarkeit der oder des Bundesbeauftragten.

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

(3) Von der Auskunftserteilung ist abzusehen, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, und deshalb der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

(4) Der Verantwortliche kann unter den Voraussetzungen des § 56 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 § 56 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 oder den Bundesbeauftragten ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie gemäß § 60 die oder den Bundesbeauftragten 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 Bundesbeauftragten zu erteilen, soweit nicht die zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die oder der Bundesbeauftragte hat die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie stattgefunden hat. Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. Die Mitteilung der oder des Bundesbeauftragten 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 Bundesbeauftragte hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

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

§ 58

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 Daten zu verlangen. Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder der Beurteilung, sondern die Tatsache, dass die Aussage oder Beurteilung so erfolgt ist. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. In diesem Fall hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wieder aufhebt. Die betroffene Person kann zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

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

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

1. Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigen würde,
2. die Daten zu Beweiszwecken in Verfahren, die Zwecken des § 45 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 verarbeitet werden, der ihrer Löschung entgegenstand.

(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 einer Stelle, die ihm die personenbezogenen Daten zuvor übermittelt hat, die Berichtigung mitzuteilen. Der Empfänger hat die Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken. In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1 bis 3 hat der Verantwortliche anderen Empfängern, denen die Daten übermittelt wurden, diese Maßnahmen mitzuteilen.

(6) Der Verantwortliche hat die betroffene Person über ein Absehen von der Berichtigung 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 § 56 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) § 57 Absatz 7 und 8 findet entsprechende Anwendung.

§ 59

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 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 § 57 Absatz 6 und des § 58 Absatz 6 unverzüglich schriftlich darüber in Kenntnis zu setzen, wie verfahren wurde.

(3) Die Erteilung von Informationen nach § 55, die Benachrichtigungen nach den §§ 56 und 66 und die Bearbeitung von Anträgen nach den §§ 57 und 58 erfolgen unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 57 und 58 kann der Verantwortliche entweder eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall muss der Verantwortliche den offenkundig unbegründeten oder exzessiven Charakter des Antrags belegen können.

(4) Hat der Verantwortliche begründete Zweifel an der Identität einer betroffenen Person, die einen Antrag nach den §§ 57 oder 58 gestellt hat, kann er von ihr zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

§ 60

Anrufung der oder des Bundesbeauftragten

(1) Jede betroffene Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die oder den Bundesbeauftragten wenden, wenn sie der Auffassung ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen zu den in § 45 genannten Zwecken in ihren Rechten verletzt worden zu sein. Dies gilt nicht für die Verarbeitung von personenbezogenen Daten durch Gerichte, soweit diese die Daten im Rahmen ihrer justiziellen Tätigkeit verarbeitet haben. Die oder der Bundesbeauftragte hat die betroffene Person über den Stand und das Ergebnis der Beschwerde zu unterrichten und sie hierbei auf die Möglichkeit gerichtlichen Rechtsschutzes nach § 61 hinzuweisen.

(2) Die oder der Bundesbeauftragte hat eine bei ihr oder ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer Aufsichtsbehörde in einem anderen Mitgliedstaat der Europäischen Union fällt, unverzüglich an die zuständige Aufsichtsbehörde des anderen Staates 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.

§ 61

Rechtsschutz gegen Entscheidungen der oder des Bundesbeauftragten oder bei deren oder dessen Untätigkeit

(1) Jede natürliche oder juristische Person kann unbeschadet anderer Rechtsbehelfe gerichtlich gegen eine verbindliche Entscheidung der oder des Bundesbeauftragten vorgehen.

(2) Absatz 1 gilt entsprechend zugunsten betroffener Personen, wenn sich die oder der Bundesbeauftragte mit einer Beschwerde nach § 60 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

§ 62

Auftragsverarbeitung

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

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

(3) Auftragsverarbeiter dürfen ohne vorherige schriftliche Genehmigung des Verantwortlichen keine weiteren Auftragsverarbeiter hinzuziehen. Hat der Verantwortliche dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, hat der Auftragsverarbeiter den Verantwortlichen

über jede beabsichtigte Hinzuziehung oder Ersetzung zu informieren. Der Verantwortliche kann in diesem Fall die Hinzuziehung oder Ersetzung untersagen.

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

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

1. nur auf dokumentierte Weisung des Verantwortlichen handelt; ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, hat er den Verantwortlichen unverzüglich zu informieren;
2. gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
3. den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten;
4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht;
5. dem Verantwortlichen alle erforderlichen Informationen, insbesondere die gemäß § 76 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt;
6. Überprüfungen, die von dem Verantwortlichen oder einem anderen von diesem beauftragten 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 § 64 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 den §§ 64 bis 67 und 69 genannten Pflichten unterstützt.

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

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

§ 63

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.

§ 64

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. Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

(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 oder Löschens 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).

Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

§ 65

Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Bundesbeauftragten

(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 Bundesbeauftragten zu melden, es sei denn, dass die Verletzung voraussichtlich keine Gefahr für die Rechtsgüter natürlicher Personen mit sich gebracht hat. Erfolgt die Meldung an die Bundesbeauftragte oder den Bundesbeauftragten nicht innerhalb von 72 Stunden, so 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) § 42 Absatz 4 findet entsprechende Anwendung.

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

§ 66

Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

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

(2) Die Benachrichtigung nach Absatz 1 hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in § 65 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 wie Verschlüsselungen, 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 Bundesbeauftragte 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 zur Folge hat.

(5) Die Benachrichtigung der betroffenen Personen nach Absatz 1 kann unter den in § 56 Absatz 2 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht die Interessen der betroffenen Person aufgrund der von der Verletzung ausgehenden erheblichen Gefahr überwiegen.

(6) § 42 Absatz 4 findet entsprechende Anwendung.

§ 67

Durchführung einer Datenschutz-Folgenabschätzung

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

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

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

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

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den 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.

§ 68

Zusammenarbeit mit der oder dem Bundesbeauftragten

Der Verantwortliche hat mit der oder dem Bundesbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben zusammenzuarbeiten.

§ 69

Anhörung der oder des Bundesbeauftragten

(1) Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die oder den Bundesbeauftragten anzuhören, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 67 hervorgeht, dass die Verarbeitung eine hohe Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hätte, wenn der Verantwortliche keine Abhilfemaßnahmen treffen würde, 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 Bundesbeauftragte kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur Anhörung nach Satz 1 unterliegen.

(2) Der oder dem Bundesbeauftragten sind im Fall des Absatzes 1 vorzulegen:

1. die nach § 67 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 Bundesbeauftragte 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 Bundesbeauftragte 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 Bundesbeauftragten im Nachhinein zu berücksichtigen und sind die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.

§ 70

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 Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen,
4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
5. gegebenenfalls die Verwendung von Profiling,
6. gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,
7. Angaben über die Rechtsgrundlage der Verarbeitung,
8. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und
9. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 64.

(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 § 64.

(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 Bundesbeauftragten zur Verfügung zu stellen.

§ 71

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 wie etwa die Datensparsamkeit 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. 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.

§ 72

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. verurteilte Straftäter,
4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und
5. andere Personen wie insbesondere Zeugen, Hinweisgeber oder Personen, die mit den in den Nummern 1 bis 4 genannten Personen in Kontakt oder Verbindung stehen.

§ 73

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.

§ 74

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.

§ 75

Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung

(1) Der Verantwortliche hat personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. Eine Berichtigung hat er einer Stelle, die die Daten zuvor an ihn übermittelt hat, mitzuteilen.

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

(4) Unbeschadet in Rechtsvorschriften festgesetzter 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.

§ 76

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 Bundesbeauftragte oder den Bundesbeauftragten 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 am Ende des auf deren Generierung folgenden Jahres zu löschen.

(5) Der Verantwortliche und der Auftragsverarbeiter haben die Protokolle der oder dem Bundesbeauftragten auf Anforderung zur Verfügung zu stellen.

§ 77

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

§ 78

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 § 45 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 weiter übermittelt, wenn der Verantwortliche diese Übermittlung zuvor genehmigt hat. Bei der Entscheidung über die Erteilung der Genehmigung hat der Verantwortliche alle maßgeblichen Faktoren zu berücksichtigen, insbesondere die Schwere der Straftat, den Zweck der ursprünglichen Übermittlung und das in dem Drittstaat oder der internationalen Organisation, an das oder an die die Daten weiter übermittelt 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.

§ 79

Datenübermittlung bei geeigneten Garantien

(1) Liegt entgegen § 78 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 § 78 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 Bundesbeauftragten auf Anforderung zur Verfügung zu stellen.

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

§ 80

Datenübermittlung ohne geeignete Garantien

(1) Liegt entgegen § 78 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 § 79 Absatz 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 78 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 § 45 genannten Zwecke oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 45 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 § 79 Absatz 2 entsprechend.

§ 81

Sonstige Datenübermittlung an Empfänger in Drittstaaten

(1) Verantwortliche können bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 78 Absatz 1 Nummer 1 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung ihrer Aufgaben unbedingt erforderlich ist und

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

2. die Übermittlung an die in § 78 Absatz 1 Nummer 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und
3. der Verantwortliche 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 § 78 Absatz 1 Nummer 1 genannten Stellen unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für Übermittlungen nach Absatz 1 gilt § 79 Absatz 2 und 3 entsprechend.

(4) Bei Übermittlungen nach Absatz 1 hat der Verantwortliche den Empfänger zu verpflichten, die übermittelten personenbezogenen Daten ohne seine Zustimmung 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

§ 82

Gegenseitige Amtshilfe

(1) Die oder der Bundesbeauftragte hat den Datenschutzaufsichtsbehörden in 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 Bundesbeauftragte hat alle geeigneten Maßnahmen zu ergreifen, um Amtshilfeersuchen unverzüglich und spätestens innerhalb eines Monats nach deren Eingang nachzukommen.

(3) Die oder der Bundesbeauftragte 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 Bundesbeauftragte 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 Bundesbeauftragte 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 Bundesbeauftragte hat Amtshilfeersuchen kostenfrei zu erledigen, soweit sie oder er nicht im Einzelfall mit der Aufsichtsbehörde des anderen Staates die Erstattung entstandener Ausgaben vereinbart hat.

(7) Ein Amtshilfeersuchen der oder des Bundesbeauftragten 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

§ 83
Schadensersatz und Entschädigung

(1) Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nach diesem Gesetz oder nach anderen auf ihre Verarbeitung anwendbaren Vorschriften rechtswidrig war, einen Schaden zugefügt, ist er oder sein Rechtsträger der betroffenen Person zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit bei einer nichtautomatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist.

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

(3) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welche 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.

§ 84
Strafvorschriften

Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von Tätigkeiten nach § 45 Satz 1, 3 oder 4 findet § 42 entsprechende Anwendung.

Teil 4
Besondere Bestimmungen für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten

§ 85
Verarbeitung personenbezogener Daten im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten

(1) Die Übermittlung personenbezogener Daten an einen Drittstaat oder an über- oder zwischenstaatliche Stellen oder internationale Organisationen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten ist über die bereits gemäß der Verordnung

(EU) 2016/679 zulässigen Fälle hinaus auch dann zulässig, wenn sie zur Erfüllung eigener Aufgaben aus zwingenden Gründen der Verteidigung oder zur Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist. Der Empfänger ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie übermittelt wurden.

(2) Für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten durch Dienststellen im Geschäftsbereich des Bundesministeriums der Verteidigung gilt § 16 Absatz 4 nicht, soweit das Bundesministerium der Verteidigung im Einzelfall feststellt, dass die Erfüllung der dort genannten Pflichten die Sicherheit des Bundes gefährden würde.

(3) Für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten durch öffentliche Stellen des Bundes besteht keine Informationspflicht gemäß Artikel 13 Absatz 1 und 2 der Verordnung (EU) 2016/679, wenn

1. es sich um Fälle des § 32 Absatz 1 Nummer 1 bis 3 handelt oder
2. durch ihre Erfüllung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen, und deswegen das Interesse der betroffenen Person an der Erteilung der Information zurücktreten muss.

Ist die betroffene Person in den Fällen des Satzes 1 nicht zu informieren, besteht auch kein Recht auf Auskunft. § 32 Absatz 2 und § 33 Absatz 2 finden keine Anwendung.

Artikel 2

Änderung des Bundesverfassungsschutzgesetzes

Das Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. § 6 wird wie folgt geändert:
   a) In Absatz 2 Satz 4 wird das Wort „sperren“ durch die Wörter „die Verarbeitung einschränken“ ersetzt.
   b) In Absatz 3 Satz 1 wird die Angabe „nach § 9“ durch die Angabe „entsprechend § 64“ ersetzt.
2. § 8 Absatz 1 Satz 1 wird wie folgt gefasst:

   „Das Bundesamt für Verfassungsschutz darf die zur Erfüllung seiner Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten verarbeiten, soweit nicht die anzuwendenden Bestimmungen des Bundesdatenschutzgesetzes oder besondere Regelungen in diesem Gesetz entgegenstehen; die Verarbeitung ist auch zulässig, wenn der Betroffene eingewilligt hat.“
3. In § 8b Absatz 2 Satz 4 werden die Wörter „Erhebung, Verarbeitung und Nutzung“ durch das Wort „Verarbeitung“ ersetzt.
4. § 12 wird wie folgt geändert:
   a) In der Überschrift wird das Wort „Sperrung“ durch das Wort „Verarbeitungseinschränkung“ ersetzt.
   b) Absatz 2 Satz 3 wird wie folgt gefasst:

      „In diesem Falle ist die Verarbeitung einzuschränken.“
5. § 13 wird wie folgt geändert:
   a) Absatz 2 wird wie folgt gefasst:

      „(2) Das Bundesamt für Verfassungsschutz hat die Verarbeitung personenbezogener Daten einzuschränken, wenn es im Einzelfall feststellt, dass ohne die Beschränkung schutzwürdige Interessen des

Betroffenen beeinträchtigt würden und die Daten für seine künftige Aufgabenerfüllung nicht mehr erforderlich sind. Verarbeitungsbeschränkte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nicht mehr genutzt oder übermittelt werden. Eine Aufhebung der Beschränkung ist möglich, wenn ihre Voraussetzungen nachträglich entfallen.“

b) Absatz 3 Satz 5 und 6 wird wie folgt gefasst:

„In diesem Fall ist die Verarbeitung der in der Akte gespeicherten personenbezogenen Daten einzuschränken und mit einem entsprechenden Vermerk zu versehen. Sie dürfen nur für die Interessen nach Satz 4 verarbeitet werden oder wenn es zur Abwehr einer erheblichen Gefahr unerlässlich ist.“

6. Dem § 14 Absatz 1 wird folgender Satz angefügt:

„Das Bundesamt für Verfassungsschutz führt ein Verzeichnis der geltenden Dateianordnungen.“

7. § 22a wird wie folgt geändert:

a) In Absatz 5 wird das Wort „Sperrung“ durch das Wort „Verarbeitungsbeschränkung“ ersetzt.

b) In Absatz 6 Satz 1 Nummer 9 wird die Angabe „nach § 8“ durch die Angabe „entsprechend § 83“ ersetzt.

8. § 22b Absatz 7 Satz 1 und 2 wird wie folgt gefasst:

„Das Bundesamt für Verfassungsschutz trifft für die Dateien die technischen und organisatorischen Maßnahmen entsprechend § 64 des Bundesdatenschutzgesetzes. § 6 Absatz 3 Satz 2 bis 5 und § 26a gelten nur für die vom Bundesamt für Verfassungsschutz eingegebenen Daten sowie dessen Abrufe.“

9. § 25 Satz 3 wird wie folgt gefasst:

„Die Vernichtung kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unvertretbarem Aufwand möglich ist; in diesem Fall ist die Verarbeitung der Daten zu beschränken.“

10. § 27 wird durch die folgenden §§ 26a und 27 ersetzt:

„§ 26a

Unabhängige Datenschutzkontrolle

(1) Jedermann kann sich an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch das Bundesamt für Verfassungsschutz in seinen Rechten verletzt worden zu sein.

(2) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert beim Bundesamt für Verfassungsschutz die Einhaltung der Vorschriften über den Datenschutz. Soweit die Einhaltung von Vorschriften der Kontrolle durch die G 10-Kommission unterliegt, unterliegt sie nicht der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, es sei denn, die G 10-Kommission ersucht die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, sie bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

(3) Das Bundesamt für Verfassungsschutz ist verpflichtet, die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und ihre oder seine schriftlich besonders Beauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Den in Satz 1 genannten Personen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 2 stehen,

2. jederzeit Zutritt in alle Diensträume zu gewähren.

Dies gilt nicht, soweit das Bundesministerium des Innern im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(4) Die Absätze 1 bis 3 gelten ohne Beschränkung auf die Erfüllung der Aufgaben nach § 3. Sie gelten entsprechend für die Verarbeitung personenbezogener Daten durch andere Stellen, wenn diese der Erfüllung der Aufgaben von Verfassungsschutzbehörden nach § 3 dient. § 16 Absatz 1 und 4 des Bundesdatenschutzgesetzes findet keine Anwendung.

§ 27

Anwendung des Bundesdatenschutzgesetzes

Bei der Erfüllung der Aufgaben nach § 3 durch das Bundesamt für Verfassungsschutz findet das Bundesdatenschutzgesetz wie folgt Anwendung:

1. § 1 Absatz 8, die §§ 4, 16 Absatz 1 und 4 und die §§ 17 bis 21 sowie 85 finden keine Anwendung,
2. die §§ 46, 51 Absatz 1 bis 4 und die §§ 52 bis 54, 62, 64, 83, 84 sind entsprechend anzuwenden.“

Artikel 3

Änderung des MAD-Gesetzes

Das MAD-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2977), das zuletzt durch Artikel 2 des Gesetzes vom 17. November 2015 (BGBl. I S. 1938) geändert worden ist, wird wie folgt geändert:

1. § 4 Absatz 1 wird wie folgt gefasst:

„(1) Der Militärische Abschirmdienst darf die zur Erfüllung seiner Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten verarbeiten nach § 8 Absatz 2, 4 und 5 des Bundesverfassungsschutzgesetzes, soweit nicht die anzuwendenden Bestimmungen des Bundesdatenschutzgesetzes oder besondere Regelungen in diesem Gesetz entgegenstehen; die Verarbeitung ist auch zulässig, wenn der Betroffene eingewilligt hat. Der Militärische Abschirmdienst ist nicht befugt, personenbezogene Daten zur Erfüllung seiner Aufgaben nach § 1 Absatz 2 zu erheben. § 8 Absatz 2 des Bundesverfassungsschutzgesetzes findet mit der Maßgabe Anwendung, dass die Zustimmung zur Dienstanweisung durch das Bundesministerium der Verteidigung erteilt wird.“

2. In § 6 Absatz 2 werden die Wörter „zu sperren“ durch die Wörter „ihre Verarbeitung einzuschränken“ ersetzt.
3. In § 10 Absatz 2 Satz 2 werden nach den Wörtern „frühere Namen,“ die Wörter „das Geburtsdatum,“ eingefügt.
4. Nach § 12 wird folgender § 12a eingefügt:

„§12a

Unabhängige Datenschutzkontrolle

§ 26a des Bundesverfassungsschutzgesetzes ist mit der Maßgabe entsprechend anzuwenden, dass an die Stelle des Bundesministeriums des Innern das Bundesministerium der Verteidigung tritt.“

5. § 13 wird wie folgt gefasst:

„§ 13

Anwendung des Bundesdatenschutzgesetzes

Bei der Erfüllung der Aufgaben nach § 1 Absatz 1 bis 3, den §§ 2 und 14 durch den Militärischen Abschirmdienst findet das Bundesdatenschutzgesetz wie folgt Anwendung:

1. § 1 Absatz 8, die §§ 4, 16 Absatz 1 und 4 und die §§ 17 bis 21 sowie 85 finden keine Anwendung,
2. die §§ 46, 51 Absatz 1 bis 4 und die §§ 52 bis 54, 62, 64, 83, 84 sind entsprechend anzuwenden.“

Artikel 4

Änderung des BND-Gesetzes

Das BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch … geändert worden ist, wird wie folgt geändert

1. In § 1 Absatz 2 Satz 2 werden die Wörter „Erhebung, Verarbeitung und Nutzung“ durch das Wort „Verarbeitung“ ersetzt.
2. § 2 Absatz 1 wird wie folgt geändert:
   a) Im Satzteil vor Nummer 1 werden die Wörter „erheben, verarbeiten und nutzen“ durch das Wort „verarbeiten“ ersetzt.
   b) Folgender Satz wird angefügt:

      „Die Verarbeitung ist auch zulässig, wenn der Betroffene eingewilligt hat.“
3. § 6 wird wie folgt geändert:
   a) In der Überschrift werden die Wörter „Erhebung und“ gestrichen.
   b) In Absatz 1 Satz 1 werden die Wörter „erheben und“ gestrichen.
4. In § 7 werden die Wörter „Verarbeitung und Nutzung“ in der Überschrift durch die Wörter „Weitere Verarbeitung“ und in Absatz 1 durch die Wörter „weitere Verarbeitung“ ersetzt.
5. In § 10 Absatz 4 Satz 6 wird das Wort „gesperrt“ durch die Wörter „in ihrer Verarbeitung eingeschränkt“ ersetzt.
6. In der Überschrift zu Abschnitt 3 wird das Wort „Datenverarbeitung“ durch das Wort „Datenweiterverarbeitung“ ersetzt.
7. § 20 wird wie folgt geändert:
   a) In der Überschrift wird das Wort „Sperrung“ durch das Wort „Verarbeitungseinschränkung“ ersetzt.
   b) In den Absätzen 1 und 2 Satz 1 werden jeweils die Wörter „zu sperren“ durch die Wörter „deren Verarbeitung einzuschränken“ ersetzt.
8. § 25 wird wie folgt geändert:
   a) In Absatz 5 wird das Wort „Sperrung“ durch das Wort „Verarbeitungseinschränkung“ ersetzt.
   b) In Absatz 6 Satz 1 Nummer 9 wird die Angabe „§ 8“ durch die Angabe „§ 83“ ersetzt.
9. In § 27 Absatz 2 wird das Wort „Sperrung“ durch das Wort „Verarbeitungseinschränkung“ ersetzt.
10. In § 28 Satz 2 Nummer 11 wird die Angabe „§ 8“ durch die Angabe „§ 83“ ersetzt.

11. § 32 wird wie folgt gefasst:

„§ 32

Unabhängige Datenschutzkontrolle

§ 26a des Bundesverfassungsschutzgesetzes ist mit der Maßgabe entsprechend anzuwenden, dass an die Stelle des Bundesministeriums des Innern das Bundeskanzleramt tritt.“

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

„§ 32a

Anwendung des Bundesdatenschutzgesetzes

Bei der Erfüllung der Aufgaben des Bundesnachrichtendienstes nach § 1 Absatz 2 ist das Bundesdatenschutzgesetz wie folgt anzuwenden:

1. von den Teilen 1 und 4 des Bundesdatenschutzgesetzes
   a) finden § 1 Absatz 8, die §§ 4, 16 Absatz 1 und 4, die §§ 17 bis 21 sowie 85 keine Anwendung,
   b) findet § 14 Absatz 2 mit der Maßgabe Anwendung, dass sich die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nur an die Bundesregierung sowie an die für die Kontrolle des Bundesnachrichtendienstes zuständigen Gremien (Parlamentarisches Kontrollgremium, Vertrauensgremium, G 10-Kommission, Unabhängiges Gremium) wenden darf; eine Befassung der für die Kontrolle des Bundesnachrichtendienstes zuständigen Gremien setzt voraus, dass sie oder er der Bundesregierung entsprechend § 16 Absatz 2 Satz 1 des Bundesdatenschutzgesetzes zuvor Gelegenheit gegeben hat, innerhalb einer von ihr oder ihm gesetzten Frist Stellung zu nehmen;
2. von Teil 3 des Bundesdatenschutzgesetzes sind die §§ 46, 51 Absatz 1 bis 4 sowie die §§ 52 bis 54, 62, 64, 83, 84 entsprechend anzuwenden.“

Artikel 5

Änderung des Sicherheitsüberprüfungsgesetzes

Das Sicherheitsüberprüfungsgesetz vom 20. April 1994 (BGBl. I S. 867), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:
   a) Die Angabe zu § 31 wird wie folgt gefasst:

      „§ 31 Datenverarbeitung in automatisierten Dateien“.
   b) Nach der Angabe zu § 36 wird folgende Angabe eingefügt:

      „§ 36a Unabhängige Datenschutzkontrolle“.
2. In § 19 Absatz 2 Satz 5 werden die Wörter „verarbeitet und genutzt“ durch die Wörter „gespeichert, genutzt, verändert, übermittelt und gelöscht“ ersetzt.
3. In § 21 Absatz 5 Satz 1 werden die Wörter „verarbeiten und nutzen“ durch die Wörter „speichern, nutzen, verändern und übermitteln“ ersetzt.
4. In § 22 Absatz 3 Satz 3 werden die Wörter „verarbeitet und genutzt“ durch die Wörter „genutzt, verändert, übermittelt und gelöscht“ ersetzt.

5. Die Überschrift von § 31 wird wie folgt gefasst:

„§ 31

Datenverarbeitung in automatisierten Dateien“.

6. § 36 wird durch die folgenden §§ 36 und 36a ersetzt:

„§ 36

Anwendung des Bundesdatenschutzgesetzes, Bundesverfassungsschutzgesetzes, MAD-Gesetzes und BND-Gesetzes

(1) Die Vorschriften des Bundesdatenschutzgesetzes finden wie folgt Anwendung:

1. § 1 Absatz 8, § 16 Absatz 1 und 4 und die §§ 17 bis 21 sowie 85 finden keine Anwendung,
2. die §§ 42, 46, 51 Absatz 1 und 3, die §§ 52, 53, 54 Absatz 1 und 2 sowie die §§ 62, 64, 83 sind entsprechend anzuwenden.

(2) Die Vorschriften des Ersten Abschnitts und die §§ 14 und 23 Nummer 3 des Bundesverfassungsschutzgesetzes auch in Verbindung mit § 12 des MAD-Gesetzes und § 31 des BND-Gesetzes sowie die §§ 1, 8 und 10 Absatz 2 Satz 2 bis 6 des MAD-Gesetzes und § 21 des BND-Gesetzes finden Anwendung.

§ 36a

Unabhängige Datenschutzkontrolle

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

(2) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert bei den öffentlichen und den nichtöffentlichen Stellen die Einhaltung der anzuwendenden Vorschriften über den Datenschutz bei der Erfüllung der Aufgaben dieses Gesetzes. Soweit die Einhaltung von Vorschriften der Kontrolle durch die G 10-Kommission unterliegt, unterliegt sie nicht der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, es sei denn, die G 10-Kommission ersucht die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, sie bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. Der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterliegen auch nicht personenbezogene Daten in Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit widerspricht.

(3) Die öffentlichen und nichtöffentlichen Stellen sind verpflichtet, die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und ihre oder seine schriftlich besonders Beauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Den in Satz 1 genannten Personen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 2 stehen,
2. jederzeit Zutritt in alle Diensträume zu gewähren.

Dies gilt nicht, soweit die zuständige oberste Bundesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.“

Artikel 6

Änderung des Artikel-10-Gesetzes

Das Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. § 4 wird wie folgt geändert:
   a) Absatz 1 Satz 7 wird wie folgt gefasst:

      „In diesem Fall ist die Verarbeitung der Daten einzuschränken; sie dürfen nur zu diesen Zwecken verwendet werden.“

   b) Absatz 4 wird wie folgt geändert:

      aa) Nach dem Wort „dürfen“ werden die Wörter „an andere als die nach § 1 Absatz 1 Nummer 1 berechtigten Stellen“ eingefügt.

      bb) Folgender Satz wird angefügt:

      „Bei der Übermittlung an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen ist daneben § 19 Absatz 3 Satz 2 und 4 des Bundesverfassungsschutzgesetzes anzuwenden.“

2. § 6 Absatz 1 Satz 7 wird wie folgt gefasst:

   „In diesem Fall ist die Verarbeitung der Daten einzuschränken; sie dürfen nur zu diesen Zwecken verwendet werden.“

3. In § 15 Absatz 5 Satz 2 werden die Wörter „Erhebung, Verarbeitung und Nutzung“ durch das Wort „Verarbeitung“ ersetzt.

4. In § 16 Satz 2 werden die Wörter „und Nutzung“ gestrichen.

Artikel 7

Änderung des Bundesdatenschutzgesetzes

Das Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 25. Februar 2015 (BGBl. I S. 162) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 42a folgende Angabe eingefügt:

   „§ 42b Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Rechtswidrigkeit eines Beschlusses der Europäischen Kommission“.

2. Nach § 22 Absatz 5 wird folgender Absatz 5a eingefügt:

   „(5a) Die oder der Bundesbeauftragte kann Aufgaben der Personalverwaltung und Personalwirtschaft auf andere Stellen des Bundes übertragen, soweit hierdurch die Unabhängigkeit der oder des Bundesbeauftragten nicht beeinträchtigt wird. Diesen Stellen dürfen personenbezogene Daten der Beschäftigten übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.“

3. Nach § 42a wird folgender § 42b eingefügt:

„§ 42b

Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Rechtswidrigkeit eines Beschlusses der Europäischen Kommission

(1) Hält eine Aufsichtsbehörde einen Angemessenheitsbeschluss der Europäischen Kommission, einen Beschluss über die Anerkennung von Standardschutzklauseln oder über die Allgemeingültigkeit von genehmigten Verhaltensregeln, auf dessen Gültigkeit es für eine Entscheidung der Aufsichtsbehörde ankommt, für rechtswidrig, so hat die Aufsichtsbehörde ihr Verfahren auszusetzen und einen Antrag auf gerichtliche Entscheidung zu stellen.

(2) Für Verfahren nach Absatz 1 ist der Verwaltungsrechtsweg gegeben. Die Verwaltungsgerichtsordnung ist nach Maßgabe der Absätze 3 bis 6 anzuwenden.

(3) Über einen Antrag der Aufsichtsbehörde nach Absatz 1 entscheidet im ersten und letzten Rechtszug das Bundesverwaltungsgericht.

(4) In Verfahren nach Absatz 1 ist die Aufsichtsbehörde beteiligungsfähig. An einem Verfahren nach Absatz 1 ist die Aufsichtsbehörde als Antragstellerin beteiligt; § 63 Nummer 3 und 4 der Verwaltungsgerichtsordnung bleibt unberührt. Das Bundesverwaltungsgericht kann der Europäischen Kommission Gelegenheit zur Äußerung binnen einer zu bestimmenden Frist geben.

(5) Ist ein Verfahren zur Überprüfung der Gültigkeit eines Beschlusses der Europäischen Kommission nach Absatz 1 bei dem Gerichtshof der Europäischen Union anhängig, so kann das Bundesverwaltungsgericht anordnen, dass die Verhandlung bis zur Erledigung des Verfahrens vor dem Gerichtshof der Europäischen Union auszusetzen sei.

(6) In Verfahren nach Absatz 1 ist § 47 Absatz 5 Satz 1 und Absatz 6 der Verwaltungsgerichtsordnung entsprechend anzuwenden. Kommt das Bundesverwaltungsgericht zu der Überzeugung, dass der Beschluss der Europäischen Kommission nach Absatz 1 gültig ist, so stellt es dies in seiner Entscheidung fest. Andernfalls legt es die Frage nach der Gültigkeit des Beschlusses gemäß Artikel 267 des Vertrags über die Arbeitsweise der Europäischen Union dem Gerichtshof der Europäischen Union zur Entscheidung vor.“

Artikel 8

Inkrafttreten, Außerkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am 25. Mai 2018 in Kraft. Gleichzeitig tritt das Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 7 des Gesetzes vom … [einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes] geändert worden ist, außer Kraft.

(2) Artikel 7 tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Am 25. Mai 2018 wird die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L EU L 119 vom 4.5.2016, S. 1) unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union sein. Ziel der Verordnung (EU) 2016/679 ist ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten in allen Mitgliedstaaten (Erwägungsgrund 10). Der Unionsgesetzgeber hat sich für die Handlungsform einer Verordnung entschieden, damit innerhalb der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist (Erwägungsgrund 13). Die Verordnung (EU) 2016/679 sieht eine Reihe von Öffnungsklauseln für den nationalen Gesetzgeber vor. Zugleich enthält die Verordnung (EU) 2016/679 konkrete, an die Mitgliedstaaten gerichtete Regelungsaufträge. Dies erfordert es, das allgemeine wie auch das bereichsspezifische Datenschutzrecht auf die Vereinbarkeit mit der Verordnung (EU) 2016/679 zu überprüfen und soweit nötig anzupassen. Dem dient der vorliegende Gesetzentwurf.

Darüber hinaus dient der vorliegende Gesetzentwurf der teilweisen Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU L 119 vom 4.5.2016, S. 89), soweit die Mitgliedstaaten nach Artikel 63 der Richtlinie verpflichtet sind, bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften zu erlassen, die erforderlich sind, um dieser Richtlinie nachzukommen. Die Umsetzung der Richtlinie (EU) 2016/680 wird über die im vorliegenden Gesetzentwurf enthaltenen relevanten Regelungen hinaus gesondert auch im Fachrecht erfolgen.

Um ein reibungsloses Zusammenspiel der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 mit dem stark ausdifferenzierten deutschen Datenschutzrecht sicherzustellen, ist es erforderlich, das bisherige Bundesdatenschutzgesetz (BDSG a. F.) durch ein neues Bundesdatenschutzgesetz (BDSG) abzulösen. Weiterer gesetzlicher Anpassungsbedarf ergibt sich hinsichtlich der bestehenden bereichsspezifischen Datenschutzregelungen des Bundes infolge der Änderungen im allgemeinen Datenschutzrecht durch die Verordnung (EU) 2016/679 und das sie ergänzende neu gefasste BDSG. Die hierzu erforderlichen Änderungen werden im Rahmen eines gesonderten Gesetzesvorhabens umgesetzt.

Im Interesse einer homogenen Entwicklung des allgemeinen Datenschutzrechts findet das neu gefasste BDSG, soweit es nicht selbst oder bereichsspezifische Gesetze abweichende Regelungen treffen, auch für die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten öffentlicher Stellen Anwendung, die außerhalb des Anwendungsbereichs des Unionsrechts liegen, wie etwa die Datenverarbeitung durch das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst oder im Bereich des Sicherheitsüberprüfungsgesetzes. Dies geht einher mit zusätzlichem gesetzlichen Änderungsbedarf in den jeweiligen bereichsspezifischen Gesetzen. Für diejenigen Bereiche, die nicht unter die beiden EU-Rechtsakte fallen und die über kein bereichsspezifisches Recht verfügen, wird die Verordnung (EU) 2016/679 und Teil 2 des neu gefassten BDSG für anwendbar erklärt, um entsprechend der Regelungssystematik des bisherigen BDSG ein datenschutzrechtliches Vollregime anzubieten.

Vor dem Hintergrund des Vorstehenden ergibt sich folgende Vierteilung des neu gefassten BDSG:

– Teil 1 „Gemeinsame Bestimmungen“ enthält Bestimmungen für jegliche Datenverarbeitung, unabhängig davon, ob sie zu Zwecken der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 oder zu nicht von

diesen beiden Unionsrechtsakten erfassten Zwecken (z. B. Datenverarbeitung durch Nachrichtendienste) erfolgt.

- Teil 2 „Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679“ betrifft Regelungen, die sich allein auf den Anwendungsbereich der Verordnung (EU) 2016/679 beziehen.
- Teil 3 „Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680“ dient der Umsetzung der Richtlinie (EU) 2016/680.
- Teil 4 „Besondere Bestimmungen für Verarbeitungen von nicht unter den Anwendungsbereich der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten“, mit dem Regelungsschwerpunkt, spezifischere Regelungen für die Behörden des Bundesministeriums der Verteidigung zu schaffen.

II. Wesentlicher Inhalt des Entwurfs

Der Gesetzentwurf sieht folgende Gesetzesänderungen vor:

1. Neufassung des BDSG (Artikel 1), das für öffentliche Stellen des Bundes und der Länder (soweit nicht landesrechtliche Regelungen greifen) sowie für nichtöffentliche Stellen gilt, bestehend aus vier Teilen:

   a. Gemeinsame Bestimmungen mit folgenden Regelungsschwerpunkten:

      - Schaffung allgemeiner Rechtsgrundlagen für die Datenverarbeitung durch öffentliche Stellen und für die Videoüberwachung (§§ 3, 4 BDSG);
      - Regelungen zu Datenschutzbeauftragten öffentlicher Stellen (§§ 5 bis 7 BDSG);
      - Ausgestaltung der unabhängigen Datenschutzaufsichtsbehörden (§§ 8 bis 16 BDSG);
      - Festlegung der deutschen Vertretung im Europäischen Datenschutzausschuss; gemeinsamer Vertreter im Ausschuss ist die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit; als Stellvertreter wählt der Bundesrat die Leiterin oder den Leiter einer Aufsichtsbehörde eines Landes (§§ 17 bis 19 BDSG);
      - Rechtsbehelfe (§§ 20, 21 BDSG).

   Die gemeinsamen Bestimmungen finden keine Anwendung, soweit das Recht der Europäischen Union unmittelbar gilt, insbesondere die Verordnung (EU) 2016/679. Sie finden außerdem Anwendung im Anwendungsbereich der Richtlinie (EU) 2016/680 sowie für die Bereiche, die außerhalb des Unionsrechts liegen.

   b. Bestimmungen zur Durchführung der Verordnung (EU) 2016/679 mit folgenden Regelungsschwerpunkten:

      - Schaffung einer Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten (§ 22 BDSG);
      - Festlegung der Zulässigkeitsvoraussetzungen für Verarbeitungen zu anderen Zwecken durch öffentliche Stellen (§ 23 BDSG) und durch nichtöffentliche Stellen (§ 24 BDSG) sowie für Datenübermittlungen durch öffentliche Stellen (§ 25 BDSG);
      - Regelung weiterer besonderer Verarbeitungssituationen (§§ 26 bis 31 BDSG);
      - Regelungen zu den Betroffenenrechten (§§ 32 bis 37 BDSG);
      - Verhängung von Geldbußen bei Verstößen gegen die Verordnung (EU) 2016/679 (§§ 41, 43 BDSG).

   c. Bestimmungen zur Umsetzung der Richtlinie EU 2016/680 mit folgenden Regelungsschwerpunkten:

      - Aussagen zu Rechtsgrundlagen der Verarbeitung, Zweckbindung und -änderung (§§ 47 bis 51 BDSG);

- Ausformung der Betroffenenrechte (§§ 55 bis 61 BDSG);
- Festlegung unterschiedlich akzentuierter Pflichten der Verantwortlichen
    - Anforderungen an Auftragsverarbeitungsverhältnisse (§ 62 BDSG);
    - Datensicherheit und Meldungen von Verletzungen des Schutzes personenbezogener Daten (§§ 64 bis 66 BDSG);
    - Instrumente zur Berücksichtigung des Datenschutzes (Datenschutz-Folgenabschätzung, Anhörung der oder des Bundesbeauftragten, Verzeichnis von Verarbeitungstätigkeiten, Protokollierung, §§ 67 bis 70 und 76 BDSG);
    - Berichtigungs- und Löschungspflichten (§ 75 BDSG);
- Datenübermittlungen an Stellen in Drittstaaten und an internationale Organisationen (§§ 78 bis 81 BDSG).

d. Besondere Bestimmungen für Datenverarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten.

2. Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes und des Sicherheitsüberprüfungsgesetzes (Artikel 2 bis 6) infolge der Ablösung des bisherigen Bundesdatenschutzgesetzes, die den Erfordernissen der außerhalb des Anwendungsbereichs des Unionsrechts fallenden Datenverarbeitungen im Bereich der nationalen Sicherheit Rechnung tragen.

3. Änderung des geltenden Bundesdatenschutzgesetzes (Artikel 7), die sicherstellt, dass das Klagerecht gegen Beschlüsse der Europäischen Kommission bereits vor Geltung der Verordnung (EU) 2016/679 zur Verfügung steht.

III. Alternativen

Keine.

IV. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt für Regelungen des Datenschutzes als Annex aus den jeweiligen Sachkompetenzen der Artikel 73 bis 74 des Grundgesetzes (GG). Im Bereich der öffentlichen Verwaltung bedarf es bundesrechtlicher Datenschutzbestimmungen, soweit dem Bund die Verwaltungskompetenz zusteht. Für nichtöffentliche Stellen folgt die Gesetzgebungskompetenz des Bundes im Bereich des Datenschutzes als Annex aus Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft). Nach Artikel 72 Absatz 2 GG steht dem Bund die Gesetzgebungskompetenz in diesen Fällen unter anderem dann zu, wenn und soweit eine bundesgesetzliche Regelung zur Wahrung der Rechtseinheit im gesamtstaatlichen Interesse erforderlich ist. Eine bundesgesetzliche Regelung des Datenschutzes ist zur Wahrung der Rechtseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Eine Regelung dieser Materie durch den Landesgesetzgeber würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch der Länder nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten. Es bestünde die Gefahr, dass z .B. die Betroffenenrechte durch die verschiedenen Landesgesetzgeber unterschiedlich eingeschränkt würden, mit der Folge, dass bundesweit agierende Unternehmen sich auf verschiedenste Vorgaben einrichten müssten.

Die Gesetzgebungskompetenz zu Teil 1 Kapitel 5 (Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle, Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union) folgt als Annexkompetenz aus Artikel 23 Absatz 1 Satz 2 GG und der Kompetenz des Bundes für auswärtige Angelegenheiten. Der Bund kann zur Verwirklichung eines vereinten Europas mit Zustimmung des Bundesrates durch Gesetz Hoheitsrechte auf die Europäische Union übertragen (Artikel 23 Absatz 1

Satz 2 GG). Die allgemeine Zuständigkeit in Fragen der europäischen Integration ist Teil der Kompetenzmaterie der auswärtigen Gewalt (Artikel 23, 24, 32, 59, 73 Nummer 1, 87a, 87b GG) und steht dem Bund zu.

Von seiner Kompetenz nach Artikel 23 Absatz 1 Satz 2 GG hat der Bund mit Zustimmung des Bundesrates mit der Übertragung von Hoheitsrechten im Bereich des Datenschutzes, insbesondere in Artikel 16 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV), Gebrauch gemacht, die in der Folge durch die Übertragung verbindlicher Einzelfallentscheidungsbefugnisse auf den mit eigener Rechtspersönlichkeit ausgestatteten Europäischen Datenschutzausschuss durch Artikel 68 ff. der Verordnung (EU) 2016/679 (im Bereich der Richtlinie (EU) 2016/680 nach Maßgabe des dortigen Artikels 51) ausgestaltet worden sind. Mit der Einrichtung eines Europäischen Datenschutzausschusses in Gestalt einer Einrichtung der Union mit eigener Rechtspersönlichkeit gemäß Artikel 68 Absatz 1 der Verordnung (EU) 2016/679 und Artikel 51 der Richtlinie (EU) 2016/680 wird der einheitliche europäische Rechtsraum in dem Querschnittsbereich des Datenschutzrechts zu einem Raum einheitlicher Rechtsanwendung und -durchsetzung fortentwickelt.

Kann der Bund mit Zustimmung des Bundesrates Hoheitsrechte auf die Europäische Union übertragen, so kann er als dessen Annex zugleich die Vertretung Deutschlands in einer Einrichtung der Union regeln, die diese Hoheitsrechte nach der Übertragung ausübt. Die unionsrechtlich in Artikel 51 Absatz 3 und 68 Absatz 4 der Verordnung (EU) 2016/679 vorgeschriebene Bestimmung des gemeinsamen Vertreters der deutschen Aufsichtsbehörden bedarf zwingend der konkretisierenden Durchführungsgesetzgebung auf nationaler Ebene. Für die Aufgabenerfüllung, insbesondere den Vollzug der durch den Europäischen Datenschutzausschuss ausgeübten unionsrechtlichen Hoheitsrechte, bedarf es zwingend der Mitwirkung des deutschen Vertreters. Einrichtung und Besetzung des Europäischen Datenschutzausschusses stehen in unmittelbarem Zusammenhang.

Der Europäische Datenschutzausschuss übt unionale und keine mitgliedstaatliche Verwaltungstätigkeit aus. Der Vertreter im Ausschuss handelt, vergleichbar den mitgliedschaftlichen Vertretern im Rat nach Artikel 16 Absatz 2 des Vertrages über die Europäische Union (EUV), als Repräsentant seines Mitgliedstaats bzw. der nationalen Datenschutzbeauftragten und zugleich für eine europäische Einrichtung, (vgl. Artikel 68 Absatz 1 der Verordnung (EU) 2016/679). Der Außenvertretung des Bundes entspricht die Einstandspflicht der Bundesrepublik Deutschland als Vertragspartei der Unionsverträge. Die europarechtliche Integrationskompetenz ist grundsätzlich auch dann Sache des Bundes, wenn innerstaatlich Zuständigkeiten der Länder betroffen sind. Gleichwohl hat der Bund den durch Kapitel VII der Verordnung (EU) 2016/679 in besonderem Maße berührten Verwaltungskompetenzen der Länder Rechnung zu tragen. Dem Grundsatz der kompetenzschonenden Kooperation wird über das Zustimmungserfordernis des Bundesrates auf institutioneller Ebene sowie das Mitwirkungsrecht zur Wahrung der Länderbelange auf inhaltlicher Ebene Rechnung getragen. Es ist angelehnt an die Konzeption des Artikels 23 Absatz 2 bis 6 GG und das Gesetz über die Zusammenarbeit von Bund und Ländern in Angelegenheiten der Europäischen Union (EUZBLG), die vergleichbare Grundkonstellationen zu lösen hatten. Im vorliegenden Gesetz wird die kompetenzschonende Kooperation verwirklicht durch die Bindung des gemeinsamen Vertreters an den mit Mehrheitsentscheidung getroffenen gemeinsamen Standpunkt aller Aufsichtsbehörden sowie die unmittelbaren Mitwirkungs- und Beteiligungsrechte des Ländervertreters im Ausschuss.

Die Gesetzgebungskompetenz des Bundes für die Vorschriften zum gerichtlichen Rechtsschutz (Artikel 1 §§ 20, 44 und 61) und über Rechtsbehelfe gegen Beschlüsse der Europäischen Kommission (Artikel 1 § 21) beruht auf Artikel 74 Absatz 1 Nummer 1 GG (Gerichtsverfassung, gerichtliches Verfahren). Für die Strafvorschriften und die Vorschriften über die Verhängung von Geldbußen ergibt sich die Gesetzgebungskompetenz des Bundes ebenfalls aus Artikel 74 Absatz 1 Nummer 1 GG (Strafrecht).

Die Kompetenz für die Änderung des Bundesverfassungsschutzgesetzes und des Artikel 10-Gesetzes ergibt sich aus Artikel 72 Absatz 1 Nummer 10b GG. Die Änderung des MAD-Gesetzes findet ihre Grundlage in Artikel 73 Absatz 1 Nummer 1 und Artikel 73 Absatz 1 Nummer 10b GG. Die Kompetenz des Bundes zur Änderung des BND-Gesetzes folgt aus Artikel 73 Absatz 1 Nummer 1 GG. Die Gesetzgebungskompetenz des Bundes für das Sicherheitsüberprüfungsgesetz ergibt sich aus der Natur der Sache und aus Artikel 74 Absatz 1 Nummer 11 GG. Nach Artikel 72 Absatz 2 GG in Verbindung mit Artikel 74 Absatz 1 Nummer 11 GG ist eine bundesgesetzliche Regelung erforderlich, weil es um sicherheitsempfindliche Tätigkeiten geht, die vom Bund zugewiesen beziehungsweise übertragen werden oder zu denen der Bund ermächtigt. Bei der Festlegung, unter welchen Bedingungen eine Sicherheitsüberprüfung vorgenommen wird, um den spezifischen staatlichen Sicherheitsinteressen des Bundes Rechnung zu tragen, handelt es sich um eine Angelegenheit, die nur vom Bund geregelt werden kann.

Hinzu kommt, dass der Bund mit den Sicherheitsüberprüfungen völkerrechtliche Verpflichtungen der Bundesrepublik Deutschland erfüllt. Insofern ist es erforderlich, die Rechtseinheit zu wahren und eine Rechtszersplitterung zu vermeiden.

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen vereinbar. Er dient der Durchführung der Verordnung (EU) 2016/679 und der Umsetzung der Richtlinie (EU) 2016/680.

Die Verordnung (EU) 2016/679 hat gemäß Artikel 288 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) allgemeine Geltung, ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat. Einer wiederholenden Wiedergabe von Teilen einer Verordnung setzt das sog. Wiederholungsverbot des Gerichtshofs der Europäischen Union (EuGH) Grenzen. Es soll verhindern, dass die unmittelbare Geltung einer Verordnung verschleiert wird, weil die Normadressaten über den wahren Urheber des Rechtsaktes oder die Jurisdiktion des EuGH im Unklaren gelassen werden (EuGH, Rs. C-34/73, Variola, Rn. 9 ff.; EuGH, Rs. C-94/77, Zerbone, Rn. 22/27).

Die sich im vorliegenden Gesetzentwurf auf die Verordnung (EU) 2016/679 beziehenden punktuellen Wiederholungen und Verweisungen sind aber aufgrund der besonderen Ausgangslage mit dem Unionsrecht vereinbar:

- Zwar formuliert die Verordnung (EU) 2016/679 in den Erwägungsgründen (siehe Erwägungsgründe 10, 9 und 13 Satz 1) das Ziel einer Vollharmonisierung, doch erreicht sie dieses Ziel nicht vollumfänglich. Die Verordnung ist als Grund-Verordnung ergänzungsbedürftig und regelt den Datenschutz nur im Grundsatz abschließend (z. B. regelt sie für den öffentlichen Bereich nicht die Rechtsgrundlagen der Verarbeitung). Sie schafft für den nationalen Gesetzgeber Spielräume durch sogenannte Öffnungsklauseln. In ca. 70 Fällen enthält sie insoweit Regelungsgebote oder -optionen. Im Umfang dieser legislativen Spielräume ist sie ein Novum und ähnelt in wesentlichen Teilen einer Richtlinie. Durch die zahlreichen Ausgestaltungsspielräume für den nationalen Gesetzgeber beschränkt bereits der Unionsgesetzgeber selbst die unmittelbare Wirkung. Bislang bekannte, vom nationalen Gesetzgeber auf der Grundlage einer Verordnung zu treffende Regelungen wie z. B. Zuständigkeitszuweisungen, Grenzwertfestsetzungen etc. bleiben erheblich hinter den komplexen Abwägungsentscheidungen zurück, zu denen der nationale Gesetzgeber im Rahmen der Öffnungsklauseln der Verordnung (EU) 2016/679 befugt bzw. verpflichtet ist (siehe z.B. das Gebot des Artikel 6 Absatz 3 der Verordnung, Rechtsgrundlagen der Verarbeitung überhaupt erst durch nationale Bestimmungen zu schaffen).

- Mit Erwägungsgrund 8 berücksichtigt der Unionsgesetzgeber den besonderen Charakter der Verordnung (EU) 2016/679. Er lässt Wiederholungen ausdrücklich zu, wenn sie (1) im sachlichen Zusammenhang mit Verordnungsbestimmungen stehen, die dem Mitgliedstaat die Möglichkeit nationaler Präzisierungen oder Einschränkungen einräumen, soweit dies erforderlich ist, um (2) Kohärenz zu wahren und (3) die nationalen Vorschriften für die Personen, für die sie gelten, verständlicher zu machen.

- Der nationale Gesetzgeber muss bis Mai 2018 das nationale Recht nicht nur an die Verordnung (EU) 2016/679 anpassen, sondern auch die Richtlinie (EU) 2016/680 umsetzen. Beide Unionsrechtsakte haben teils wortgleiche Regelungen (z. B. Begriffsbestimmungen nach Artikel 4 der Verordnung (EU) 2016/679 bzw. Artikel 3 der Richtlinie (EU) 2016/680); darauf war bei den Verhandlungen aus Kohärenzgründen geachtet worden. Zudem bestehen strukturelle Gemeinsamkeiten (z. B. bezüglich der Ausgestaltung der Rolle des Datenschutzbeauftragten und der Aufsichtsbehörden).

- Die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 sind nicht in allgemein gesetzlicher Form trennscharf auseinanderzuhalten. Es ist im Einzelfall auslegungsfähig, ob eine Behörde Daten zu in der Verordnung oder der Richtlinie geregelten Zwecken verarbeitet. Die von der Aufteilung der Datenschutzreform in zwei Rechtsakte nahegelegte Trennung der Anforderungen an die Datenverarbeitung sowohl in formaler (beteiligte Behörden) als auch materieller Hinsicht (Annahme, dass Behörden entweder nur zu Verordnungs- oder nur zu Richtlinienzwecken Daten verarbeiten) entspricht nicht der Praxis. In Deutschland gibt es verschiedene Behörden, die zur Ausübung ihrer gesetzlichen Aufgaben sowohl Zwecke nach der Verordnung als auch der Richtlinie verfolgen. Dies erkennt Erwägungsgrund 19 der Verordnung (EU) 2016/679 ausdrücklich an. Dabei sind die Mitgliedstaaten gehalten, ihrer administrativen, ver-

fassungsmäßigen und organisatorischen Struktur Rechnung zu tragen Dies wiederum muss Wege für ein kohärentes, anwender- und betroffenenfreundliches nationales Recht eröffnen.

- Es gibt kein unionsrechtliches Gebot, einen Unionsrechtsakt in einem einzigen nationalen Gesetz umzusetzen bzw. ihn dort anzupassen. D. h. es ist sowohl möglich, einen Rechtsakt mit verschiedenen Gesetzen als auch mehrere Rechtsakte mit einem nationalen Gesetz zu erfassen.
- Es besteht darüber hinaus im Interesse eines kohärenten und anwenderfreundlichen nationalen Datenschutzrechts ein Bedürfnis, mit einem und demselben Gesetzentwurf auch die Rechtsbereiche zu regeln, die außerhalb des Unionsrechts liegen und daher weder der Verordnung (EU) 2016/679 noch der Richtlinie (EU) 2016/680 unterfallen. So ist etwa allein der nationale Gesetzgeber regelungsbefugt für den Bereich der nationalen Sicherheit, insbesondere für die Nachrichtendienste (Artikel 4 Absatz 2 Satz 3 des Vertrages über die Europäischen Union (EUV); in diesem Sinne auch Artikel 2 Absatz 2 Buchstabe a i. V. m. Erwägungsgrund 16 der Verordnung (EU) 2016/679; Artikel 2 Absatz 3 Buchstabe a i. V. m. Erwägungsgrund 14 der Richtlinie (EU) 2016/680).

Bereits aufgrund dieser Ausgangslage bestehen triftige Gründe, das Ausmaß des sog. Wiederholungsverbots auf die vorliegende Anpassungs- und Umsetzungsgesetzgebung den oben genannten Aspekten entsprechend angemessen zu beurteilen und anzuwenden.

Über diese Ausgangslage hinaus ist zu berücksichtigen, dass der EuGH auch bisher schon Ausnahmen vom Wiederholungsverbot für rechtmäßig erachtet hat. So hat der EuGH zunächst anerkannt, dass manche Bestimmungen einer Verordnung zu ihrer Durchführung des Erlasses von Durchführungsmaßnahmen durch die Mitgliedstaaten bedürfen, wobei ihnen ein weiter Ermessensspielraum zustehe (EuGH, Rs. C-403/98, Monte Arcosu, Rn. 26, 28). Auch räumt der EuGH dem nationalen Gesetzgeber seit langem ein, eine zersplitterte Rechtslage ausnahmsweise durch den Erlass eines zusammenhängenden Gesetzeswerks zu bereinigen und hierbei im Interesse eines inneren Zusammenhangs und der Verständlichkeit für den Adressaten notwendige punktuelle Normwiederholungen vorzunehmen (EuGH, Rs. C-272/83, Kommission/Italien, Rn. 27). Denn die Mitgliedstaaten haben allgemein durch geeignete innerstaatliche Maßnahmen die uneingeschränkte Anwendbarkeit einer Verordnung sicherzustellen (EuGH, Rs. C-72/85 Kommission/Niederlande, LS 2). Hierzu müssen die Mitgliedstaaten nicht nur ihr eigenes Recht anpassen bzw. bereinigen, sondern darüber hinaus eine so bestimmte, klare und transparente Lage schaffen, dass der Einzelne seine Rechte in vollem Umfang erkennen und sich vor den nationalen Gerichten darauf berufen kann (EuGH, Rs. C-162/99, Kommission/Italien, LS 3). Dies verdeutlicht, dass der Gerichtshof in seiner Rechtsprechung atypische Konstellationen berücksichtigt und Aspekten wie Verständlichkeit und Kohärenz Bedeutung beimisst.

Es ist daher im Interesse der Kohärenz des Datenschutzrechts sowie der Erhöhung der Verständlichkeit und Übersichtlichkeit für den Rechtsanwender mit dem Unionsrecht vereinbar und zweckmäßig, dass dieser Gesetzentwurf Wiederholungen einzelner Passagen bzw. Bestimmungen der Verordnung (EU) 2016/679 oder Verweisungen auf sie enthält. Dies betrifft sowohl die Ausgestaltung der eingeräumten Öffnungsklauseln als auch die in einem Allgemeinen Teil (Teil 1 „Allgemeine Bestimmungen“) zusammengefassten gemeinsamen Schnittmengen aus den Bereichen der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und dem nicht unionsrechtlich geregelten Bereich. Durch diesen integrativen Ansatz des Gesetzentwurfs wird dem mit dem EU-Datenschutzpaket verbundenen Harmonisierungsziel in besonderer Weise und über das reine Soll hinaus Rechnung getragen.

VI. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Der Entwurf sieht keine Rechts- und Verwaltungsvereinfachung vor.

2. Nachhaltigkeitsaspekte

Die Managementregeln und Indikatoren der Nationalen Nachhaltigkeitsstrategie wurden geprüft und, soweit einschlägig, beachtet.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

4. Erfüllungsaufwand

Die gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31) bereits bestehenden Betroffenenrechte, wie etwa Informations- und Auskunftsrechte gegenüber der betroffenen Person, das Recht auf Berichtigung und Löschung, das Recht auf Einschränkung der Verarbeitung sowie das Widerspruchsrecht, werden durch die Verordnung (EU) 2016/679 gestärkt. Dadurch entsteht zusätzlicher Erfüllungsaufwand für die Bürgerinnen und Bürger, die Wirtschaft und die Verwaltung, der aber durch die Verordnung (EU) 2016/679 und nicht dieses Gesetz verursacht wird.

Das neu gefasste Bundesdatenschutzgesetz schränkt zugleich in dem durch Artikel 23 der Verordnung (EU) 2016/679 eröffneten Rahmen einzelne Betroffenenrechte ein. Dies führt bei den Unternehmen zu einer Reduzierung von Pflichten und einer Verringerung des Erfüllungsaufwandes. Die im Bundesdatenschutz zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen als Ausgleich für die Einschränkung der Betroffenenrechte von dem Verantwortlichen zu ergreifenden Schutzmaßnahmen, wie etwa das Nachholen einer Informationspflicht oder die Dokumentation, aus welchen Gründen von einer Information abgesehen wird, löst unmittelbaren Erfüllungsaufwand aus. Ohne diese beiden zusammenhängenden Maßnahmen wäre der durch die Verordnung (EU) 2016/679 auslöste Aufwand für die Wirtschaft deutlich höher.

Für Bürgerinnen und Bürger entsteht kein neuer Erfüllungsaufwand.

Das Gesetz verpflichtet die Wirtschaft im Rahmen der Verarbeitung personenbezogener Daten Maßnahmen zum Schutz der betroffenen Person in den Fällen zu ergreifen, in denen sie davon absehen wollen, die betroffene Person nach Artikel 13 und 14 der Verordnung (EU) 2016/679 zu informieren. Dazu gehört etwa das Nachholen der Informationspflicht durch Bereitstellen der Information auf einer allgemein zugänglichen Webseite. Darüber hinaus hat der Verantwortliche zu dokumentieren, aus welchen Gründen von einer Information abgesehen werden soll.

Durch diese Maßnahmen entstehen für die Wirtschaft jährliche Bürokratiekosten aus Informationspflichten in Höhe von rund 17,2 Millionen Euro. Darüber hinaus fällt einmaliger Erfüllungsaufwand in Höhe von rund 58,9 Millionen Euro an.

Bürokratiekosten aus Informationspflichten für die Wirtschaft

Vorgabe	Paragraf/ Gesetz/Artikel	Art der Vorgabe	Fallzahl jährlich/einmalig	Zeitaufwand pro Fall in Min.	Lohnsatz in €/h	Summe jährl. Erfüllungsaufwand in €	Summe einm. Erfüllungsaufwand in €
Unterbleibt eine Information nach Art. 13 DS-GVO, sind geeignete Maßnahmen zum Schutz der Rechte, Freiheiten und Interessen der betroffenen Personen zu ergreifen	§ 32 Abs. 2 BDSG (Artikel 1)	IP	217.780/ 1.088.900	10	30,90	1.065.489	5.327.443

Vorgabe	Paragraf/ Gesetz/Artikel	Art der Vorgabe	Fallzahl jährlich/einmalig	Zeitaufwand pro Fall in Min.	Lohnsatz in €/h	Summe jährl. Erfüllungsaufwand in €	Summe einm. Erfüllungsaufwand in €
Dokumentation, wann von der Information nach Art. 13, 14 DS-GVO abgesehen werden kann	§§ 32 Abs. 2, 33 Abs. 2 BDSG (Artikel 1)	IP	255.000/ 2.700.000	75	47,30	15.076.875	48.285.909
Unterbleibt eine Information nach Art. 14 DS-GVO, sind geeignete Maßnahmen zum Schutz der Rechte, Freiheiten und Interessen der betroffenen Personen zu ergreifen	§ 33 Abs. 2 BDSG (Artikel 1)	IP	217.780/ 1.088.900	10	30,90	1.065.489	5.327.443
Summe						**17.207.853**	**58.940.795**

Im Einzelplan 21 der Bundesbeauftragten für Datenschutz und Informationsfreiheit entstehen Mehrausgaben insbesondere durch die Wahrnehmung der Funktion des gemeinsamen Vertreters im Europäischen Datenschutzausschuss nach Artikel 68 der Verordnung (EU) 2016/679 (§ 17 BDSG) sowie durch die bei der Bundesbeauftragten für Datenschutz und Informationsfreiheit angesiedelte Einrichtung der zentralen Anlaufstelle aufgrund Artikel 51 Absatz 2 i. V. m. Erwägungsgrund 119 der Verordnung (EU) 2016/679 (§ 17 BDSG). Dies konnte im Haushalt 2017 nicht berücksichtigt werden, weil der Gesetzentwurf bei Verabschiedung des Haushalts noch nicht etatreif war. Nach Schätzung der Bundesbeauftragten für Datenschutz und Informationsfreiheit werden hierfür 10 Stellen benötigt. Für die Verwaltung des Bundes entstünde damit insgesamt jährlicher Erfüllungsaufwand in Höhe von rund 940.000 Euro sowie einmalige Umsetzungskosten in Höhe von rund 74.000 Euro.

Erfüllungsaufwand für die Verwaltung des Bundes (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)

Vorgabe	Paragraf/ Gesetz/Artikel	Vollzug	Fallzahl jährlich/einmalig	Zeitaufwand pro Fall in Min.	Lohnsatz in €/h	Summe jährl. Erfüllungsaufwand in €	Summe einm. Erfüllungsaufwand in €
Warnung des für die Verarbeitung Verantwortlichen durch den BfDI bei Verdacht auf Verstöße gegen das BDSG	§ 16 Abs. 2 BDSG (Artikel 1)	Bund	100/0	301	35,70	23.898	0

Vorgabe	Paragraf/ Gesetz/Artikel	Vollzug	Fallzahl jährlich/einmalig	Zeitaufwand pro Fall in Min.	Lohnsatz in €/h	Summe jährl. Erfüllungsaufwand in €	Summe einm. Erfüllungsaufwand in €
Tätigkeit als gemeinsamer Vertreter im Europäischen Datenschutzausschuss sowie zentrale Anlaufstelle	§ 17 Abs. 1 BDSG (Artikel 1)	Bund	1/0	960.000 (10 Stellen)	45,09	912.440	0
Dokumentation, wann von der Information nach Art. 13, 14 DS-GVO abgesehen werden kann	§§ 33 Abs. 2, 33 Abs. 2 BDSG (Artikel 1)	Bund	308/0	75	57,80	0	26.849
Akkreditierung der Zertifizierungsstellen durch die Aufsichtsbehörden	§ 39 BDSG (Artikel 1)	Bund	1/17	2.400	57,80	2.790	47.422
Summe						**939.128**	**74.271**

Weiterer neuer Erfüllungsaufwand entsteht für die Verwaltung nicht. Die bestehenden allgemeinen wie bereichsspezifischen Regelungen im Datenschutzrecht, die öffentliche Stellen betreffen, können durch Ausnutzung der in der Verordnung (EU) 2016/679 enthaltenen Öffnungsklauseln fortbestehen.

Die im neu gefassten Bundesdatenschutzgesetz zur Umsetzung der Richtlinie (EU) 2016/680 geschaffenen Regelungen schaffen in Teilen gegenüber dem bestehenden Recht und der bestehenden Verwaltungspraxis neue Pflichten für die Verwaltung. Davon betroffen sind im Bereich des Bundes das Zollkriminalamt, die Zollverwaltung, die Bundespolizei, das Bundeskriminalamt, der Generalbundesanwalt und die Bundesgerichte. Diesen Pflichten steht nach derzeitiger Schätzung ein jährlicher Erfüllungsaufwand in Höhe von rund 562.000 Euro sowie einmalige Umsetzungskosten in Höhe von rund 60.000 Euro gegenüber. Die große Mehrzahl der im neu gefassten Bundesdatenschutzgesetz enthaltenen Pflichten für die Verwaltung sind bereits im geltenden Bundesdatenschutzgesetz – ggf. in Verbindung mit dem für die jeweilige Behörde maßgeblichen Fachrecht – und in der Verwaltungspraxis abgebildet. Der jährliche Erfüllungsaufwand wird ausgelöst durch Anforderungen an die Durchführung von Datenschutzfolgenabschätzungen nach § 63 BDSG (jährlich: 510.000 Euro). Bei diesem Kostenansatz ist zu berücksichtigen, dass bereits bestehende und zukünftig wegfallende Pflichten zur Erstellung und Abstimmung von Errichtungsanordnungen sowie zur Vorabkontrolle durch den behördlichen Datenschutzbeauftragten und der damit zusammenhängende Aufwand in der neuen Datenschutzfolgenabschätzung weitgehend aufgehen wird. Darüber hinaus fällt jährlicher Erfüllungsaufwand an durch die Einholung einer Genehmigung der zuvor an die jeweilige deutsche Stelle übermittelnden Stelle in einem anderen EU-Mitgliedstaat, bevor diese zuvor übermittelten Daten an einen Drittstaat weiterübermittelt werden – § 73 Absatz 3 BDSG (jährlich: 33.000 Euro) und durch den zusätzlichen Aufwand der Bundesbeauftragten für Datenschutz und Informationsfreiheit, wenn diese Datenschutzbehörden in anderen EU-Staaten Amtshilfe nach § 79 BDSG leistet und hierzu maßgebliche Informationen übermittelt und Auskunftsersuchen nachkommt (jährlicher Erfüllungsaufwand: rd. 19.000 Euro).

Zusätzlich entsteht einmaliger Erfüllungsaufwand für die Verwaltung in Höhe von rd. 60.000 Euro für Softwareanpassungen zur Protokollierung von Datenverarbeitungen in automatisierten Verarbeitungssystemen nach § 73 BDSG.

Etwaiger Mehrbedarf an Sach- und Personalmitteln soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

Für die Länder entstehen Mehrausgaben durch die die Tätigkeit als Stellvertreter des gemeinsamen Vertreters im Europäischen Datenschutzausschuss (§ 17 BDSG), die mit schätzungsweise vier Stellen veranschlagt werden kann, und die Ausfüllung des Verfahrens der Zusammenarbeit der Aufsichtsbehörden des Bundes zur und der Länder zur Findung eines gemeinsamen Standpunktes (§ 18 BDSG), für die schätzungsweise in der Summe mindestens eine Stelle im höheren Dienst in jedem Land anzusetzen sein wird. Dadurch entsteht jährlicher Erfüllungsaufwand in Höhe von rund 1,98 Millionen Euro.

Erfüllungsaufwand der Verwaltung für Länder und Kommunen

Vorgabe	Paragraf/ Gesetz	Vollzug	Fallzahl jährlich/einmalig	Zeitaufwand pro Fall in Min.	Lohnsatz in €/h	Summe jährl. Erfüllungsaufwand in €	Summe einm. Erfüllungsaufwand in €
Tätigkeit als Stellvertreter des BfDI im Europäischen Datenschutz-ausschuss	§ 17 Abs. 1 BDSG (Artikel 1)	Land	1/0	192.000 (4 Stellen)	46,75	187.800	0
Informationsaustausch und gegenseitige Stellungnahmen zwischen den BfDI und den Aufsichtsbehörden der Länder zur Findung eines gemeinsamen Standpunktes	§ 18 BDSG (Artikel 1)	Land	16/0	96.000 (jeweils 1 Stelle)	58,10	1.792.960	0
Summe						**1.980.760**	

5. Weitere Kosten

Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

6. Weitere Gesetzesfolgen

Auswirkungen von gleichstellungspolitischer Bedeutung

Die Regelungen sind inhaltlich geschlechtsneutral. Auswirkungen von gleichstellungspolitischer Bedeutung sind nicht zu erwarten.

7. Demografie-Check

Das Vorhaben führt nicht zu finanziellen Belastungen für künftige Generationen.

VII. Befristung; Evaluierung

Eine Befristung des Gesetzes ist nicht vorgesehen, weil auch die korrespondierenden EU-Rechtsakte nicht zeitlich befristet sind. Das Regelungsvorhaben wird spätestens drei Jahre nach dem Inkrafttreten evaluiert.

B. Besonderer Teil

Zu Artikel 1 (Bundesdatenschutzgesetz)

Zu § 1 (Anwendungsbereich des Gesetzes)

Die Vorschrift bestimmt den Anwendungsbereich des Gesetzes.

Nach Absatz 1 Satz 1 gilt das Gesetz, wie bisher auch das Bundesdatenschutzgesetz in der bisher geltenden Fassung (BDSG a. F.), für jede Form der Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes sowie durch öffentliche Stellen der Länder. Es hat also, wie bisher auch, einen weiteren Anwendungsbereich als die Verordnung (EU) 2016/679.

Für nichtöffentliche Stellen gilt das BDSG nach Absatz 1 Satz 2 im Rahmen des sachlichen Anwendungsbereichs der Verordnung (EU) 2016/679. Wer öffentliche Stelle des Bundes und der Länder und wer nichtöffentliche Stelle ist, ergibt sich aus § 2 Absatz 1 bis 4 BDSG.

Für die Verarbeitung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken fand das BDSG a. F. nach dem sogenannten Presseprivileg des § 41 Absatz 1 BDSG a. F. nur sehr eingeschränkt Anwendung. Für das Pressewesen sind nunmehr ausschließlich die Länder zuständig. Aus kompetenzrechtlichen Gründen kann § 41 Absatz 1 BDSG a. F. daher nicht beibehalten werden. Der Bundesgesetzgeber geht aber davon aus, dass die insofern zuständigen Landesgesetzgeber das Presseprivileg wie bisher absichern werden.

Soweit die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten öffentlicher Stellen des Bundes erfolgt, die weder vom Anwendungsbereich der Verordnung (EU) 2016/679 noch von der Richtlinie (EU) 680/2016 erfasst sind richtet sich das anzuwendende Datenschutzrecht allein nach nationalen Regelungen. So besitzt die Europäische Union etwa gemäß Artikel 4 Absatz 2 Satz 3 des Vertrages über die Europäischen Union (EUV) keine Regelungskompetenz für den Bereich der nationalen Sicherheit. Dies betrifft die Datenverarbeitung durch das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst, den Militärischen Abschirmdienst sowie den Bereich des Sicherheitsüberprüfungsgesetzes. Dies ist auch sekundärrechtlich klargestellt, Artikel 2 Absatz 2 Buchstabe a i. V. m. Erwägungsgrund 16 der Verordnung (EU) 2016/679; Artikel 2 Absatz 3 Buchstabe a i. V. m. Erwägungsgrund 14 der Richtlinie (EU) 2016/680. Das neu gefasste Bundesdatenschutzgesetz (BDSG) gibt für diese Bereiche außerhalb des Rechts der Europäischen Union allgemeine Regelungen vor. Soweit in bereichsspezifischen Gesetzen, wie etwa im Bundesverfassungsschutzgesetz, im Bundesnachrichtendienstgesetz, im Gesetz über den Militärischen Abwehrdienst oder im Sicherheitsüberprüfungsgesetz abweichende Regelungen getroffen werden, gehen sie gemäß § 1 Absatz 2 den Vorschriften des BDSG vor.

Absatz 2 Satz 1 bestimmt das Verhältnis dieses Gesetzes zu spezifischen datenschutzrechtlichen Vorschriften. Dieses Gesetz hat den Charakter eines „Auffanggesetzes“. Spezifische Rechtsvorschriften des Bundes genießen gegenüber den Vorschriften des BDSG grundsätzlich Vorrang. Dies wird durch die Formulierung in Satz 1 ausdrücklich klargestellt. Durch Satz 2 wird zusätzlich klargestellt, dass die jeweilige bereichsspezifische Spezialregelung nur vorrangig ist, wenn eine Tatbestandskongruenz vorliegt. Sie beurteilt sich im Einzelfall nach den Tatbeständen des jeweiligen bereichsspezifischen Gesetzes (für einen Vergleich heranzuziehen sind danach etwa der Sachverhalt „Datenverarbeitung“, ggf. in den jeweiligen Verarbeitungsphasen, oder bezogen auf sog. Individual- oder Betroffenenrechte der Sachverhalt „Informationspflicht“, „Auskunftsrecht“, „Widerspruchsrecht“). Dies gilt unabhängig davon, ob in der tatbestandskongruenten Vorschrift eine im Vergleich zum BDSG weitergehende oder engere gesetzliche Regelung getroffen ist. Liegt allerdings keine bereichsspezifische Datenschutzregelung für einen vergleichbaren Sachverhalt vor, so übernimmt das BDSG seine lückenfüllende Auffangfunktion. Auch eine nicht abschließende (teilweise) Regelung oder das Schweigen eines bereichsspezifischen Gesetzes führt dazu, dass subsidiär auf die Vorschriften des BDSG zurückgegriffen werden kann. Bedeutsam ist dies insbesondere mit Blick auf die in Teil 2 Kapitel 2 des BDSG vorgenommenen Einschränkungen der Betroffenenrechte. Auf diese Regelungen kann als Auffangregelung zurückgegriffen werden, sofern im bereichsspezifischen Recht keine tatbestandskongruente Regelung vorgehalten ist. Dies gilt allerdings nicht, wenn spezifische Regelungen für einen bestimmten Bereich insgesamt umfassend und damit abschließend die Datenverarbeitung regeln und somit für das BDSG kein Anwendungsbereich verbleibt. Das ist z. B. für den im SGB X in Verbindung mit dem

SGB I sowie in den übrigen Sozialgesetzbüchern geregelten Schutz von Sozialdaten oder etwa im Bereich der Abgabenordnung der Fall.

Absatz 2 Satz 2 entspricht der bisherigen Regelung des § 1 Absatz 3 Satz 2 BDSG a. F.

Absatz 3 entspricht der bisherigen Regelung des § 1 Absatz 4 BDSG a. F.

Nach Absatz 4 Satz 1 Nummer 1 findet das Gesetz auf Datenverarbeitung im Inland Anwendung. Absatz 4 Satz 1 Nummer 2 bestimmt, dass die Vorschriften des BDSG nur dann zur Anwendung kommen, wenn eine Datenverarbeitung durch eine in Deutschland ansässige Niederlassung vorliegt. Dies entspricht dem Harmonisierungsgedanken der Verordnung (EU) 2016/679. Absatz 4 Satz 1 Nummer 3 entspricht § 1 Absatz 5 Satz 2 BDSG a. F.

Absatz 5 berücksichtigt, dass der Verordnung (EU) 2016/679 im Rahmen ihres Anwendungsbereichs unmittelbare Geltung im Sinne des Artikels 288 Absatz 2 AEUV zukommt. Insoweit in diesem Kapitel punktuelle Wiederholungen von sowie Verweise auf Bestimmungen aus der Verordnung (EU) 2016/679 erfolgen, so geschieht dies aus Gründen der Verständlichkeit und Kohärenz und lässt die unmittelbare Geltung der Verordnung (EU) 2016/679 unberührt. Dies wird hiermit an herausgehobener Stelle klargestellt. Die punktuellen Wiederholungen und Verweise im BDSG sind außerdem dem komplexen Mehrebenensystem geschuldet, das sich aus dem Zusammenspiel zwischen der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 sowie dem nationalen allgemeinen und fachspezifischen Recht ergibt. In einem solchen hat es der EuGH dem nationalen Gesetzgeber eingeräumt, im Interesse eines inneren Zusammenhangs und der Verständlichkeit für den Adressaten notwendige punktuelle Normwiederholungen vorzunehmen (EuGH, Rs. C-272/83, Kommission/Italien, Rn. 27). Für den Bereich der Richtlinie (EU) 2016/680 sind damit einhergehende strengere Vorgaben möglich. Dies stellt ausdrücklich Erwägungsgrund 15 klar, wonach die Mitgliedstaaten nicht daran gehindert werden, zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden Garantien festzulegen, die strenger sind als die Garantien dieser Richtlinie. Durch den integrativen Ansatz, gemeinsame Bestimmungen „vor die Klammer“ zu ziehen, trägt der Gesetzgeber diesem hier besonderen Umstand Rechnung und mindert die Herausforderungen für den Rechtsanwender soweit europarechtlich vertretbar unter gleichzeitiger normökonomischer Entlastung des Fachrechts.

Die Absätze 6 und 7 dienen der Klarstellung, welche Staaten den Mitgliedstaaten der Europäischen Union gleich gestellt sind.

Absatz 8 bestimmt, dass für Verarbeitungen personenbezogener Daten im Rahmen von Tätigkeiten, die weder dem Anwendungsbereich der Verordnung (EU) 2016/679 noch der Richtlinie (EU) 2016/680 unterfallen, die Verordnung (EU) 2016/679 und Teil 1 und Teil 2 des BDSG Anwendung finden. Die Regelung gilt nur für öffentliche Stellen, denn nach § 1 Absatz 1 Satz 1 BDSG beschränkt sich der Geltungsbereich dieses Gesetzes nicht nur auf den sachlichen Anwendungsbereich der Verordnung (EU) 2016/679. Absatz 8 stellt sicher, dass auch für die nicht unter die beiden EU-Rechtsakte fallenden Bereiche entsprechend der bisherigen Regelungssystematik des BDSG a. F. ein datenschutzrechtliches Vollregime im Geltungsbereich des Grundgesetzes angeboten wird. Die besondere Erwähnung der Anwendbarkeit des Teils 1 BDSG erfolgt lediglich aus Gründen der Klarstellung, da die Anwendbarkeit sich bereits aus Absatz 1 Satz 1 unmittelbar ergibt.

Zu § 2 (Begriffsbestimmungen)

Die Absätze 1 bis 4 der Regelung entsprechen § 2 BDSG a. F. Sie bestimmen, welche öffentlichen Stellen und nichtöffentlichen Stellen unter den Anwendungsbereich nach § 1 Absatz 1 BDSG fallen.

Absatz 5 vollzieht den Regelungsgehalt des § 27 Absatz 1 Satz 1 Nummer 2 BDSG a. F. nach, indem bestimmt wird, dass öffentliche Stellen des Bundes und öffentliche Stellen der Länder dann als nichtöffentliche Stellen im Sinne dieses Gesetzes gelten, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, und – im Fall öffentlicher Stellen der Länder – zudem Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist. Er dient damit auch der Klarstellung, auf welche Verarbeitungsbefugnisse bzw. Ausnahmen von Betroffenenrechte abzustellen ist, wenn eine Unterscheidung nach öffentlichen und nichtöffentlichen Stellen vorgenommen wird.

Zu § 3 (Verarbeitung personenbezogener Daten durch öffentliche Stellen)

Die Vorschrift enthält eine allgemeine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen.

Durch die Stellung im Teil 1 „Gemeinsame Bestimmungen“ dieses Gesetzes können Verantwortliche vorbehaltlich anderer bereichsspezifischer Regelungen auf die Regelung unabhängig davon zurückgreifen, zu welchen Zwecken die Datenverarbeitung erfolgt.

Wer zu dem Kreis der öffentlichen Stellen gehört, wird in § 2 Absatz 1 bis 3 BDSG bestimmt. Soweit nichtöffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen (sog. Beliehene), gelten sie nach § 2 Absatz 4 Satz 2 BDSG als öffentliche Stellen und können ihre Datenverarbeitung daher ebenfalls auf die Befugnis in § 3 BDSG stützen.

Soweit die Vorschrift für Datenverarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679 zur Anwendung kommt, wird mit ihr eine Rechtsgrundlage auf der Grundlage von Artikel 6 Absatz 1 Buchstabe e i. V. m. Artikel 6 Absatz 3 Satz 1 der Verordnung (EU) 2016/679 geschaffen. Dies ist rechtlich notwendig, da Artikel 6 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 selbst keine Rechtsgrundlage für die Verarbeitung von Daten schafft, was sich aus der Formulierung in Artikel 6 Absatz 3 Satz 1 der Verordnung (EU) 2016/679 ergibt. Der Unions- oder der nationale Gesetzgeber hat eine Rechtsgrundlage zu setzen. Diesem Regelungsauftrag kommt der deutsche Gesetzeber an dieser Stelle nach.

Die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist nach der Vorschrift zulässig, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder wenn sie in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Beides kann sich sowohl aus nationalen Rechtvorschriften als auch aus EU-Vorgaben ergeben. Die Verarbeitung personenbezogener Daten ist allerdings nicht nur auf dieser Rechtsgrundlage zulässig ist, sondern auch auf der Grundlage der weiteren in Artikel 6 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Erlaubnistatbestände einschließlich der auf der Grundlage der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 erlassenen bereichsspezifischen Regelungen. So ist etwa die Zulässigkeit der Verarbeitung von Sozialdaten abschließend im SGB X in Verbindung mit dem SGB I sowie in den übrigen Sozialgesetzbüchern geregelt.

Die Regelung nimmt den bisher in §§ 13 Absatz 1 und 14 Absatz 1 BDSG a. F. enthaltenen Regelungsgehalt auf, unterscheidet aber nicht mehr zwischen den Phasen der Erhebung, Speicherung, Veränderung und Nutzung, sondern verwendet, dem Grundgedanken der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 folgend, allgemein den umfassenden Begriff der Verarbeitung. Wie nach geltendem Recht enthält § 3 eine subsidiäre, allgemeine Rechtsgrundlage für Datenverarbeitungen mit geringer Eingriffsintensität in die Rechte der betroffenen Person.

Zu § 4 (Videoüberwachung öffentlich zugänglicher Räume)

Die Vorschrift enthält eine § 6b BDSG a. F. weitgehend entsprechende Regelung zur Videoüberwachung in öffentlich zugänglichen Räumen unter Beibehaltung des Stufenverhältnisses der Beobachtung (Absatz 1) sowie der Speicherung oder Verwendung (Absatz 3) sowie der Kennzeichnungs-, Informations- und Löschungspflichten (Absatz 2, 4 und 5). Der Gebrauch des Begriffs „Verwendung“ in Absatz 3 statt – wie bisher im BDSG a. F. – „Nutzung“ entspricht einem Unterbegriff des unionsrechtlichen Verarbeitungsbegriffs des Artikels 4 Nummer 2 der Verordnung (EU) 2016/679, ohne dass damit ein Bedeutungsunterschied verbunden ist.

Absatz 1 Satz 2 schreibt die bisherige Regelung des § 6b Absatz 1 Satz 2 BDSG a. F. fort, die mit dem Entwurf eines Videoüberwachungsverbesserungsgesetzes in das BDSG a. F. aufgenommen werden soll. Soweit der Betreiber eine Videoüberwachung einsetzen möchte und die Schutzgüter Leben, Gesundheit oder Freiheit in den dort genannten Anlagen betroffen sein können, wird durch die Formulierung „gilt als…ein besonders wichtiges Interesse“ die Abwägungsentscheidung zugunsten der Zulässigkeit des Einsatzes einer Videoüberwachungsmaßnahme geprägt.

Zu §§ 5 bis 7 (Kapitel 3 – Datenschutzbeauftragte öffentlicher Stellen)

Kapitel 3 enthält Vorschriften für die Benennung, die Stellung und die Aufgaben der Datenschutzbeauftragten öffentlicher Stellen des Bundes. Die Rechtsstellung der behördlichen Datenschutzbeauftragten in der Bundesverwaltung sollte im Anwendungsbereich der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und für die Bereiche außerhalb des Unionsrechts (z. B. für die Nachrichtendienste) einheitlich ausgestaltet sein.

Zu § 5 (Benennung)

In Umsetzung des Artikels 32 Absatz 1 der Richtlinie (EU) 2016/680 erfolgt in Absatz 1 eine Übernahme des Artikels 37 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679.

Die Absätze 2, 3 und 5 setzen Artikel 32 Absatz 2 bis 4 der Richtlinie (EU) 2016/680 um. Sie entsprechen Artikel 37 Absatz 3, 5 und 7 der Verordnung (EU) 2016/679.

Absatz 4 überträgt die Regelung des Artikels 37 Absatz 6 der Verordnung (EU) 2016/679, nach welcher sowohl interne als auch externe Datenschutzbeauftragte zulässig sind, auf den gesamten Bereich der Bundesverwaltung. Dies geht über die Vorgaben der Richtlinie (EU) 2016/680 hinaus.

Zu § 6 (Stellung)

Die Absätze 1 und 2 setzen Artikel 33 der Richtlinie (EU) 2016/680 um. Sie entsprechen Artikel 38 Absatz 1 und 2 der Verordnung (EU) 2016/679.

Die Absätze 3 und 5 Satz 1 übertragen die Vorgaben des Artikels 38 Absatz 3 und 4 der Verordnung (EU) 2016/679 auf alle öffentlichen Stellen des Bundes, unabhängig davon, zu welchem Zweck die Datenverarbeitung erfolgt. Dies geht über die Vorgaben der Richtlinie (EU) 2016/680 hinaus. Durch die Erstreckung der Vorgaben der Verordnung (EU) 2016/679 auf den Anwendungsbereich der Richtlinie (EU) 2016/680 und der Datenverarbeitung zu Zwecken, für die der Anwendungsbereich des Rechts der Europäischen Union nicht eröffnet ist (z. B. Nachrichtendienste), wird die Rechtsstellung der oder des behördlichen Datenschutzbeauftragten in öffentlichen Stellen des Bundes einheitlich ausgestaltet.

Absatz 4 entspricht der bisherigen Regelung des § 4f Absatz 3 Satz 4 bis 6 BDSG a. F. Bei dem besonderen Abberufungs- und Kündigungsschutz der oder des Datenschutzbeauftragten handelt es sich um eine arbeitsrechtliche Regelung, die ergänzend zu den Vorgaben der Verordnung (EU) 2016/679 beibehalten werden kann.

Die Regelung zur Verschwiegenheitspflicht in Absatz 5 Satz 2 entspricht § 4f Absatz 4 BDSG a. F. Die Verletzung von Privatgeheimnissen durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten ist gemäß § 203 Absatz 2a des Strafgesetzbuches zudem strafbewehrt. Das Zeugnisverweigerungsrecht in Absatz 6 sichert die Verschwiegenheitspflicht ab und entspricht § 4f Absatz 4a BDSG a. F. Die Regelungskompetenz für den Bereich der Verordnung (EU) 2016/679 folgt aus Artikel 38 Absatz 5 der Verordnung (EU) 2016/679. Die Regelung geht über die Vorgaben der Richtlinie (EU) 2016/680 hinaus und erfolgt zum Zweck einer kohärenten Rechtsstellung der oder des behördlichen Datenschutzbeauftragten in der gesamten Bundesverwaltung.

Zu § 7 (Aufgaben)

Absatz 1 Satz 1 setzt Artikel 34 der Richtlinie (EU) 2016/680 um. Um die Aufgaben der oder des Datenschutzbeauftragten öffentlicher Stellen für alle Verarbeitungszwecke einheitlich auszugestalten, entspricht die Norm unter lediglich redaktioneller Anpassung Artikel 39 der Verordnung (EU) 2016/679.

Absatz 1 Satz 2 stellt klar, dass die Aufgaben eines behördlichen Datenschutzbeauftragten eines Gerichtes sich nicht auf das Handeln des Gerichts im Rahmen seiner justiziellen Tätigkeit beziehen.

Absatz 2 stellt klar, dass die oder der behördliche Datenschutzbeauftragte weitere Aufgaben und Pflichten wahrnehmen kann, sofern diese nicht zu einem Interessenkonflikt führen. Die Regelung entspricht Artikel 38 Absatz 6 der Verordnung (EU) 2016/679, deren Regelungsgehalt auf den Anwendungsbereich der Richtlinie (EU) 2016/680 und der Datenverarbeitung außerhalb des Anwendungsbereichs des Rechts der Europäischen Union (z. B zu nachrichtendienstlichen Zwecken) erstreckt wird.

Absatz 3 entspricht Artikel 39 Absatz 2 der Verordnung (EU) 2016/679. Die Regelung hat keine Entsprechung in Artikel 34 der Richtlinie (EU) 2016/680, wird aber auch außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 als allgemeiner Grundsatz festgeschrieben.

Zu den §§ 8 bis 17 (Kapitel 4 – Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)

Kapitel 4 passt die Regelungen des BDSG a. F. zu der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (die oder der Bundesbeauftragte) an die Vorgaben der Verordnung (EU) 2016/679 an. Zugleich werden die Vorgaben der Richtlinie (EU) 2016/680 umgesetzt.

Die Regelungen der §§ 21 bis 26 BDSG a. F. werden inhaltlich weitgehend übernommen, aus Gründen der Lesbarkeit allerdings neu strukturiert unter Orientierung an dem Aufbau der Kapitel VI der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680. Im Einzelnen geregelt werden die Errichtung, die Zuständigkeit, die

Unabhängigkeit, die Ernennung und Amtszeit, das Amtsverhältnis, die Rechte und Pflichten, die Aufgaben und Befugnisse der oder des Bundesbeauftragten. Die Bundeskompetenz ergibt sich aus der Natur der Sache.

Zu § 8 (Errichtung)

§ 8 Absatz 1 und 2 regelt in unveränderter Übernahme des bisherigen § 22 Absatz 5 BDSG a. F. die Errichtung und Einrichtung der oder des Bundesbeauftragten und die näheren Modalitäten. Hierdurch werden Artikel 54 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstabe a der Richtlinie (EU) 2016/680 durchgeführt bzw. umgesetzt, welche den Mitgliedstaaten vorgeben, Aufsichtsbehörden zu errichten.

Die Errichtung der oder des Bundesbeauftragten als oberste Bundesbehörde (Absatz 1 Satz 1) steht im engen Zusammenhang mit dem Erfordernis der völligen Unabhängigkeit der oder des Bundesbeauftragten. Die völlige Unabhängigkeit und Weisungsfreiheit der Aufsichtsbehörden sind unionsrechtlich vorgegeben (Artikel 16 Absatz 2 AEUV, Artikel 52 der Verordnung (EU) 2016/679 bzw. Artikel 42 der Richtlinie (EU) 2016/680). Zugleich wird hierdurch die dienstrechtliche Personalhoheit der oder des Bundesbeauftragten über die Beschäftigten sichergestellt (Artikel 52 Absatz 5 der Verordnung (EU) 2016/679, Artikel 42 Absatz 5 der Richtlinie (EU) 2016/680).

Die Festlegung des Dienstsitzes (Absatz 1 Satz 2) und die körperschaftliche Zuweisung der bei der oder dem Bundesbeauftragten beschäftigten Beamtinnen und Beamten als solche des Bundes (Absatz 2) stehen in unmittelbarem Sachzusammenhang zu der Errichtung und Ausstattung der Aufsichtsbehörden.

Absatz 3 schafft eine Rechtsgrundlage für die Übertragung von Aufgaben der Personalverwaltung und Personalwirtschaft von der oder dem Bundesbeauftragten auf andere Behörden und die damit einhergehende Übermittlungsbefugnis für die Beschäftigtendaten. Die Regelung ist an § 108 Absatz 5 Satz 1 und 2 BBG angelehnt und erweitert diesen auf Aufgaben außerhalb der Beihilfebearbeitung. Hierdurch ist es der oder dem Bundesbeauftragten als oberster Bundesbehörde ohne eigenen Geschäftsbereich möglich, bestimmte Aufgaben der Personalverwaltung und Personalwirtschaft, bei denen aufgrund des selbständigen Charakters der Aufgabenerledigung das Instrument der Auftragsdatenverarbeitung nicht in Betracht kommt, durch andere Behörden im Wege der Funktionsübertragung ausführen zu lassen. Betroffen sind beispielsweise Aufgaben der Reisevorbereitung, Reisekostenabrechnung, Gewährung von Trennungsgeld und Umzugskostenerstattung, Geltendmachung von Schadensersatzansprüchen gegenüber Dritten oder Unterstützung bei Stellenbesetzungsverfahren.

Zu § 9 (Zuständigkeit)

Artikel 51 Absatz 1 der Verordnung (EU) 2016/679 und Artikel 41 Absatz 1 der Richtlinie (EU) 2016/680 überlassen es den Mitgliedstaaten, eine oder mehrere Aufsichtsbehörden für die Überwachung der Anwendung der Datenschutz-Grundverordnung und der Richtlinie (EU) 2016/680 einzurichten. Artikel 55 Absatz 1 der Verordnung (EU) 2016/679 bestimmt zudem, dass jede Aufsichtsbehörde für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit der Verordnung (EU) 2016/679 übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig ist. Eine vergleichbare Regelung enthält Artikel 45 Absatz 1 der Richtlinie (EU) 2016/680.

Die Bundesrepublik verfügt mit ihrem föderalen Staatsaufbau über Datenschutzaufsichtsbehörden auf Bundes- und auf Länderebene. Es ist daher auch innerhalb der Bundesrepublik eine Abgrenzung der Zuständigkeiten der Aufsichtsbehörden erforderlich.

Absatz 1 legt die sachliche Zuständigkeit der oder des Bundesbeauftragten fest. Die oder der Bundesbeauftragte ist zuständig für die datenschutzrechtliche Aufsicht über alle öffentlichen Stellen des Bundes, gleich ob die Datenverarbeitung unter den Anwendungsbereich des Unionsrechts fällt oder nicht. Hierzu wird der bisherige § 24 Absatz 1 BDSG a. F. ohne inhaltliche Änderungen sprachlich an die Verordnung (EU) 2016/679 angepasst. Auch Stellen des Bundes im Sinne des § 2 Absatz 5, die als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, unterfallen wie bisher (§ 27 Absatz 1 Satz 1 Nummer 2 Buchstabe a i. V. m. Satz 3 BDSG a. F.) der Zuständigkeit der oder des Bundesbeauftragten. Spezialgesetzliche Zuweisungen der Datenschutzaufsicht über nichtöffentliche Stellen an die Bundesbeauftragte oder den Bundesbeauftragten bleiben – wie bisher – von der Regelung unberührt. Satz 2 führt den bisherigen Verweis des § 11 Absatz 4 Nummer 1 b BDSG a. F. (nichtöffentliche Auftragnehmer in öffentlicher Hand) fort.

Die justizielle Tätigkeit der Bundesgerichte unterliegt – wie bisher nach § 24 Absatz 3 BDSG a. F. – nicht der Aufsicht durch die Bundesbeauftragte oder den Bundesbeauftragten. Absatz 2 passt die bisherige Regelung, nach

welcher die Bundesgerichte der Kontrolle der oder des Bundesbeauftragten nur unterliegen, soweit sie in Verwaltungsangelegenheiten tätig werden, an den Wortlaut der Verordnung (EU) 2016/679 bzw. der Richtlinie (EU) 2016/680 an. Hierdurch wird Artikel 45 Absatz 2 Satz 1 der Richtlinie (EU) 2016/680 umgesetzt; Artikel 55 Absatz 3 der Verordnung (EU) 2016/679 gilt hingegen unmittelbar. Auch bei anderen Einrichtungen mit verfassungsrechtlich garantierter Unabhängigkeit wie dem Bundesrechnungshof, soweit dessen Mitglieder im Rahmen ihrer richterlichen Unabhängigkeit handeln, sollte die oder der Bundesbeauftragte diese Unabhängigkeit achten und bei der Ausübung ihrer oder seiner Befugnisse wahren.

Zu § 10 (Unabhängigkeit)

Absatz 1 setzt Artikel 42 Absatz 1 und 2 der Richtlinie (EU) 2106/680 zur völligen Unabhängigkeit der oder des Bundesbeauftragten um. Hierzu wird der bisherige § 22 Absatz 4 Satz 2 BDSG a. F. an den Wortlaut der Artikel 42 Absatz 1 und 2 der Richtlinie (EU) 2016/680 angepasst. Für den Bereich der Verordnung (EU) 2016/679 gilt Artikel 52 Absatz 1 und 2 unmittelbar. Insoweit wird auch auf die Erläuterungen zu § 1 Absatz 5 verwiesen.

Absatz 2 trägt Artikel 52 Absatz 6, erster Satzteil der Verordnung (EU) 2016/679 und Artikel 42 Absatz 6, erster Satzteil der Richtlinie (EU) 2016/680 Rechnung. Jeder Mitgliedstaat hat sicherzustellen, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt. Wie aus Erwägungsgrund 118 der Verordnung (EU) 2016/679 folgt, bedeutet die Unabhängigkeit der Aufsichtsbehörden nicht, dass sie hinsichtlich ihrer Ausgaben keinem Kontroll- oder Überwachungsmechanismus unterworfen sind. Jedoch findet die Finanzkontrolle ihre Grenzen in der Unabhängigkeit der Datenschutzaufsicht. Die Haushalts- und Wirtschaftsführung der oder des Bundesbeauftragten unterliegt der Prüfung des Bundesrechnungshofs daher nur soweit hierdurch die Unabhängigkeit der oder des Bundesbeauftragten nicht beeinträchtigt wird.

Zu § 11 (Ernennung und Amtszeit)

§ 11 regelt in Durchführung der Artikel 53 Absatz 1, Artikel 54 Absatz 1 Buchstabe c und e der Verordnung (EU) 2016/679 sowie in Umsetzung der Artikel 43 Absatz 1, 44 Absatz 1 Buchstabe c und e der Richtlinie (EU) 2016/680 das Verfahren der Ernennung und die Amtszeit der oder des Bundesbeauftragten. Hierzu wird der bisherige § 22 Absatz 1 3 BDSG a. F. unverändert übernommen. Im Anschluss an die Regelung zum Mindestalter (§ 22 Absatz 1 Satz 2 BDSG a. F.) wird die Vorschrift in Absatz 1 Satz 4 und 5 um weitere Anforderungen an die Qualifikation und sonstige Voraussetzungen für die Ernennung der oder des Bundesbeauftragten ergänzt (Artikel 53 Absatz 2, 54 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 und Artikel 43 Absatz 2, 44 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/680).

Absatz 1 Satz 1 und 2 regelt das Verfahren der Wahl und Ernennung der oder des Bundesbeauftragten. Nach Artikel 53 Absatz 1 der Verordnung (EU) 2016/679 und Artikel 43 Absatz 1 der Richtlinie (EU) 2016/680 sehen die Mitgliedstaaten ein transparentes Ernennungsverfahren durch das Parlament, die Regierung, das Staatsoberhaupt oder eine unabhängige Stelle, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird, vor. Die Mitgliedstaaten haben zudem die Vorschriften und Verfahren für die Ernennung des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde zu schaffen (Artikel 54 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679, Artikel 44 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/680). Dem entspricht die bisherige Rechtslage in § 22 Absatz 1 Satz 1 und 3 BDSG a. F.

Mit Absatz 1 Satz 3 bis 5 werden in Durchführung des Artikels 53 Absatz 2, 54 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 und in Umsetzung des gleichlautenden Artikels 43 Absatz 2, 44 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/680 die Anforderungen an die Qualifikation und sonstigen Voraussetzungen für die Ernennung der oder des Bundesbeauftragten geregelt.

Das in Absatz 1 Satz 3 vorgesehene Mindestalter von 35 Jahren ist eine „sonstige“ Voraussetzung für die Ernennung im Sinne der vorbezeichneten Artikel. Die Regelung ist eine wortgleiche Übernahme des bisherigen § 22 Absatz 1 Satz 2 BDSG a. F. Absatz 1 Satz 4 setzt Artikel 43 Absatz 2 der Richtlinie (EU) 2016/680 um, nach welchem jedes Mitglied einer Aufsichtsbehörde über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen muss. Eine wortgleiche Regelung findet sich in Artikel 53 Absatz 2 der Verordnung (EU) 2016/679. Satz 5 konkretisiert die erforderlichen Qualifikationen der oder des Bundesbeauftragten, die oder der über durch einschlägige Berufserfahrung im Bereich des Datenschutzes praktisch belegbare Kenntnisse des deutschen und europäischen Datenschutzrechts verfügen und die Befähigung zum Richteramt oder höheren Verwaltungsdienst haben muss.

In Absatz 2 wird die bisherige Regelung des § 22 Absatz 2 BDSG a. F. zum Amtseid unverändert übernommen. Der Amtseid der oder des Bundesbeauftragten ist eine Konkretisierung des mitgliedstaatlich zu regelnden Ernennungsverfahrens gemäß Artikel 54 Absatz 1 Buchstabe c Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/680.

Die in Absatz 3 unverändert aus § 22 Absatz 3 BDSG a. F. übernommene Regelung zur Länge der Amtszeit und zur einmaligen Wiederwahl entsprechen den Vorgaben des Artikels 54 Absatz 1 Buchstabe d und e der Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstabe d und e der Richtlinie (EU) 2016/680.

Zu § 12 (Amtsverhältnis)

§ 12 regelt die Ausgestaltung, den Beginn und das Ende des Amtsverhältnisses der oder des Bundesbeauftragten.

In Absatz 1 wird der bisherige § 22 Absatz 4 Satz 1 BDSG a. F. unverändert übernommen. Die Ausgestaltung als öffentlich-rechtliches Amtsverhältnis eigener Art sichert die Unabhängigkeit der oder des Bundesbeauftragten dienstrechtlich ab. Es handelt sich um eine unionsrechtlich gemäß Artikel 54 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 und Artikel 42 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/680 zulässige Konkretisierung der Amtsstellung der oder des Bundesbeauftragten.

Absatz 2 regelt den Beginn und das Ende der Amtszeit der oder des Bundesbeauftragten. Die Regelung entspricht den Vorgaben der Artikel 53 Absatz 3 und 4, 54 Absatz 1 Buchstabe c, d und f der Verordnung (EU) 2016/679 und der Artikel 43 Absatz 3 und 4, 44 Absatz 1 Buchstabe c, d und f der Richtlinie (EU) 2016/680 und konkretisiert diese.

Nach Absatz 2 Satz 1 beginnt das Amtsverhältnis der oder des Bundesbeauftragten in wortgleicher Übernahme des bisherigen § 23 Absatz 1 Satz 1 BDSG a. F. mit der Aushändigung der Ernennungsurkunde. Die Regelung ist eine nähere Ausgestaltung des Ernennungsverfahrens der Leiterin oder des Leiters der Aufsichtsbehörden, das nach Artikel 54 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/680 durch die Mitgliedstaaten zu regeln ist.

Absatz 2 Satz 2 bis 6 konkretisieren die Voraussetzungen und das Verfahren der Beendigung des Amtsverhältnisses und der Amtsenthebung (Artikel 53 Absatz 3 und 4, 54 Absatz 1 Buchstabe f letzter Satzteil der Verordnung (EU) 2016/679 und Artikel 43 Absatz 3 und 4, Artikels 44 Absatz 1 Buchstabe f letzter Satzteil der Richtlinie (EU) 2016/680). Diese orientieren sich unter Anpassung an die Anforderungen der genannten EU-Rechtsakte inhaltlich an der bisherigen Regelung des § 23 Absatz 1 Satz 2 bis 6 BDSG a. F.

Absatz 2 Satz 2 sieht in Übereinstimmung mit Artikel 53 Absatz 3 der Verordnung (EU) 2016/679 und Artikel 43 Absatz 3 der Richtlinie (EU) 2016/680 als Gründe der Beendigung des Amtsverhältnisses den Ablauf der Amtszeit und den Rücktritt der oder des Bundesbeauftragten vor. Die in Artikel 53 Absatz 3 der Verordnung (EU) 2016/679 und Artikel 43 Absatz 3 der Richtlinie (EU) 2016/680 als weiterer Beendigungsgrund vorgesehene verpflichtende Versetzung in den Ruhestand gemäß dem mitgliedstaatlichen Recht kommt wegen der Ausgestaltung des Amtes der oder des Bundesbeauftragten als öffentlich-rechtliches Amtsverhältnis eigener Art, wie nach bisheriger Rechtslage, nicht in Betracht.

Die bislang in § 23 Absatz 1 Satz 2 Nummer 2 BDSG a. F. geregelte Entlassung der oder des Bundesbeauftragten wird, der Systematik der Artikel 53 Absatz 3 und 4 der Verordnung (EU) 2016/679 und Artikel 43 Absatz 3 und 4 der Richtlinie (EU) 2016/680 folgend, künftig unter dem Begriff der Amtsenthebung in den Sätzen 3 bis 5 unter Fortentwicklung der bisherigen Regelung des § 23 Absatz 1 Satz 3 bis 5 BDSG a. F. fortgeführt. Satz 3 sieht – wie bisher – ein Amtsenthebungsverfahren durch die Bundespräsidentin oder den Bundespräsidenten auf Vorschlag der Präsidentin oder des Präsidenten des Deutschen Bundestages vor. Der bislang in § 23 Absatz 1 Satz 3 BDSG a. F. vorgesehene Bezug auf die Entlassungsgründe bei einer Richterin oder einem Richter auf Lebenszeit musste jedoch an Artikel 53 Absatz 4 der Verordnung (EU) 2016/679 bzw. Artikel 43 Absatz 4 der Richtlinie (EU) 2016/680 angepasst werden, der eine Amtsenthebung nur bei einer schweren Verfehlung oder bei Nichterfüllung der Voraussetzungen für die weitere Wahrnehmung des Amtes vorsieht.

Die Sätze 4 und 5 enthalten weitere, auf Artikel 54 Absatz 1 Buchstabe f letzter Satzteil der Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstabe f letzter Satzteil der Richtlinie (EU) 2016/680 beruhende Verfahrensregelungen, welche an § 23 Absatz 1 Satz 4 und 5 BDSG a. F. angelehnt sind.

Satz 6 regelt die bislang in § 23 Absatz 1 Satz 6 BDSG a. F. vorgesehene Pflicht der oder des Bundesbeauftragten zur Weiterführung des Amtes bis zur Ernennung einer Nachfolgerin oder eines Nachfolgers. Um dem ausscheidenden Amtswalter eine persönliche Perspektive und Planungssicherheit zu geben, wird die Pflicht zur Weiterführung des Amtes auf höchstens sechs Monate begrenzt. Nach Ablauf dieser Frist erfolgt die Vertretung durch die Leitende Beamtin oder den Leitenden Beamten gemäß Absatz 3.

Die Beendigung des Beschäftigungsverhältnisses der Bediensteten der oder des Bundesbeauftragten bestimmt sich nach allgemeinen beamten- und arbeitsrechtlichen Grundsätzen, so dass es weitergehender Regelungen nach Artikel 54 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstabe f der Richtlinie (EU) 2016/680 nicht bedarf.

Absatz 3 führt die bisherige Vertretungsregelung des §22 Absatz 6 BDSG a. F. unverändert fort. Die Wahrnehmung der Rechte der oder des Bundesbeauftragten durch die Leitende Beamtin oder den Leitenden Beamten ist eine zweckmäßige, im engen Zusammenhang zu den Regelungsaufträgen des Artikel 54 Absatz 1 Buchstabe a und d der Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstabe a und d der Richtlinie (EU) 2016/680 stehende Regelung zur Gewährleistung der Funktionsfähigkeit und Aufgabenerfüllung bei Abwesenheit der oder des Bundesbeauftragten.

In Absatz 4 werden die Besoldung, Versorgung und sonstigen Bezüge der oder des Bundesbeauftragten unverändert unter wortgleicher Übernahme des bisherigen § 23 Absatz 7 BDSG a. F. beibehalten. Es handelt sich um eine notwendige mitgliedstaatliche Begleitregelung zur Regelung der Errichtung der Aufsichtsbehörden und des Verfahrens für die Ernennung der Leiterin oder des Leiters der Aufsichtsbehörde (Artikel 54 Absatz 1 Buchstabe a und c der Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstabe a und c der Richtlinie (EU) 2016/680).

Zu § 13 (Rechte und Pflichten)

§ 13 regelt die Rechte und Pflichten der oder des Bundesbeauftragten. Die bisherigen Regelungen des § 23 Absatz 2 bis 6 und 8 BDSG a. F. werden weitestgehend unverändert übernommen.

Absatz 1 Satz 1 enthält ein umfassendes Verbot sämtlicher nicht mit dem Amt zu vereinbarender Handlungen und Tätigkeiten, gleich ob entgeltlich oder unentgeltlich. Der Wortlaut entspricht Artikel 52 Absatz 3 der Verordnung (EU) 2016/679, der aus Gründen der Verständlichkeit und Kohärenz auch für Artikel 42 Absatz 3 der Richtlinie (EU) 2016/680 gelten soll. Satz 2 und 3 übernehmen die bisherige Regelung des § 23 Absatz 2 BDSG a. F. inhaltlich unverändert, gestalten diese nunmehr aber als Konkretisierung des allgemeinen Verbots der Ausübung mit dem Amt nicht zu vereinbarender Handlungen und Tätigkeiten (Satz 1) aus. Hierdurch werden Artikel 54 Absatz 1 Buchstabe f zweiter Satzteil der Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstabe f zweiter Satzteil der Richtlinie (EU) 2016/680 umgesetzt.

Die Absätze 2 bis 6 entsprechen § 23 Absatz 3 bis 6 und 8 BDSG a. F.

Die Mitteilungspflicht der oder des Bundesbeauftragten über Geschenke (Absatz 2) ist eine Konkretisierung der aus Artikel 52 Absatz 3 und 54 Absatz 1 Buchstabe f zweiter Satzteil der Verordnung (EU) 2016/679 und Artikel 42 Absatz 3 und 44 Absatz 1 Buchstabe f zweiter Satzteil der Richtlinie (EU) 2016/680 folgenden mitgliedstaatlichen Regelungsspielräume zu den Pflichten und Handlungsverboten. Der bisherige § 23 Absatz 3 BDSG a. F. wird unverändert übernommen.

Absatz 3 regelt das Zeugnisverweigerungsrecht der oder des Bundesbeauftragten und ihrer Mitarbeiterinnen oder seiner Mitarbeiter. Als Konkretisierung der Ausgestaltung der Aufsichtsbehörden und sachgerechte Ergänzung der aus Absatz 4 folgenden Verschwiegenheitspflicht sichert das Zeugnisverweigerungsrecht die effektive Aufgabenwahrnehmung der oder des Bundesbeauftragten ab. Hierzu wird der bisherige § 23 Absatz 4 BDSG a. F. wortgleich übernommen.

Absatz 4 setzt Artikel 54 Absatz 2 der Verordnung (EU) 2016/679 und Artikel 44 Absatz 2 der Richtlinie (EU) 2016/680 zur Verschwiegenheitspflicht um. Hierzu wird der bisherige § 23 Absatz 5 BDSG a. F. wortgleich übernommen.

In Absatz 5 (Zeugenaussage und dessen Einschränkungen) wird der bisherige § 23 Absatz 6 BDSG a. F. wortgleich übernommen. Das Recht zur Zeugenaussage steht in unmittelbarem Bezug zu dem Zeugnisverweigerungsrecht (Absatz 3) und der Verschwiegenheitspflicht (Absatz 4) der oder des Bundesbeauftragten.

Absatz 6 ist eine Kombination des Regelungsgehalts aus § 12 Absatz 3 und § 23 Absatz 8 BDSG a. F. zur Erstreckung des Zeugnisverweigerungsrechts und der Beistands- und Unterrichtungspflichten der oder des Bundesbeauftragten gegenüber den Finanzbehörden auf die Landesbeauftragten für den Datenschutz.

Zu § 14 (Aufgaben)

§ 14 Absatz 1 regelt die Aufgaben der oder des Bundesbeauftragten zum Zweck der Umsetzung des Artikels 46 der Richtlinie (EU) 2016/680. Zu diesem Zweck werden die in Artikel 57 der Verordnung (EU) 2016/679 vorgesehenen Aufgaben der Aufsichtsbehörden unter redaktioneller Anpassung des Wortlauts insoweit wiederholt, als sie inhaltlich deckungsgleich mit den Vorgaben der Richtlinie (EU) 2016/680 sind. Es handelt sich somit um die gemeinsame Schnittmenge der aus der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 resultierenden Aufgaben. Die Regelung gilt unbeschadet anderer Aufgaben nach der Verordnung (EU) 2016/679. Soweit sich die Auflistung in Absatz 1 Satz 1 nicht explizit nur auf die Verordnung oder die Richtlinie bezieht, gelten die Aufgaben der oder des Bundesbeauftragten – wie bisher § 24 Absatz 1 BDSG a. F. – auch für Datenverarbeitungen, die nicht in den Anwendungsbereich des Unionsrechts fallen. Satz 2 setzt Artikel 46 Absatz 1 Buchstabe g der Richtlinie (EU) 2016/680 um; dieser hat in Artikel 57 der Verordnung (EU) 2016/679 keine Entsprechung.

Soweit die oder der Bundesbeauftragte im Rahmen der Aufgabenwahrnehmung nach § 14 Absatz 1 Nummer 2 die Öffentlichkeit über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten speziell von Kindern sensibilisiert und aufklärt, kann dies insbesondere in Zusammenarbeit mit den für den Kinder- und Jugendschutz zuständigen Stellen des Bundes erfolgen.

Absatz 2 konkretisiert die Beratungsbefugnisse der oder des Bundesbeauftragten für den gesamten Anwendungsbereich des BDSG. Hierdurch wird Artikel 47 Absatz 3 der Richtlinie (EU) 2016/680 umgesetzt. Zugleich wird der Adressatenkreis des Artikels 58 Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 konkretisiert, indem klargestellt wird, dass im Einklang mit dem mitgliedstaatlichen Recht die Beratungsbefugnisse auch gegenüber allen sonstigen Einrichtungen und Stellen sowie den Ausschüssen des Deutschen Bundestages und dem Bundesrat als Teil des nationalen Parlaments bestehen. Satz 2 greift § 26 Absatz 2 Satz 2 BDSG a. F. auf.

Absatz 3 und 4 setzt Artikel 46 Absatz 2 bis 4 der Richtlinie (EU) 2016/680 in Übereinstimmung mit der Regelung des Artikels 57 Absatz 2 bis 4 der Verordnung (EU) 2016/679 um.

Zu § 15 (Tätigkeitsbericht)

§ 15 bestimmt, dass die oder der Bundesbeauftragte einen jährlichen Bericht über ihre oder seine Tätigkeit zu erstellen hat. Der Jahresbericht gilt sowohl für Datenverarbeitungen im Rahmen von Tätigkeiten, die dem Unionsrecht unterfallen als auch für solche, die nicht dem Unionsrecht unterfallen. Die Abweichung von dem bisher (§ 26 Absatz 1 BDSG a. F.) vorgesehenen Berichtszeitraum von zwei Jahren beruht auf den Vorgaben des in Artikel 59 der Verordnung (EU) 2016/679 und Artikel 49 der Richtlinie (EU) 2016/680 genannten Tätigkeitsberichts (Jahresbericht). Dieser Zeitraum wird aus Gründen der Einheitlichkeit und Praktikabilität auf Datenverarbeitungen im Rahmen von Tätigkeiten, die nicht dem Unionsrecht unterfallen, ausgedehnt, so dass die oder der Bundesbeauftragte wie bisher einen einheitlichen Bericht erstellen kann.

Satz 2 konkretisiert die Empfänger des in Artikel 59 der Verordnung (EU) 2016/679 und Artikel 49 der Richtlinie (EU) 2016/680 genannten Tätigkeitsberichts (Jahresbericht). Auch der Bundesrat ist nach unionsrechtlichem Verständnis nationales Parlament im Sinne des Artikels 12 des Vertrags über die Europäische Union (EUV) und der Protokolle Nummer 1 und 2 des Lissabon-Vertrags. Der Bericht der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich zu machen (Artikel 59 Satz 3 der Verordnung (EU) 2016/679 und Artikel 49 Satz 3 der Richtlinie (EU) 2016/680). Der oder dem Bundesbeauftragten steht es frei, den Tätigkeitsbericht darüber hinaus betroffenen oder interessierten Behörden zur Verfügung zu stellen.

Zu § 16 (Befugnisse)

§ 16 regelt für den gesamten Anwendungsbereich des BDSG die Befugnisse der oder des Bundesbeauftragten. Absatz 1 verweist für die Befugnisse und deren Ausübung im Anwendungsbereich der Verordnung (EU) 2016/679 auf Artikel 58 der Verordnung (EU) 2016/679. Absatz 2 regelt die Befugnisse der oder des Bundesbeauftragten bei Datenverarbeitungen, deren Zwecke außerhalb der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 liegen, auch wenn für diese durch die Regelung des § 1 Absatz 8 BDSG die Verordnung (EU) 2016/679 entsprechend anzuwenden ist, sowie bei Datenverarbeitungen im Geltungsbereich der Richtlinie (EU)

2016/680. Absatz 3 bis 5 gilt sowohl im Anwendungsbereich der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 als auch außerhalb der Vorgaben des europäischen Rechts.

Absatz 1 Satz 1 nimmt im Anwendungsbereich der Verordnung (EU) 2016/679 aus Gründen der Klarstellung und Lesbarkeit auf die Befugnisse des Artikels 58 der Verordnung (EU) 2016/679 Bezug.

Satz 2 bis 4 enthält Verfahrensregelungen im Sinne des Artikels 58 Absatz 4 der Verordnung (EU) 2016/679. Danach erfolgt die Ausübung der den Aufsichtsbehörden übertragenen Befugnisse vorbehaltlich geeigneter Garantien, einschließlich ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten. Die bisherigen Regelungen des § 25 Absatz 1 BDSG a. F. werden aufgegriffen und modifiziert.

Hierdurch wird sichergestellt, dass von der oder dem Bundesbeauftragten festgestellte Verstöße gegen die Vorschriften des Datenschutzes der jeweils zuständigen Rechts- oder Fachaufsichtsbehörde mitgeteilt werden und diese vor der Ausübung der aufgezählten Abhilfebefugnisse des Artikels 58 Absatz 2 der Verordnung (EU) 2016/679 unter Setzung einer angemessenen Frist Gelegenheit zur Stellungnahme erhält. Bei den übrigen Abhilfebefugnissen des Artikel 58 Absatz 2 der Verordnung (EU) 2016/679 besteht hingegen kein Bedarf an einer vorherigen Information der Rechts- oder Fachaufsichtsbehörde. Durch die Mitteilung wird insbesondere gewährleistet, dass die zuständige Fachaufsichtsbehörde – unter den an § 28 Absatz 2 Nummer 1 und Absatz 3 VwVfG angelehnten Ausnahmen für Eilfälle und entgegenstehende zwingende öffentliche Interessen – Kenntnis von dem Verstoß erhält und vor der Ausübung weitergehender Befugnisse durch die oder den Bundesbeauftragten Anspruch auf rechtliches Gehör findet. Die Gefahr divergierender Anweisungen zwischen Datenschutzaufsicht und Recht- oder Fachaufsicht wird hierdurch reduziert. Widersprüchliche Auffassungen der Datenschutzaufsicht und der Fachaufsicht sind auf dem Gerichtsweg zu klären. Widerspricht die Verfügung der oder des Bundesbeauftragten der Rechtsauffassung der Fachaufsichtsbehörde, kann diese den Verantwortlichen zur gerichtlichen Klärung anweisen.

Absatz 2 regelt die Befugnisse der oder des Bundesbeauftragten bei Datenverarbeitungen, deren Zwecke außerhalb der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 liegen sowie Datenerarbeitungen im Geltungsbereich der Richtlinie (EU) 2016/680. Der oder dem Bundesbeauftragten werden nach der Regelungssystematik in diesem Gesetz keine Durchgriffsbefugnisse gegenüber Verantwortlichen gegeben, die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten – wobei die Verfolgung von Straftaten den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit umfasst – zuständig sind und soweit sie zu diesen Zwecken Daten verarbeiten. Dies folgt aus der unterschiedlichen Ausgestaltung der Abhilfebefugnisse in der Verordnung (EU) 2016/679 einerseits und der Richtlinie (EU) 2016/680 und den dort bestehenden fachlichen Bedürfnissen andererseits, weshalb die Richtlinie mehr Flexibilität eröffnet. Im Bereich der Straftatenverhütung, -ermittlung und -verfolgung sowie der darauf bezogenen Gefahrenabwehr lassen sich Letztentscheidungs- und Anordnungsbefugnisse der oder des Bundesbeauftragten nicht mit der Sensibilität und Komplexität der entsprechenden Verarbeitungen und dem Bedürfnis nach ständiger Verfügbarkeit rechtmäßig erhobener Daten und Datenverarbeitungsanlagen in Einklang bringen. Dies gilt entsprechend für den nicht EU-rechtlich erfassten Bereich von Verarbeitungen zu Zwecken außerhalb beider Rechtsakte. Der oder dem Bundesbeauftragten stehen mit dem aus § 25 BDSG a. F. bekannten Instrument der Beanstandung, der aus Artikel 47 Absatz 2 Buchstabe a der Richtlinie (EU) 2016/680 entnommenen Warnung und sonstigen nicht regelungsbedürftigen Möglichkeiten, den als öffentliche Stelle an Recht und Gesetz gebundenen Verantwortlichen auf aus ihrer oder seiner Sicht rechtswidrige Verarbeitungen aufmerksam zu machen, ausreichend Möglichkeiten zur Verfügung, ihren Beitrag dazu zu leisten, aus ihrer oder seiner Sicht rechtswidrigen Zuständen abzuhelfen. Es bleibt dem Gesetzgeber unbenommen, in sicherheitsbehördlichen fachgesetzlichen Regelungen – wie etwa § 67 Absatz 2 BKAG-E – die in Absatz 2 genannten Befugnisse weiter auszugestalten und gegebenenfalls um Durchgriffsbefugnisse auch anzureichern.

In Absatz 3 wird für den gesamten Anwendungsbereich des BDSG der bisherige § 24 Absatz 2 Satz 1 und 2 BDSG a. F. weitgehend übernommen. Für Berufsgeheimnisträger findet sich im Anwendungsbereich der Verordnung (EU) 2016/679 eine Spezialregelung in § 29 BDSG.

Absatz 4 greift die bislang in § 24 Absatz 4 Satz 2 BDSG a. F. geregelten Zugangs- und Informationsrechte der oder des Bundesbeauftragten auf. Hierdurch wird Artikel 47 Absatz 1 der Richtlinie (EU) 2016/680 umgesetzt und die gemäß Artikel 58 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 zur Ausübung der Untersuchungsbefugnisse notwendigen mitgliedstaatlichen Verfahrensvorschriften für die Zugangs- und Betretensrechte von Grundstücken und Diensträumen geschaffen (Nummer 1).

Das umfassende Informationsrecht der oder des Bundesbeauftragten in Nummer 2 erfolgt in Umsetzung des Artikels 47 Absatz 1 der Richtlinie (EU) 2016/680 wortgleicher Anlehnung an Artikel 58 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679.

Absatz 5 enthält die bislang in § 26 Absatz 4 BDSG a. F. vorgesehene Hinwirkungsfunktion der oder des Bundesbeauftragten auf die Zusammenarbeit mit den Aufsichtsbehörden der Länder im öffentlichen und nichtöffentlichen Bereich.

Zu § 17 (Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle)

Mitgliedstaaten mit mehr als einer Aufsichtsbehörde sind verpflichtet, im Einklang mit den nationalen Rechtsvorschriften eine Aufsichtsbehörde zu bestimmen, die als gemeinsamer Vertreter im Europäischen Datenschutzausschuss fungiert (Artikel 51 Absatz 3 und 68 Absatz 4 der Verordnung (EU) 2016/679).

§ 17 Absatz 1 Satz 1 setzt diesen Regelungsauftrag mit der Benennung der oder des Bundesbeauftragten zum gemeinsamen Vertreter der deutschen Aufsichtsbehörden um. Zugleich wird mit der Einrichtung einer zentralen Anlaufstelle bei der oder dem Bundesbeauftragten der Erwägungsgrund 119 der Verordnung (EU) 2016/679 aufgegriffen.

Die gesetzliche Bestimmung des gemeinsamen Vertreters setzt den Regelungsauftrag des Artikels 51 Absatz 3 und 68 Absatz 4 der Verordnung (EU) 2016/679 und des Artikels 41 Absatz 4 der Richtlinie (EU) 2016/680 um, garantiert die Kontinuität der Amtswahrnehmung und ist am besten geeignet, der Stimme der deutschen Aufsichtsbehörden im Europäischen Datenschutzausschuss Gewicht zu verleihen. Die Regelung stellt eine strukturelle Parität zu den übrigen Mitgliedstaaten her, die fast ausschließlich nur über eine Aufsichtsbehörde verfügen. Die Ernennung der oder des Bundesbeauftragten entspricht dem Grundsatz der Außenvertretung des Bundes, wie er Artikel 23 des Grundgesetzes und dem Gesetz über die Zusammenarbeit von Bund und Ländern in Angelegenheiten der Europäischen Union (EUZBLG) zugrunde liegt. Aufgrund der Funktion der oder des Bundesbeauftragten in der Artikel 29-Gruppe, dem Vorgängergremium des Europäischen Datenschutzausschusses, verfügt die Dienststelle über jahrelange Erfahrungen und organisatorisch verfestigte Strukturen zur Wahrnehmung der Aufgabe.

Durch Absatz 1 Satz 1 wird zudem die zentrale Anlaufstelle bei der oder dem Bundesbeauftragten eingerichtet. Diese soll gemäß Erwägungsgrund 119 der Verordnung (EU) 2016/679 eine wirksame Beteiligung aller Aufsichtsbehörden am Kohärenzverfahren und eine rasche und reibungslose Zusammenarbeit mit den Aufsichtsbehörden der anderen Mitgliedstaaten, dem Europäischen Datenschutzausschuss und der Europäischen Kommission gewährleisten.

Die zentrale Anlaufstelle soll es den Aufsichtsbehörden der anderen Mitgliedstaaten, dem Europäischen Datenschutzausschuss und der Europäischen Kommission ermöglichen, ohne Kenntnis der innerstaatlichen Zuständigkeitsverteilung effektiv mit den deutschen Aufsichtsbehörden zu kommunizieren. Zu diesem Zweck leitet die zentrale Anlaufstelle alle ihr zugeleiteten Informationen und den bei ihr eingehenden Geschäftsverkehr an die hiervon betroffenen deutschen Aufsichtsbehörden weiter.

Umgekehrt können sich die Aufsichtsbehörden bei der Kommunikation mit dem Europäischen Datenschutzausschuss, der Europäischen Kommission und den Aufsichtsbehörden der übrigen Mitgliedstaaten der zentralen Anlaufstelle zur Weiterleitung zweckdienlicher Informationen bedienen. Insbesondere im Fall der Federführung einer deutschen Aufsichtsbehörde kann die zentrale Anlaufstelle bei der Identifizierung der betroffenen Aufsichtsbehörden in anderen Mitgliedstaaten unterstützend tätig sein.

Der zentralen Anlaufstelle kommt eine rein unterstützende Aufgabe zu. Sie übt keine hoheitlichen Verwaltungsaufgaben aus. Zu den Unterstützungsleistungen der zentralen Anlaufstelle zählt die Koordinierung der gemeinsamen Willensbildung unter den Aufsichtsbehörden des Bundes und der Länder. Die zentrale Anlaufstelle wirkt zudem auf die Einhaltung der von der Verordnung (EU) 2016/679 vorgesehenen Fristen und Verfahren des Informationsaustauschs, beispielsweise durch standardisierte Formate nach Artikel 67 der Verordnung (EU) 2016/679, hin. Die Unterstützungsfunktion der zentralen Anlaufstelle besteht über das in Erwägungsgrund 119 genannte Kohärenzverfahren hinaus für alle Angelegenheiten der Europäischen Union, insbesondere für das Verfahren der Zusammenarbeit der Artikel 60 bis 62 der Verordnung (EU) 2016/679.

Die zentrale Anlaufstelle wird bei der oder dem Bundesbeauftragten eingerichtet. Die Bündelung der Funktion der zentralen Anlaufstelle mit der Aufgabe des gemeinsamen Vertreters bei der oder dem Bundesbeauftragten ist

effizient und daher zweckmäßig. Die zentrale Anlaufstelle ist der Dienststelle der oder des Bundesbeauftragten organisatorisch angegliedert. Ihre Aufgabe ist von den übrigen Aufgaben der oder des Bundesbeauftragten organisatorisch getrennt.

Absatz 1 Satz 2 trägt der innerstaatlichen Zuständigkeitsverteilung zwischen Bund und Ländern bei der Vertretung im Europäischen Datenschutzausschuss Rechnung. Er sieht vor, dass eine Leiterin oder ein Leiter einer Aufsichtsbehörde der Länder als Stellvertreter des gemeinsamen Vertreters fungiert (Artikel 68 Absatz 3 der Verordnung (EU) 2016/679). Der Stellvertreter hat nicht nur ein permanentes Anwesenheitsrecht, das Gewähr für die Wahrung der Länderbelange und die Sicherstellung des Informationsflusses zu den Aufsichtsbehörden der Länder bietet, sondern kann gemäß Absatz 2 von dem gemeinsamen Vertreter verlangen, die Übertragung der Verhandlungsführung und das Stimmrecht verlangen, sofern es sich um eine Angelegenheit handelt, für welche die Länder alleine das Recht zur Gesetzgebung haben oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen. Die Stellung des Stellvertreters geht daher über partielle Anwesenheitsrechte, wie sie das EUZBLG im ausschließlichen Zuständigkeitsbereich der Länder vorsieht, hinaus.

Die Benennung der oder des Bundesbeauftragten zum gemeinsamen Vertreter und deren oder dessen Vertretung durch eine Aufsichtsbehörde der Länder führt das bewährte Modell der deutschen Repräsentation in der Artikel 29-Gruppe fort.

Die Wahl des Stellvertreters erfolgt durch den Bundesrat. Sie erfolgt gemäß Absatz 1 Satz 3 für die Dauer von fünf Jahren. Scheidet der Stellvertreter früher aus dem Amt als Leiterin oder Leiter der Aufsichtsbehörde aus, endet zugleich die Funktion als Stellvertreter (Absatz 1 Satz 4). Eine mehrmalige Wiederbestellung des Vertreters ist zulässig (Absatz 1 Satz 5).

Absatz 2 sieht die Beteiligungsrechte des Stellvertreters bei der Außenvertretung der deutschen Aufsichtsbehörden im Europäischen Datenschutzausschuss vor. In Anlehnung an das und in Erweiterung des EUZBLG überträgt der gemeinsame Vertreter in Angelegenheiten, die die Wahrnehmung einer Aufgabe betreffen, für welche die Länder alleine das Recht zur Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, dem Stellvertreter auf dessen Verlangen die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss. Die Außenvertretung des Stellvertreters umfasst alle Angelegenheiten, die ausschließlich Gesetzgebungsbefugnisse der Länder oder die Datenverarbeitung durch Landesbehörden betreffen.

Zu § 18 (Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder)

Die in Kapitel VII der Verordnung (EU) 2016/679 geregelten Verfahren der Zusammenarbeit und Kohärenz enthalten Zuständigkeitsverteilungen und Verfahrensregelungen zwischen den Aufsichtsbehörden verschiedener Mitgliedstaaten. Sie regeln aber nicht die Einzelheiten der innerstaatlichen Koordination und Willensbildung in Mitgliedstaaten mit mehr als einer Aufsichtsbehörde. Mitgliedstaaten, die wie die Bundesrepublik Deutschland über mehrere für die Überwachung der Anwendung der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörden verfügen, haben gemäß Erwägungsgrund 119 und Artikel 51 Absatz 3 der Verordnung (EU) 2016/679 die wirksame Beteiligung aller nationalen Aufsichtsbehörden und die Einhaltung der Regeln für das Kohärenzverfahren durch alle nationalen Aufsichtsbehörden innerstaatlich sicherzustellen.

Dieser Regelungsauftrag gilt über den unmittelbaren, auf das Kohärenzverfahren im Europäischen Datenschutzausschuss bezogenen Regelungsauftrag hinaus für alle Angelegenheiten des Europäischen Datenschutzausschusses nach Artikel 70 der Verordnung (EU) 2016/679 und Artikel 51 der Richtlinie (EU) 2016/680 sowie für das Verfahren der Zusammenarbeit der europäischen Aufsichtsbehörden nach den Artikeln 60 bis 62 der Verordnung (EU) 2016/679. § 18 Absatz 1 erfasst alle Fallgestaltungen, in denen aufgrund der Wirkung für und gegen die übrigen deutschen Datenschutzbehörden und deren Vollzugsentscheidungen eine inhaltliche Vorabstimmung erforderlich ist, also unter anderem auch die Fälle gemäß Artikel 60 Absatz 6 der Verordnung (EU) 2016/679, in denen eine betroffene Aufsichtsbehörde Einspruch gegen den Vorschlag der federführend zuständigen Aufsichtsbehörde in einem Einzelfall einlegt.

Das Verfahren der Zusammenarbeit ist dem Kohärenzverfahren nach Maßgabe des Artikels 65 Absatz 1 Buchstabe a und b der Verordnung (EU) 2016/679 strukturell vorgelagert. Auch hier müssen Mitgliedstaaten mit mehreren Aufsichtsbehörden die wirksame Beteiligung aller nationalen Aufsichtsbehörden und die Einhaltung der Regeln der Zusammenarbeit gewährleisten.

§ 18 regelt das Verfahren der innerstaatlichen Willensbildung zwischen den für die Überwachung und Durchsetzung der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörden des Bundes und der Länder.

Absatz 1 Satz 1 greift das in den Artikeln 51 Absatz 2, 60 Absatz 1 und 63 der Verordnung (EU) 2016/679 niedergelegte Prinzip der Zusammenarbeit zwischen den Aufsichtsbehörden der Mitgliedstaaten für die Aufsichtsbehörden von Bund und Ländern mit dem Ziel einer einheitlichen Anwendung der Verordnung auf. Das Prinzip der gegenseitigen Unterstützung und Kooperation der Aufsichtsbehörden auf Unionsebene wird hierdurch auf das Verhältnis der Aufsichtsbehörden des Bundes und der Länder untereinander übertragen. Auch eine divergierende Rechtspraxis zwischen den deutschen Aufsichtsbehörden ist dem Ziel einer einheitlichen Anwendung der Verordnung (EU) 2016/679 abträglich.

Die in Absatz 1 Satz 2 und 3 niedergelegten Pflichten der frühzeitigen Beteiligung und des Austauschs zweckdienlicher Informationen stehen in unmittelbarem Zusammenhang mit dem Prinzip der Zusammenarbeit und konturieren dieses inhaltlich. Die frühzeitige Einbindung aller Aufsichtsbehörden des Bundes und der Länder in den nationalen Willensbildungsprozess stellt im Sinne des Erwägungsgrundes 119 der Verordnung (EU) 2016/679 eine wirksame Beteiligung der nationalen Aufsichtsbehörden am Kohärenzverfahren und darüber hinaus sicher.

Normadressaten sind alle Aufsichtsbehörden, einschließlich der federführenden Aufsichtsbehörde im Sinne des § 19 Absatz 1. Auch die federführende Aufsichtsbehörde muss vor der Übermittlung eines Beschlussentwurfs an die betroffenen Aufsichtsbehörden der anderen Mitgliedstaaten im Verfahren der Zusammenarbeit nach Artikel 60 Absatz 3 der Verordnung (EU) 2016/679 die übrigen Aufsichtsbehörden des Bundes und der Länder einbinden und einen nach Maßgabe des Absatzes 2 festgelegten gemeinsamen Standpunkt ermitteln. Die frühzeitige Ermittlung eines gemeinsamen Standpunktes der Aufsichtsbehörden ist notwendig, um die Kontinuität des deutschen Standpunktes während des gesamten Verfahrens der Zusammenarbeit und Kohärenz sicherzustellen.

Der nach Absatz 1 Satz 3 vorgesehene Austausch aller zweckdienlichen Informationen schafft zwischen den Aufsichtsbehörden die rechtliche Grundlage für die Übermittlung personenbezogener Daten oder Informationen, die einem Betriebs- und Geschäftsgeheimnis unterliegen. Die Regelung ist an Artikel 60 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 sowie § 38 Absatz 1 Satz 4 BDSG a. F. angelehnt.

Absatz 1 Satz 4 verpflichtet die Aufsichtsbehörden des Bundes und der Länder dazu, die nach Artikel 85 und 91 der Verordnung (EU) 2016/679 eingerichteten spezifischen Aufsichtsbehörden an der Festlegung des gemeinsamen Standpunktes zu beteiligen, soweit diese von der Angelegenheit betroffen sind. Bei der Festlegung eines gemeinsamen Standpunktes berücksichtigen die Aufsichtsbehörden die Stellungnahmen der spezifischen Aufsichtsbehörden.

Absatz 2 regelt das Verfahren der Festlegung eines gemeinsamen Standpunktes der Aufsichtsbehörden des Bundes und der Länder, wenn kein Einvernehmen erzielt werden konnte. In Anlehnung an Artikel 60 Absatz 1 Satz 1 der Verordnung (EU) 2016/679 sollen die Aufsichtsbehörden des Bundes und der Länder einen Konsens anstreben. Sofern ein Einvernehmen nicht zu erreichen ist, legen die federführende Aufsichtsbehörde bzw. der gemeinsame Vertreter und sein Stellvertreter einen Vorschlag für einen gemeinsamen Standpunkt vor, der den Verhandlungen zu Grunde gelegt wird. Etwas anderes gilt gemäß Absatz 2 Satz 4, wenn die Aufsichtsbehörden des Bundes und der Länder einen Gegenvorschlag beschließen, der von der einfachen Mehrheit der mitwirkenden Aufsichtsbehörden unterstützt wird. Inhaltlich kann die Ausübung der Vertretungsfunktionen somit in jeder Phase des Verfahrens durch Weisungen auf Grundlage von Mehrheitsentscheidungen aller Datenschutzbehörden bestimmt werden. Der Bund und jedes Land haben gemäß Absatz 2 Satz 5 bei der Entscheidungsfindung eine Stimme. Länder mit mehr als einer Aufsichtsbehörde können die Stimme nur einheitlich ausüben. Insbesondere im Hinblick auf die von dem Verfahren der Zusammenarbeit und der Kohärenz, aber auch von den übrigen Entscheidungsmaterien des Europäischen Datenschutzausschusses ausgehenden Präjudiz- und Bindungswirkungen für alle Aufsichtsbehörden ist die Mitwirkung aller Aufsichtsbehörden an der Entscheidungsfindung sachgerecht. Eine Pflicht zur Mitwirkung bei der Entscheidungsfindung besteht nicht; die Aufsichtsbehörden können im Rahmen möglicher Schwerpunktsetzungen von ihrem Recht auf Stimmenthaltung (Absatz 2 Satz 6) Gebrauch machen.

Die in Absatz 2 und 3 differenziert geregelten Verfahrens- und Mitwirkungsrechte der Aufsichtsbehörden und des gemeinsamen Vertreters und seines Stellvertreters bei der Festlegung des gemeinsamen Standpunktes und der darauf beruhenden Verhandlungsführung im Europäischen Ausschuss tragen in Anlehnung an die in § 5 Absatz 2 und § 6 Absatz 2 EUZBLG entwickelten Mechanismen den innerstaatlichen Zuständigkeiten des Bundes und der

Länder Rechnung und gewährleisten gleichzeitig eine effektive Vertretung der Aufsichtsbehörden im Europäischen Datenschutzausschuss. Bei der Festlegung des gemeinsamen Standpunktes ist die nach § 17 Absatz 1 Satz 1 eingerichtete zentrale Anlaufstelle eng einzubinden. Diese hat eine unterstützende Funktion bei der Koordinierung und Abfassung gemeinsamer Standpunkte und wirkt auf die Einhaltung der Fristen und vorgesehenen Verfahren des Informationsaustauschs hin.

Die Aufsichtsbehörden können die Einzelheiten des Verfahrens wie die fortlaufende Unterrichtung aller Aufsichtsbehörden durch den gemeinsamen Vertreter und dessen Stellvertreter oder die Möglichkeit der Anpassung des mehrheitlich festgelegten gemeinsamen Standpunktes im Verhandlungsfortgang durch interne Verfahrensregeln konkretisieren.

Zu § 19 (Zuständigkeiten)

§ 19 trifft ergänzend zu den Verfahrensregelungen des § 18 Regelungen zur innerstaatlichen Zuständigkeit der Aufsichtsbehörden des Bundes und der Länder im Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII der Verordnung (EU) 2016/679. Die Zuständigkeit der nach Artikel 85 und 91 der Verordnung (EU) 2016/679 eingerichteten spezifischen Aufsichtsbehörden im Bereich der Presse, des Rundfunks und der Kirchen und religiösen Vereinigungen bleibt hiervon unberührt.

Die in der Verordnung (EU) 2016/679 enthaltenen Definitionen der Artikel 56 Absatz 1 i. V. m. Artikel 4 Nummer 16 (federführende Behörde) bzw. Artikel 4 Nummer 22 (betroffene Behörde) dienen der Zuständigkeitsabgrenzung zwischen den Aufsichtsbehörden verschiedener Mitgliedstaaten. Sie verhalten sich nicht zur innerstaatlichen Zuständigkeitsverteilung. Aus innerstaatlicher Perspektive adressiert die Verordnung (EU) 2016/679 daher die mitgliedstaatliche Aufsicht in ihrer Gesamtheit, nicht aber jede einzelne Aufsichtsbehörde in einem föderal strukturierten Mitgliedstaat. Auch wenn die Mitgliedstaaten bei der Festlegung der innerstaatlichen Zuständigkeiten die Möglichkeit zu Abweichungen haben, ist die Übertragung des von der Verordnung (EU) 2016/679 vorgesehenen Rollenkonzepts sachgerecht. Dies stellt den Gleichlauf zwischen der Verordnung und der innerstaatlichen Ausgestaltung der Zuständigkeiten in Verfahren grenzüberschreitender Datenverarbeitung her.

Mit Absatz 1 wird ein an Artikel 56 Absatz 1 i. V. m. Artikel 4 Nummer 16 (federführende Behörde) der Verordnung (EU) 2016/679 eng angelehntes Konzept zur innerstaatlichen Festlegung der federführenden Behörde etabliert. Innerhalb der sachlichen Zuständigkeit der Aufsichtsbehörden der Länder ist federführende Aufsichtsbehörde die Aufsichtsbehörde desjenigen Landes, in dem der für die Datenverarbeitung Verantwortliche seine Hauptniederlassung im Sinne des Artikel 4 Nummer 16 oder einzige Niederlassung in der Europäischen Union im Sinne des Artikel 56 der Verordnung (EU) 2016/679 hat (Satz 1). Satz 2 enthält eine Sonderregelung für die oder den Bundesbeauftragten. Die oder der Bundesbeauftragte ist in ihrem oder seinen sachlichen Zuständigkeitsbereich federführende Aufsichtsbehörde, wenn der Verantwortliche seine Hauptniederlassung oder einzige EU-Niederlassung in der Bundesrepublik Deutschland hat. Artikel 56 der Verordnung (EU) 2016/679 findet daher entsprechende Anwendung. Satz 3 verweist im Fall von widersprüchlichen Standpunkten auf den in § 18 Absatz 2 vorgesehenen Entscheidungsmechanismus. Besteht kein Einvernehmen zwischen den Aufsichtsbehörden des Bundes und der Länder über die federführende Aufsichtsbehörde, legen der gemeinsame Vertreter und sein Stellvertreter einen Entscheidungsvorschlag vor. Besteht auch zwischen diesen Dissens, gibt die Stimme des gemeinsamen Vertreters den Ausschlag. Der gemeinsame Vorschlag kann durch die einfache Mehrheit der Aufsichtsbehörden des Bundes und der Länder ersetzt werden.

Der Bestimmung der federführenden Aufsichtsbehörde kommt eine Doppelfunktion zu. Innerstaatlich sind an den Status der federführenden Behörde Rechte (§ 18 Absatz 2 Satz 1) und Pflichten (§ 19 Absatz 2 Satz 1) geknüpft. Zugleich legt die Verordnung (EU) 2016/679 der federführenden Behörde zahlreiche Pflichten auf. Im Verfahren der Zusammenarbeit nach Artikel 60 hat die federführende Behörde Koordinierungs- und Informationspflichten. Nach Artikel 60 Absatz 6 im Verfahren der Zusammenarbeit und nach Artikel 65 Absatz 2 Satz 3 im Verfahren der Kohärenz gefasste Beschlüsse sind für die federführende Behörde und alle betroffenen Aufsichtsbehörden verbindlich und müssen nach Maßgabe des Artikels 60 Absatz 7 bis 9, gegebenenfalls in Verbindung mit Artikel 65 Absatz 6 der Verordnung (EU) 2016/679, vollzogen werden.

Artikel 51 Absatz 3 der Verordnung (EU) 2016/679 verpflichtet Mitgliedstaaten mit mehreren Aufsichtsbehörden dazu, sicherzustellen, dass alle innerstaatlichen Aufsichtsbehörden die Regeln für das Kohärenzverfahren einhalten. § 19 Absatz 1 legt daher fest, welche deutsche Aufsichtsbehörde den aus der Verordnung (EU) 2016/679 folgenden Verpflichtungen der federführenden Behörde nachzukommen hat.

Einer Bestimmung der innerstaatlich „betroffenen“ Aufsichtsbehörde bedarf es hingegen nicht. Sofern die Voraussetzungen des Artikels 4 Nummer 22 der Verordnung (EU) 2016/679 vorliegen, sind die Aufsichtsbehörden des Bundes und der Länder in ihrer Gesamtheit betroffen und an die Einhaltung der aus dem Verfahren der Zusammenarbeit und Kohärenz gemäß Kapitel VII der Verordnung (EU) 2016/679 erwachsenden Pflichten gebunden. Insbesondere sind Beschlüsse, die gemäß der Verordnung (EU) 2016/679 Bindungswirkung entfalten, für alle Aufsichtsbehörden des Bundes und der Länder im Rahmen ihrer Zuständigkeit verbindlich.

Absatz 2 trifft die innerstaatlich notwendige Festlegung, welche Aufsichtsbehörde gegenüber dem Beschwerdeführer, der bei einer deutschen Aufsichtsbehörde Beschwerde eingelegt hat, den Beschluss gemäß Artikel 60 Absatz 7 bis 9, ggf. in Verbindung mit Artikel 65 Absatz 6, der Verordnung (EU) 2016/679 zu erlassen hat. Die Verordnung (EU) 2016/679 bestimmt mit unmittelbarer Geltung, dass ein Beschwerdeführer, der bei einer deutschen Aufsichtsbehörde eine Beschwerde einlegt, von einer deutschen Aufsichtsbehörde beschieden werden muss. Die Verordnung (EU) 2016/679 ermöglicht jedoch die Berücksichtigung innerstaatlicher Zuständigkeiten und somit Abgaben von Beschwerden an die jeweils sachnächste Aufsichtsbehörde.

Satz 1 bestimmt, dass eingehende Beschwerden an die federführende Aufsichtsbehörde oder – nachrangig – an die Aufsichtsbehörde einer Niederlassung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters abzugeben sind. Besteht weder eine inländische Hauptniederlassung noch eine anderweitige Niederlassung in der Bundesrepublik, gibt eine sachlich unzuständige Aufsichtsbehörde die Beschwerde an die sachlich zuständige Aufsichtsbehörde am Wohnsitz des Beschwerdeführers ab (Satz 2). Wird hingegen eine Beschwerde bei einer sachlich zuständigen Aufsichtsbehörde eingereicht, ist diese unabhängig davon, ob der Beschwerdeführer in einem anderen Bundesland einen Wohnsitz hat, für die Bearbeitung der Beschwerde zuständig, sofern eine Abgabe nach Satz 1 (Hauptniederlassung oder Niederlassung in einem anderen Bundesland) nicht in Betracht kommt. Satz 3 bestimmt, dass die nach Satz 1 und 2 die Beschwerde übernehmenden Aufsichtsbehörden für die gegenüber dem Beschwerdeführer nach Maßgabe der Verordnung (EU) 2016/679 zu erlassenden Beschlüsse zuständig sind.

Zu § 20 (Gerichtlicher Rechtsschutz)

§ 20 dient sowohl der Durchführung des Artikels 78 Absatz 1 der Verordnung (EU) 2016/679 als auch der Umsetzung des Artikels 53 Absatz 1 der Richtlinie (EU) 2016/680. Danach hat jede natürliche oder juristische Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde.

§ 20 findet keine Anwendung, soweit durch bereichsspezifische Rechtsvorschriften des Bundes der Rechtsweg vor anderen Gerichten als den Gerichten der Verwaltungsgerichtsbarkeit eröffnet ist (siehe z. B. § 51 Sozialgerichtsgesetz für die Gerichte der Sozialgerichtsbarkeit; zudem behält sich der Gesetzgeber z. B. vor, für datenschutzrechtliche Fragen im Anwendungsbereich der Abgabenordnung in einem gesonderten Gesetzgebungsverfahren den Finanzrechtsweg zu eröffnen).

Absatz 1 Satz 2 stellt klar, dass von § 20 Absatz 1 Satz 1 das Bußgeldverfahren ausgenommen ist, da in dessen Anwendungsbereich nicht der Verwaltungsrechtsweg, sondern der Weg zu den Gerichten der ordentlichen Gerichtsbarkeit gegeben ist.

Durch Absatz 3 wird die örtliche Zuständigkeit beim Verwaltungsgericht am Sitz der Aufsichtsbehörde konzentriert.

Absatz 4 ist im Rahmen des Artikels 74 Absatz 1 Nummer 1 des Grundgesetzes eine kompetenzrechtlich zulässige Abweichung von § 61 Nummern 3 und 4 der Verwaltungsgerichtsordnung.

Nach Absatz 6 ist das Vorverfahren ausgeschlossen. Mangels einer der Aufsichtsbehörde übergeordneten Behörde würde der mit einem Vorverfahren angestrebte Devolutiveffekt nicht erreicht.

Nach Absatz 7 ist die Aufsichtsbehörde nicht befugt, durch Verwaltungsentscheidung die aufschiebende Wirkung der Anfechtungsklage einer anderen Behörde oder deren Rechtsträgers auszuschließen. Unbeschadet der Anordnungskompetenz der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit stehen sich die beteiligten Verwaltungsträger nicht in einem Subordinationsverhältnis gegenüber. Im Fall einer Verwaltungsstreitsache kann eine verbindliche Entscheidung allein durch das Verwaltungsgericht getroffen werden.

Zu § 21 (Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Rechtswidrigkeit eines Beschlusses der Europäischen Kommission)

Nach Artikel 58 Absatz 5 der Verordnung (EU) 2016/679 und Artikel 47 Absatz 5 der Richtlinie (EU) 2016/680 sehen die Mitgliedstaaten durch Rechtsvorschriften vor, dass Aufsichtsbehörden befugt sind, gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die Bestimmungen der Verordnung oder Richtlinie durchzusetzen.

§ 21 enthält erstmals eine Regelung zu Rechtsbehelfen der Aufsichtsbehörden des Bundes und der Länder gegen Angemessenheitsbeschlüsse der Europäischen Kommission nach Artikel 45 der Verordnung (EU) 2016/679 und Artikel 36 der Richtlinie (EU) 2016/680, gegen Genehmigungen von Standarddatenschutzklauseln und genehmigte Verhaltensregeln nach Artikel 46 Absatz 2 Buchstabe c bis e Verordnung (EU) 2016/679 sowie gegen Beschlüsse über die Allgemeingültigkeit von Verhaltensregeln nach Artikel 40 Absatz 9 der Verordnung (EU) 2016/679.

§ 21 dient insbesondere der Umsetzung des EuGH-Urteils vom 6. Oktober 2015 (Rs. C-362/14, Maximillian Schrems ./. Data Protection Commissioner), in dem der Europäische Gerichtshof die Angemessenheitsentscheidung der Europäischen Kommission [Entscheidung der Europäischen Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (2000/520/EG)] für ungültig erklärt hat. In Rn. 65 des Urteils heißt es: „Hält die Kontrollstelle die Rügen der Person, die sich mit einer Eingabe zum Schutz ihrer Rechte und Freiheiten bei der Verarbeitung ihrer personenbezogenen Daten an sie gewandt hat, dagegen für begründet, muss sie nach Artikel 28 Absatz 3 Unterabsatz 1 dritter Gedankenstrich der Richtlinie 95/46 im Licht insbesondere von Artikel 8 Absatz 3 der Charta ein Klagerecht haben. Insoweit ist es Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel der Kontrollstelle an der Gültigkeit der Entscheidung der Europäischen Kommission teilen, um eine Vorabentscheidung über deren Gültigkeit ersuchen.“ Ein nationales Gericht wird den Europäischen Gerichtshof im Wege des Vorabentscheidungsverfahren nach Artikel 267 AEUV befassen, wenn es die Zweifel der Kontrollstelle an der Gültigkeit des Beschlusses der Europäischen Kommission teilt; im Rahmen des § 21 kann sich die Aufsichtsbehörde nunmehr gerichtlich an das Bundesverwaltungsgericht wenden, dieses hat die nach Artikel 267 AEUV bestehende Prüfungskompetenz.

Absatz 4 Satz 2 ist § 47 Absatz 2 Satz 3 Verwaltungsgerichtsordnung, Absatz 5 ist § 47 Absatz 4 Verwaltungsgerichtsordnung entlehnt.

Zu § 22 (Verarbeitung besonderer Kategorien personenbezogener Daten)

Nach Artikel 9 Absatz 1 Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich untersagt. Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 sieht jedoch Ausnahmen von diesem Verbot vor. In den Fällen des Artikels 9 Absatz 2 Buchstaben b, g, h und i der Verordnung (EU) 2016/679 sind die Ausnahmen durch nationale Regelungen auszugestalten. Neben einem Ausnahmetatbestand ist im Übrigen stets erforderlich, dass eine Rechtsgrundlage für die Verarbeitung nach Artikel 6 Absatz 1 der Verordnung (EU) 2016/679 vorliegt.

§ 22 Absatz 1 legt fest, unter welchen Voraussetzungen die Verarbeitung besonderer Kategorien personenbezogener Daten ausnahmsweise zulässig ist. Durch die Stellung im Teil 2 findet die Regelung nur Anwendung für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679. Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nicht nur auf dieser Rechtsgrundlage zulässig, sondern etwa auch auf der Grundlage der sich unmittelbar aus Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 ergebenden Ausnahmetatbestände einschließlich sonstiger auf der Grundlage der Verordnung (EU) 2016/679 erlassenen bereichsspezifischen Regelungen.

Auf Absatz 1 Nummer 1 kann die Verarbeitung besonderer Kategorien personenbezogener Daten durch öffentliche und nichtöffentliche Stellen gleichermaßen gestützt werden, während Absatz 1 Nummer 2 nur Ausnahmetatbestände für öffentliche Stellen enthält. Im Einzelnen wird mit der Vorschrift von den Öffnungsklauseln des Artikels 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 (in Bezug auf Absatz 1 Nummer 1 Buchstabe a), des Artikels 9 Absatz 2 Buchstabe h i. V. m. Absatz 3 der Verordnung (EU) 2016/679 (in Bezug auf Absatz 1

Nummer 1 Buchstabe b), des Artikels 9 Absatz 2 Buchstabe i der Verordnung (EU) 2016/679 (in Bezug auf Absatz 1 Nummer 1 Buchstabe c) und des Artikels 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 (in Bezug auf Absatz 1 Nummer 2 Buchstabe a bis d Gebrauch gemacht. Der zweite Halbsatz in Absatz 1 Nummer 1 Buchstabe c dient der Klarstellung in Umsetzung des Artikels 9 Absatz 2 Buchstabe i der Verordnung (EU) 2016/679: Das deutsche Recht sieht bereits umfangreiche angemessene und spezifische Maßnahmen zum Schutz des Berufsgeheimnisses vor, insbesondere durch § 203 StGB und die einschlägigen Berufsordnungen. Daneben können auch die in § 22 Absatz 2 genannten Maßnahmen der Wahrung des Berufsgeheimnisses dienen.

Die Verarbeitung besonderer Kategorien personenbezogener nach Absatz 1 Nummer 2 erfordert zusätzlich eine Interessensabwägung, wie dies Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 vorsieht, indem die Verarbeitung in einem angemessenen Verhältnis zu dem verfolgten Zweck stehen und den Wesensgehalt des Rechts auf Datenschutz wahren muss.

Absatz 1 Nummer 1 Buchstabe b entspricht im wesentlichen § 13 Absatz 2 Nummer 7 und § 28 Absatz 7 BDSG a. F. und setzt Artikel 9 Absatz 2 Buchstabe h der Verordnung (EU) 2016/679 um. Auf eine explizite Nennung der Arbeitsmedizin wird verzichtet, da der Begriff der Gesundheitsvorsorge auch die arbeitsmedizinische Vorsorge beinhaltet. In Deutschland gibt es im Übrigen keine Verarbeitung besonderer Kategorien personenbezogener Daten zu Zwecken besonderer Facharztrichtungen, zum Beispiel zum Zweck der Arbeitsmedizin. Die Verarbeitung erfolgt jeweils entsprechend den inhaltlichen Zwecken, die sich aus Buchstabe b oder dem bereichsspezifischen Recht ergeben.

Mit der gewählten Formulierung wird klargestellt, dass ein Vertrag zwischen einem Patienten und einem Angehörigen eines Gesundheitsberufs, also der Behandlungsvertrag gemäß §§ 630a ff. BGB, gemeint ist. Daher findet die Regelung im Bereich der Humanmedizin für (Zahn-)Ärzte, Psychologische Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten Anwendung. Darüber hinaus werden vom Behandlungsvertrag auch Angehörige anderer Heilberufe, deren Ausbildung nach Artikel 74 Absatz 1 Nummer 19 des Grundgesetzes durch Bundesgesetz (Hebammen, Masseure und medizinische Bademeister, Ergotherapeuten, Logopäden, Physiotherapeuten u. a.) geregelt ist, oder Heilpraktiker erfasst.

Soweit es nach § 22 Absatz 1 Nummer 1 b) zulässig ist, dass „diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal dem Berufsgeheimnis unterliegt" sind auch die Erfüllungsgehilfen der genannten Gesundheits- und Heilberufe erfasst.

Absatz 1 Nummer 2 Buchstaben a bis d entsprechen im wesentlichen § 13 Absatz 1 Nummern 1, 5, 6 und 9 BDSG a. F. Ein erhebliches öffentliches Interesse nach Absatz 1 Nummer 2 Buchstabe a ist insbesondere in den Fällen anzunehmen, in denen biometrische Daten zu Zwecken der eindeutigen Identifikation Betroffener verarbeitet werden.

Absatz 2 Satz 1 und 2 setzt das Erfordernis aus Artikel 9 Absatz 2 Buchstabe b, g und i der Verordnung (EU) 2016/679 um, „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“ bzw. „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ vorzusehen. Die in Absatz 2 Satz 2 aufgeführten Maßnahmen treffen jeden Verantwortlichen und damit auch jeden, der besondere Kategorien personenbezogener Daten verarbeitet.

Die in Artikel 9 Absatz 2 Buchstabe h der Verordnung (EU) 2016/679 unter Bezugnahme auf den Artikel 9 Absatz 3 der Verordnung (EU) 2016/679 geforderten besonderen Garantien sind unmittelbar durch Absatz 1 Nummer 1 Buchstabe b umgesetzt und werden daher mit Absatz 2 Satz 3 von Absatz 2 ausgenommen.

Zu § 23 (Verarbeitung zu anderen Zwecken durch öffentliche Stellen)

Die Vorschrift schafft für öffentliche Stellen im Rahmen der jeweiligen Aufgabenerfüllung eine nationale Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch denselben Verarbeiter zu einem anderen Zweck als zu demjenigen, zu dem er sie ursprünglich erhoben hat (Weiterverarbeitung). Soweit eine der tatbestandlichen Voraussetzungen nach Absatz 1 erfüllt ist, kann die Weiterverarbeitung personenbezogener Daten durch öffentliche Stellen auf diese Vorschrift gestützt werden. Dies gilt unabhängig davon, ob die Zwecke der Weiterverarbeitung mit den Zwecken, für die die Daten ursprünglich erhoben wurden, nach Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 vereinbar sind.

Absatz 2 stellt für die Weiterverarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 klar, dass neben dem Vorliegen einer der tatbestandlichen Voraussetzungen des Absatzes 1 auch ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 vorliegen muss.

Mit der Vorschrift wird von dem durch die Verordnung (EU) 2016/679 eröffneten Regelungsspielraum Gebrauch gemacht, wonach die Mitgliedstaaten nationale Regelungen in Fällen, in denen der Zweck der Weiterverarbeitung nicht mit dem ursprünglichen Zweck vereinbar ist, erlassen dürfen, soweit die nationale Regelung eine „in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt".

Die Vorschrift orientiert sich an den Regelungen des § 13 Absatz 2 und des § 14 Absatz 2 bis 5 BDSG a. F.

Zu § 24 (Verarbeitung zu anderen Zwecken durch nichtöffentliche Stellen)

Die Vorschrift schafft eine nationale Rechtsgrundlage für die Weiterverarbeitung personenbezogener Daten durch nichtöffentliche Stellen. Soweit eine der tatbestandlichen Voraussetzungen nach Absatz 1 erfüllt ist, kann die Weiterverarbeitung personenbezogener Datendurch die nichtöffentliche Stelle auf diese Vorschrift gestützt werden unabhängig davon, ob die Zwecke der Weiterverarbeitung mit den ursprünglichen Zwecken, für die die Daten ursprünglich erhoben wurden, nach Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 vereinbar sind.

Absatz 2 stellt für die Weiterverarbeitung besonderer Kategorien personenbezogener Daten klar, dass neben dem Vorliegen einer der tatbestandlichen Voraussetzungen des Absatzes 1 auch ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 muss.

Mit der Vorschrift wird von dem durch die Verordnung (EU) 2016/679 eröffneten Regelungsspielraum Gebrauch gemacht, wonach die Mitgliedstaaten nationale Regelungen in Fällen, in denen der Zweck der Weiterverarbeitung nicht mit dem ursprünglichen Zweck vereinbar ist, erlassen dürfen, soweit die nationale Regelung eine „ in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 genannten Ziele darstellt".

Die Vorschrift orientiert sich an den Regelungen der § 28 Absatz 2 Nummer 2 Buchstabe b, § 28 Absatz 2 i. V. m. Absatz 1 Nummer 2 sowie § 28 Absatz 8 Satz 1 i. V. m. Absatz 6 Nummern 1 bis 3 und Absatz 7 Satz 2 BDSG a. F.

Zu § 25 (Datenübermittlungen durch öffentliche Stellen)

Die Vorschrift führt den präzisen Ansatz der §§ 15, 16 BDSG a. F. zur Datenübermittlung durch öffentliche Stellen fort und trägt damit dem strengen Gesetzesvorbehalt Rechnung. Die Vorschrift schafft materiell eine nationale Rechtsgrundlage für die Übermittlung personenbezogener Daten durch öffentliche Stellen soweit diese zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, erfolgt. Die Norm findet auch auf den Fall Anwendung, in denen eine öffentliche Stelle Daten, die sie ursprünglich zu Zwecken nach § 45 erhoben hat, an einen Dritten übermittelt, der die Daten zu Zwecken der Verordnung (EU) 2016/679 verarbeiten möchte.

Absatz 1 regelt die tatbestandlichen Voraussetzungen der Datenübermittlung an öffentliche Stellen. Die Regelung erfasst Datenübermittlungen, soweit diese zur Aufgabenerfüllung erforderlich sind. Eine Übermittlung ist gemäß dieser Vorschrift zulässig, wenn die Voraussetzungen für eine Verarbeitung zu einem anderen Zweck nach § 23 vorliegen. Die Regelung entspricht § 15 Absatz 1 und 3 BDSG a. F.

Absatz 2 regelt die tatbestandlichen Voraussetzungen der Datenübermittlung an nichtöffentliche Stellen. Die Regelung entspricht § 16 Absatz 1 und 4 BDSG a. F. Die bisher in § 16 Absatz 3 BDSG a. F. normierten Informationspflichten ergeben sich unmittelbar aus Artikel 13 Absatz 3 bzw. Artikel 14 Absatz 4 der Verordnung (EU) 2016/679.

Absatz 3 stellt für die Übermittlung besonderer Kategorien personenbezogener Daten klar, dass neben dem Vorliegen einer der tatbestandlichen Voraussetzungen der Absätze 1 oder 2 auch ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 Absatz 1 vorliegen muss.

Zu § 26 (Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses)

Die Öffnungsklausel des Artikels 88 der Verordnung (EU) 2016/679 lässt nationale Regelungen zur Datenverarbeitung im Beschäftigungskontext zu. Mit § 26 hat der Gesetzgeber hiervon Gebrauch gemacht. § 26 führt die

spezialgesetzliche Regelung des § 32 BDSG a. F. fort. Der Wortlaut ist an die Terminologie der Verordnung (EU) 2016/679 angepasst. Der Gesetzgeber behält sich vor, Fragen des Datenschutzes im Beschäftigungsverhältnis innerhalb dieser Vorschrift oder im Rahmen eines gesonderten Gesetzes konkretisierend bestimmte Grundsätze, die im Rahmen der Rechtsprechung zum geltenden Recht bereits angelegt sind, zu regeln. Dies gilt insbesondere für das Fragerecht bei der Begründung eines Beschäftigungsverhältnisses, den expliziten Ausschluss von heimlichen Kontrollen im Beschäftigungsverhältnis, die Begrenzung der Lokalisierung von Beschäftigten sowie den Ausschluss von umfassenden Bewegungsprofilen, den Ausschluss von Dauerüberwachungen und die Verwendung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken.

Absatz 1 regelt – wie bisher § 32 Absatz 1 BDSG a. F. –, zu welchen Zwecken und unter welchen Voraussetzungen personenbezogene Daten vor, im und nach dem Beschäftigungsverhältnis verarbeitet werden dürfen, wenn dies zum Zweck des Beschäftigungsverhältnisses erforderlich ist.

Im Rahmen der Erforderlichkeitsprüfung sind die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz abzuwägen. Dabei sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt.

Absatz 1 Satz 1 in Verbindung mit Absatz 5 setzt auch Artikel 10 der Verordnung (EU) 2016/679 um, der es den Mitgliedsstaaten ermöglicht, die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln im Beschäftigungskontext zuzulassen. Der Arbeitgeber kann auf diese Weise beispielsweise sicherstellen, dass die Beschäftigten keinem Verbot nach § 25 Jugendarbeitsschutzgesetz unterliegen und mit der Beaufsichtigung, Anweisung oder Ausbildung von Jugendlichen beauftragt werden dürfen.

Ebenfalls von Satz 1 umfasst ist die Verarbeitung personenbezogener Daten zum Zweck des Beschäftigungsverhältnisses, wenn dies zur Ausübung oder Erfüllung der sich aus Gesetz oder Kollektivvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Dies wird durch die Ergänzung am Ende des Satzes 1 gegenüber der bisherigen Fassung des § 32 Absatz 1 BDSG a. F. klargestellt. Unter Kollektivvereinbarungen sind Tarifverträge, Betriebsvereinbarungen und Dienstvereinbarungen zu verstehen (siehe Erwägungsgrund 155 der Verordnung (EU) 2016/679).

Satz 2 benennt die Voraussetzungen für die Verarbeitung personenbezogener Daten von Beschäftigten zur Aufdeckung von Straftaten, die im Beschäftigungsverhältnis begangen worden sind.

Absatz 2 trägt der Besonderheit des Beschäftigungsverhältnisses als Abhängigkeitsverhältnis und der daraus resultierenden Situation der Beschäftigten Rechnung. Es handelt sich ebenfalls um eine spezifischere Vorschrift im Sinne von Artikel 88 Absatz 1 der Verordnung (EU) 2016/679. Nach Erwägungsgrund 155 der Verordnung (EU) 2016/679 können insbesondere Vorschriften über die Bedingungen erlassen werden, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage einer Einwilligung der Beschäftigten verarbeitet werden dürfen.

Bei der Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, sind insbesondere die im Beschäftigungsverhältnis grundsätzlich bestehende Abhängigkeit der oder des Beschäftigten vom Arbeitgeber und die Umstände des Einzelfalls zu berücksichtigen. Neben der Art des verarbeiteten Datums und der Eingriffstiefe ist zum Beispiel auch der Zeitpunkt der Einwilligungserteilung maßgebend. Vor Abschluss eines (Arbeits-)Vertrages werden Beschäftigte regelmäßig einer größeren Drucksituation ausgesetzt sein, eine Einwilligung in eine Datenverarbeitung zu erteilen. Satz 2 legt fest, dass eine freiwillige Einwilligung insbesondere vorliegen kann, wenn die oder der Beschäftigte infolge der Datenverarbeitung einen rechtlichen oder wirtschaftlichen Vorteil erlangt oder Arbeitgeber und Beschäftigter gleichgerichtete Interessen verfolgen. Die Gewährung eines Vorteils liegt beispielsweise in der Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder der Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen. Auch die Verfolgung gleichgerichteter Interessen spricht für die Freiwilligkeit einer Einwilligung. Hierzu kann etwa die Aufnahme von Name und Geburtsdatum in eine Geburtstagsliste oder die Nutzung von Fotos für das Intranet zählen, bei der Arbeitgeber und Beschäftigter im Sinne eines betrieblichen Miteinanders zusammenwirken.

Als formelle Voraussetzung einer Einwilligung ist grundsätzlich die Schriftform angeordnet, um die informationelle Selbstbestimmung der betroffenen Beschäftigten abzusichern. Damit wird die Nachweispflicht des Arbeitgebers im Sinne von Artikel 7 Absatz 1 der Verordnung (EU) 2016/679 konkretisiert. Hinzu kommt die Pflicht

des Arbeitgebers zur Aufklärung in Textform über den Zweck der Datenverarbeitung und den jederzeit möglichen Widerruf durch den Beschäftigten sowie dessen Folgen nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679.

Absatz 3 dient (neben § 22 Absatz 1 Nummer 1 Buchstabe a) der Umsetzung von Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679. Im Einklang mit der Verordnung ist eine Verarbeitung besonderer Kategorien personenbezogener Daten zu Beschäftigungszwecken zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses kann auch die Verarbeitung von Daten zur Beurteilung der Arbeitsfähigkeit einschließen. Die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten für andere Zwecke bleibt unberührt; zum Beispiel richtet sich diese im Fall der Verarbeitung zu Zwecken der Gesundheitsvorsorge nach § 22 Absatz 1 Nummer 1 Buchstabe b. Sollte eine Verarbeitung zugleich mehreren Zwecken dienen, gilt für den jeweiligen Zweck die jeweils einschlägige Verarbeitungsgrundlage. Neben der Verhältnismäßigkeitsprüfung im Rahmen der Erforderlichkeit darf wie bisher nach § 28 Absatz 6 BDSG a. F. kein Grund zu der Annahme bestehen, dass die schutzwürdigen Interessen der Betroffenen die Interessen der Verantwortlichen an der Verarbeitung überwiegen. Die Vorschriften des Absatzes 2 gelten auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten, wie z.B. von Gesundheitsdaten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. An die Freiwilligkeit einer Einwilligung in die Datenverarbeitung besonderer Kategorien personenbezogener Daten sind strenge Anforderungen zu stellen. Nach Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 muss die nationale Regelung geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen. Dem trägt der Verweis auf § 22 Absatz 2 Rechnung.

Absatz 4 bestimmt, dass die Verarbeitung personenbezogener Beschäftigtendaten aufgrund von Kollektivvereinbarungen zulässig ist. Artikel 88 Absatz 1 der Verordnung (EU) 2016/679 ermöglicht es, spezifischere Regelungen zum Datenschutz im Beschäftigungskontext in Kollektivvereinbarungen zu treffen. Hinsichtlich besonderer Kategorien personenbezogener Daten beruht Absatz 4 auf Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679. Besonders Betriebs- und Dienstvereinbarungen sind nach bisherigem Recht wichtige Regelungsinstrumente im Bereich des Beschäftigtendatenschutzes. Absatz 4 stellt deshalb in Umsetzung des Artikel 88 Absatz 1 der Verordnung (EU) 2016/679 klar, dass Tarifverträge, Betriebsvereinbarungen oder Dienstvereinbarungen weiterhin die Rechtsgrundlage für Regelungen zum Beschäftigtendatenschutz bilden können. Sie sollen den Verhandlungsparteien der Kollektivvereinbarungen die Ausgestaltung eines auf die betrieblichen Bedürfnisse zugeschnittenen Beschäftigtendatenschutzes ermöglichen. Dabei steht ihnen ein Ermessensspielraum im Rahmen des geltenden Rechts einschließlich der Verordnung (EU) 2016/679 zu; Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 ist zu beachten. Damit wird auch den Anforderungen des Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 bei der Verarbeitung besonderer Kategorien personenbezogener Daten Rechnung getragen.

Nach Absatz 5 muss der Verantwortliche geeignete Maßnahmen zur Wahrung der Grundrechte und Interessen des Beschäftigten vorsehen. Beispielsweise muss bei der Datenverarbeitung sichergestellt sein, dass sie auf rechtmäßige Weise, nach Treu und Glauben und in einer für den Beschäftigten nachvollziehbaren Weise erfolgt. Die Daten werden in einer Form gespeichert, die die Identifizierung des Beschäftigten nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Der Verantwortliche stellt sicher, dass die Verarbeitung in einer Weise erfolgt, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung. Er trifft sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen, die darauf ausgelegt sind, die Datenschutzgrundsätze wie etwa die Datenminimierung wirksam umzusetzen. Der Verantwortliche unternimmt Schritte um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur aufgrund seiner Anweisung verarbeiten, es sei denn, diese sind rechtlich zur Verarbeitung verpflichtet. Damit wird insbesondere auch das Erfordernis aus Artikel 10 der Verordnung (EU) 2016/679 umgesetzt, geeignete Garantien für die Rechte und Freiheiten der Beschäftigten vorzusehen.

Absatz 6 entspricht dem § 32 Absatz 3 BDSG a. F. und stellt klar, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt bleiben.

Absatz 7 legt fest, dass die Absätze 1 bis 6 im Beschäftigungsverhältnis auch gelten, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Er geht dabei von der Beschreibung des Anwendungsbereichs in Artikel 2 Absatz 1 der Verordnung (EU) 2016/679 aus und führt § 32 Absatz 2 BDSG a. F. fort.

Absatz 8 übernimmt weitgehend die bisher in § 3 Absatz 11 BDSG a. F. vorgesehenen Begriffsbestimmungen. In Nummer 1 wird klargestellt, dass Leiharbeitnehmer nicht nur im Verhältnis zum Verleiher, sondern auch im Verhältnis zum Entleiher als Beschäftigte gelten. In Nummer 5 wurden die Ausführungen zum Jugendfreiwilligendienstegesetz redaktionell überarbeitet und um das Bundesfreiwilligendienstgesetz ergänzt.

Zu § 27 (Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken)

Mit § 27 Absatz 1, der für die öffentliche und private Forschung durch öffentliche und nichtöffentliche Stellen gilt, wird von der Ermächtigung aus Artikel 9 Absatz 2 Buchstabe j der Verordnung (EU) 2016/679 Gebrauch gemacht. Nach Artikel 9 Absatz 1 Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich untersagt. Artikel 9 Absatz 2 der Verordnung sieht Ausnahmen von diesem Verbot vor. Die Ausnahmen gelten teilweise unmittelbar aus der Verordnung (z. B. die ausdrückliche Einwilligung nach Artikel 9 Absatz 2 Buchstabe a. Mit § 27 Absatz 1 wird darüber hinaus auf Basis von Artikel 9 Absatz 2 Buchstabe j eine zusätzliche Regelung im nationalen Recht für die Verarbeitung besonderer Kategorien personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken geschaffen. Die Verarbeitung nach § 27 Absatz 1 setzt dabei das Vorliegen einer Rechtsgrundlage nach Artikel 6 Absatz 1 der Verordnung (EU) 2016/679 voraus (z. B. gemäß Artikel 6 Absatz 1 Buchstabe f eines berechtigten Interesses des Verantwortlichen).

Artikel 9 Absatz 2 Buchstabe j der Verordnung (EU) 2016/679 erfordert, dass eine Forschungsklausel in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht. Dem trägt der Verweis auf § 22 Absatz 2 Satz 2 Rechnung.

§ 27 Absatz 1 gilt nur für die Verarbeitung von Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679. Die Verarbeitung von nicht unter Artikel 9 fallenden Daten richtet sich entweder unmittelbar nach der Verordnung (EU) 2016/679 (insbesondere Artikel 6 Absatz 1) oder nach im Einklang mit der Verordnung erlassenen Rechtsgrundlagen des Unions- oder nationalen Gesetzgebers. Nationale Vorschriften finden sich in diesem Gesetz oder im bereichsspezifischen Recht.

Für die Weiterverarbeitung personenbezogener Daten durch öffentliche und nichtöffentliche Stellen gilt: Nach Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 gilt eine Weiterverarbeitung für wissenschaftliche oder historische Forschungszwecke und für statistische Zwecke nicht als unvereinbar mit den ursprünglichen Zwecken. Da diese Zwecke bei der Weiterverarbeitung kompatibel mit dem Zweck der Erstverarbeitung sind, kann sich der Verantwortliche als Rechtsgrundlage erneut auf die Rechtsgrundlage stützen, die bereits für die Erstverarbeitung galt.

Dies trifft auch auf die Weiterverarbeitung besonderer Kategorien personenbezogener Daten zu, für die § 27 Absatz 1 als Ausnahmetatbestand von dem Verbot des Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 gilt. §§ 23, 24 finden insoweit keine Anwendung. Entsprechendes gilt für die Übermittlung besonderer Kategorien von Daten durch öffentliche Stellen zu wissenschaftlichen oder historischen und statistischen Forschungszwecken; § 25 findet insoweit keine Anwendung.

§ 27 Absatz 2 Satz 1 schränkt unter Ausnutzung der Öffnungsklausel des Artikel 89 Absatz 2 der Verordnung (EU) 2016/679 die Rechte nach den Artikeln 15, 16, 18 und 21 der Verordnung (EU) 2016/679 ein. Im Sinne des Absatzes 2 Satz 1 kann die Verwirklichung des Forschungszwecks in bestimmten Einzelfällen ohne Einschränkungen des Auskunftsrechts aus Artikel 15 der Verordnung (EU) 2016/679 z. B. dann unmöglich sein, wenn die zuständige Ethikkommission zum Schutz der betroffenen Person eine Durchführung des Projekts andernfalls untersagen würde. Darüber hinaus schränkt Absatz 2 Satz 2 in Anlehnung an § 33 Absatz 2 Satz 1 Nummer 5 i. V. m. § 34 Absatz 7 sowie § 19a Absatz 2 Nummer 2 BDSG a. F. das Auskunftsrecht für die Fälle unverhältnismäßigen Aufwands unter Ausnutzung der Öffnungsklausel des Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679 ein. Das kann beispielsweise dann der Fall sein, wenn ein Forschungsvorhaben mit besonders großen

Datenmengen arbeitet.. Die Einschränkung der Betroffenenrechte in Absatz 2 gilt für alle Kategorien personenbezogener Daten.

Absätze 3 und 4 sind § 40 Absatz 2 und 3 BDSG a. F. entlehnt.

Soweit spezialgesetzliche Regelungen zur Datenverarbeitung aus dem bereichsspezifischen Recht anzuwenden sind, gehen sie § 27 vor (§ 1 Absatz 2 BDSG). Solche spezialgesetzlichen Regelungen finden sich derzeit etwa in den Sozialgesetzbüchern oder in medizinrechtlichen Gesetzen (z. B. Arzneimittelgesetz, Gendiagnostikgesetz, Transplantationsgesetz).

Zu § 28 (Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken)

§ 28 gilt für die Verarbeitung personenbezogener Daten durch öffentliche und nichtöffentliche Stellen. Er bezieht sich sowohl auf öffentliches als auch privates Archivgut.

Mit § 28 Absatz 1 wird von der Ermächtigung aus Artikel 9 Absatz 2 Buchstabe j der Verordnung (EU) 2016/679 Gebrauch gemacht. Nach Artikel 9 Absatz 1 Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich untersagt. Artikel 9 Absatz 2 der Verordnung sieht Ausnahmen von diesem Verbot vor. Die Ausnahmen gelten teilweise unmittelbar aus der Verordnung (z.B. die ausdrückliche Einwilligung nach Artikel 9 Absatz 2 Buchstabe a). Mit § 28 Absatz 1 wird darüber hinaus auf Basis von Artikel 9 Absatz 2 Buchstabe j im nationalen Recht ein zusätzlicher Ausnahmetatbestand für die Verarbeitung besonderer Kategorien personenbezogener Daten geschaffen. Der Verweis in Absatz 1 auf den Beispielskatalog des § 22 Absatz 2 Satz 2 hat nicht zur Folge, dass die Anwendung mindestens einer genannten Maßnahme bei der Verarbeitung besonderer Kategorien von Daten zu im öffentlichen Interesse liegenden Archivzwecken zwingend ist. Vielmehr können auch andere angemessene und spezifische Maßnahmen getroffen werden.

§ 28 Absatz 1 gilt nur für die Verarbeitung von Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679. Die Verarbeitung von nicht unter Artikel 9 fallenden Daten richtet sich entweder unmittelbar nach der Verordnung (EU) 2016/679 (insbesondere Artikel 6 Ab-satz 1) oder nach im Einklang mit der Verordnung erlassenen Rechtsgrundlagen des Unions- oder nationalen Gesetzgebers. Nationale Vorschriften finden sich in diesem Gesetz oder im bereichsspezifischen Recht.

Für die Weiterverarbeitung gilt: Nach Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 gilt eine Weiterverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken nicht als unvereinbar mit den ursprünglichen Zwecken. Daher kann sich der Verantwortliche hinsichtlich der Rechtsgrundlage für die Weiterverarbeitung erneut auf die Rechtsgrundlage stützen, die bereits für die Erstverarbeitung galt. §§ 23, 24 und 25 finden keine Anwendung. Will der Verantwortliche aber besondere Kategorien von Daten weiterverarbeiten, benötigt er nicht nur eine Rechtsgrundlage, sondern auch einen Ausnahmetatbestand von dem Verbot des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679. Er muss mithin auch bei der Weiterverarbeitung § 28 Absatz 1 beachten.

In den Absätzen 2 bis 4 werden unter Ausnutzung der Öffnungsklausel des Artikels 89 Absatz 3 der Verordnung (EU) 2016/679 die Rechte gemäß der Artikel 15, 16, 18, 20 und 21 der Verordnung (EU) 2016/679 eingeschränkt. Die Ausnahme gemäß Absatz 2 bezieht sich auf sämtliche durch Artikel 15 der Verordnung (EU) 2016/679 gewährten Rechte, insbesondere auch auf das Recht auf Erhalt einer Kopie. Die Absätze 2 bis 4 gelten für die Verarbeitung sämtlicher personenbezogenen Daten, einschließlich besonderer Kategorien personenbezogener Daten.

Zu § 29 (Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten)

Auf der Grundlage der Öffnungsklausel des Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679 beschränkt Absatz 1 wie bisher nach dem BDSG a. F. gegenüber Geheimnisträgern das Recht auf Information (§ 19a Absatz 3 i. V. m. § 19 Absatz 4 Nummer 3; § 33 Absatz 2 Satz 1 Nummer 3 BDSG a. F.) und Auskunft § 19 Absatz 4 Nummer 3; § 34 Absatz 7 BDSG a. F. Satz 2 beschränkt die Betroffenenrechte auch für die Fälle, in denen Informationen „nach einer Rechtsvorschrift“ geheim gehalten werden müssen; Satz 1 bezieht sich nicht auf diese nach Rechtsvorschriften bestehenden Geheimhaltungspflichten, da die Informationspflicht hier bereits unmittelbar durch Artikel 14 Absatz 5 Buchstabe d der Verordnung (EU) 2016/679 beschränkt wird. Sätze 3 und 4 beziehen sich auf eine Beschränkung der Benachrichtigungspflicht nach Artikel 34 der Verordnung (EU) 2016/679.

Absatz 2 dient dem Schutz der ungehinderten Kommunikation zwischen Mandant und Berufsgeheimnisträger. Wirtschaftsprüfer und Rechtsanwälte werden oftmals nicht (nur) mit der Verfolgung von Rechtsansprüchen (vgl. hierzu § 32 Absatz 1 Nummer 4), sondern mit vielfältigen Beratungsdienstleistungen (Steuerberatung; Begleitung

von Unternehmenstransaktionen; Gutachter- und Sachverständigentätigkeit etc.) beauftragt. Es widerspräche dem besonderen Schutz des Mandatsverhältnisses, wenn der Mandant in jedem Fall sämtliche durch die Datenübermittlung an den Berufsgeheimnisträger betroffenen Personen über die Zwecke der Datenübermittlung, die Identität der beauftragten Berufsgeheimnisträger etc. informieren müsste. Durch die in Absatz 2 letzter Halbsatz eingefügte Abwägungsklausel wird den Rechten der Betroffenen angemessen Rechnung getragen. Die Einschränkung der Informationspflicht beruht auf der Öffnungsklausel des Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679.

Absatz 3 Satz 1 macht von der Öffnungsklausel des Artikels 90 der Verordnung (EU) 2016/679 Gebrauch, ihr entspricht Erwägungsgrund 164 der Verordnung. Nach Artikel 58 Absatz 1 Buchstaben e und f der Verordnung (EU) 2016/679 haben die Aufsichtsbehörden die Befugnis, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu erhalten zu allen für die Erfüllung ihrer Aufgaben notwendigen personenbezogenen Daten und Informationen sowie zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte. Artikel 90 Absatz 1 Verordnung (EU) 2016/679 eröffnet den Mitgliedstaaten die Möglichkeit, die Befugnisse der Aufsichtsbehörden im Sinne des Artikels 58 Absatz 1 Buchstaben e und f gegenüber Geheimnisträgern zu regeln. Mit Absatz 3 Satz 1 wird diese Möglichkeit insbesondere dergestalt umgesetzt, dass eine Aufsichtsbehörde entgegen Artikel 58 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 dann keinen Zugang zu Daten und Informationen hat, soweit dadurch die Geheimhaltungspflicht verletzt würde. Ohne eine Einschränkung der Befugnisse der Aufsichtsbehörden käme es zu einer Kollision mit Pflichten des Geheimnisträgers. Gerade bei den freien Berufen schützt die berufsrechtliche Schweigepflicht das Vertrauen des Mandanten und der Öffentlichkeit in den Berufsstand. Nach bundesverfassungsgerichtlicher Rechtsprechung darf das Mandatsverhältnis nicht mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet sein (vgl. BVerfG, Urteil vom 12. April 2005 – 2 BvR 1027/02). Absatz 3 Satz 2 verlängert die Geheimhaltungspflicht auf die Aufsichtsbehörde. Berufsgeheimnisträger bedienen sich vermehrt externer IT-Dienstleister und verpflichten diese als Auftragsverarbeiter vertraglich zur Verschwiegenheit. Um zu vermeiden, dass die Auftragsverarbeiter vertragsbrüchig werden, wenn sie die ihnen anvertrauten Daten gegenüber den Aufsichtsbehörden offenlegen müssten, umfasst Absatz 3 auch den Auftragsverarbeiter.

Zu § 30 (Verbraucherkredite)

Die Vorschrift entspricht § 29 Absatz 6 und 7 BDSG a. F. Mit diesen Absätzen war Artikel 9 der Verbraucherkreditrichtlinie 2008/48/EG umgesetzt worden. Um der Umsetzungspflicht gemäß dieser Richtlinie weiterhin nachzukommen, ist § 30 erforderlich.

Zu § 31 (Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften)

Die Vorschrift erhält den materiellen Schutzstandard der §§ 28a und 28b BDSG a. F. Die in der bisherigen Fassung des BDSG enthaltenen Regelungen zu Auskunfteien und Scoring dienen dem Schutz des Wirtschaftsverkehrs und besitzen für Betroffene wie auch für die Wirtschaft eine überragende Bedeutung. Verbraucher vor Überschuldung zu schützen, liegt sowohl im Interesse der Verbraucher selbst als auch der Wirtschaft. Die Ermittlung der Kreditwürdigkeit und die Erteilung von Bonitätsauskünften bilden das Fundament des deutschen Kreditwesens und damit auch der Funktionsfähigkeit der Wirtschaft.

Die Regelung übernimmt die in § 28b BDSG a. F. festgelegten Voraussetzungen und konkretisiert, welche Voraussetzungen ein von einer Auskunftei ermittelter Score-Wert im Hinblick auf sog. Negativ-Merkmale erfüllen muss, damit er im Wirtschaftsverkehr verwendet werden darf. Für die Verwendung des Score-Wertes wird auf die Kriterien der derzeitigen § 28a Absatz 1 und § 28b zurückgegriffen, die die im Wirtschaftsleben bedeutsame Tätigkeit von Auskunfteien sowie die Ermittlung von Score-Werten grundsätzlich ermöglichen. Die Kriterien des § 28a Absatz 1 und des § 28b begrenzen die Zulässigkeit der Ermittlung von Score-Werten in bestimmten Fällen und schaffen so einen angemessenen Ausgleich der widerstreitenden Interessen, beispielsweise dadurch, dass Auskunfteien offene Forderungen nur dann gemeldet werden dürfen und dort verarbeitet werden können, wenn sie unbestritten oder tituliert sind. § 29a Absatz 2 BDSG lässt die Vorschriften des allgemeinen Datenschutzrechts über die Zulässigkeit der Verarbeitung von personenbezogenen Daten unberührt. Dies betrifft etwa unter anderem auch die Übermittlung und Verwendung für die Ermittlung von Wahrscheinlichkeitswerten von personenbezogenen Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses eines Geschäfts mit finanziellem Ausfallrisiko (Positivdaten).

Insoweit wird für alle Beteiligten Sicherheit in der Weise geschaffen, dass Scoringverfahren und Kreditinformationssysteme mit der Einmeldung von Positiv- und Negativdaten, die z. B. durch Kreditinstitute, Finanzdienstleistungsunternehmen, Zahlungsinstitute, Telekommunikations-, Handels-, Energieversorgungs- und Versicherungsunternehmen oder Leasinggesellschaften erfolgt, prinzipiell weiter zulässig bleiben. Sie werden nach wie vor als wichtige Voraussetzungen für das Wirtschaftsleben angesehen.

Zu §§ 32 bis 37 (Kapitel 2 – Rechte der betroffenen Person)

Artikel 23 der Verordnung (EU) 2016/679 sieht vor, dass die Rechte und Pflichten gemäß den Artikeln 12 bis 22 und Artikel 34 sowie die in Artikel 5 geregelten Grundsätze für die Verarbeitung personenbezogener Daten, sofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, durch Rechtsvorschriften der Union oder der Mitgliedstaaten beschränkt werden können.

Die Beschränkung muss den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen, um die in Artikel 23 Absatz 1 Buchstaben a bis j aufgezählten Ziele sicherzustellen.

Artikel 23 der Verordnung (EU) 2016/679 verlangt besondere Maßnahmen zum Schutz der Grundrechte und Grundfreiheiten der von der Beschränkung betroffenen Person. Insbesondere muss gemäß Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 jede Gesetzgebungsmaßnahme „insbesondere gegebenenfalls spezifische Vorschriften“ zumindest in Bezug auf die in Artikel 23 Absatz 2 der Verordnung (EU) 2016/670 Buchstaben a bis h aufgezählten Maßnahmen enthalten.

Die in Kapitel 2 vorgenommenen Einschränkungen der Betroffenenrechte und Pflichten des Verantwortlichen und Auftragsverarbeiters ergänzen die in der Verordnung (EU) 2016/679 unmittelbar vorgesehenen Ausnahmen.

Die Beschränkungen der Betroffenenrechte in Kapitel 2 finden auch Anwendung auf die in Artikel 89 der Verordnung (EU) 2016/679 geregelte Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken. Zwar bestimmt Artikel 89 Absatz 2 und 3, dass bei einer Verarbeitung zu den dort genannten Forschungs- und statistischen Zwecken Mitgliedstaaten insoweit Ausnahmen von den Rechten gemäß der Artikel 15, 16, 18 und 21 sowie bei der Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken zusätzlich Artikel 19 und 20 vorsehen können, als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind. Eine Beschränkung der Betroffenenrechte muss jedoch nicht nur nach Artikel 89 Absatz 2 und 3, sondern auch nach Artikel 23 der Verordnung (EU) 2016/679 möglich sein, da die Verarbeitung zu den in Artikel 89 genannten Zwecken andernfalls gegenüber sonstigen Verarbeitungen schlechter gestellt wäre, obwohl der Verordnungsgeber die Verarbeitung zu Archiv-, Forschungs- und Statistikzwecken ausweislich der Sonderreglung in Kapitel IX der Verordnung (EU) 2016/679 privilegieren wollte.

Zu § 32 (Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person)

Die in Absatz 1 vorgesehene Beschränkung der Informationspflicht gilt nur für die in Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 vorgesehene Fallgruppe, dass der Verantwortliche beabsichtigt, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die Daten bei der betroffenen Person erhoben wurden. Die Informationspflicht aus Artikel 13 Absatz 1 und 2 der Verordnung (EU) 2016/679 wird demgegenüber nicht beschränkt.

Die mit der Verordnung (EU) 2016/679 erstmals eingeführte (Folge-)Informationspflicht des Verantwortlichen bei beabsichtigter Zweckänderung findet im BDSG a. F. bislang keine Entsprechung. In dieser Konstellation besteht im Gegensatz zu der in Artikel 13 Absatz 1 und 2 der Verordnung (EU) 2016/679 vorgesehenen Informationspflicht zum Zeitpunkt der Erhebung der Daten typischerweise kein unmittelbarer Kontakt zwischen dem Verantwortlichen und der betroffenen Person.

In diesen Fällen kann sich die Information der betroffenen Person als unverhältnismäßig erweisen. Absatz 1 Nummer 1 sieht daher eine Ausnahme von der Informationspflicht nach Artikel 13 Absatz 3 der Verordnung (EU) 2016 vor, wenn und soweit die Erteilung der Information einen unverhältnismäßigen Aufwand erfordern würde und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere wegen des Zusammenhangs, in dem die Daten erhoben wurden, als gering anzusehen ist. Ein unver-

hältnismäßiger Aufwand kann beispielsweise vorliegen, wenn die Kontaktdaten des Betroffenen dem Verantwortlichen nicht bekannt und auch nicht ohne Weiteres zu ermitteln sind. Als Anhaltspunkte für die Beurteilung der Unverhältnismäßigkeit können die Anzahl der betroffenen Personen, das Alter der Daten oder das Bestehen geeigneter Garantien einbezogen werden (Erwägungsgrund 62 der Verordnung (EU) 2016/679). Ebenso ist die Art der zur Verfügung stehenden Kommunikationswege zu berücksichtigen.

Die Nummern 2 und 3 enthalten speziell für öffentliche Stellen geltende Einschränkungen der Informationspflicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben gefährden (Nummer 2) oder die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde (Nummer 3). Einschränkende Voraussetzung ist in beiden Fällen, dass die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.

Nummer 4 sieht eine Einschränkung zur Sicherstellung der Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor (Artikel 23 Absatz 1 Buchstabe j der Verordnung (EU) 2016/679).

Nummer 5 schützt die vertrauliche Übermittlung von Daten an öffentliche Stellen (Artikel 23 Absatz 1 Buchstabe e der Verordnung 2016/679). Erfasst sind beispielsweise Fallgruppen, in denen die Information der betroffenen Person über die Weiterverarbeitung zu einer Vereitelung oder ernsthaften Beeinträchtigung des – legitimen – Verarbeitungszwecks führen würde, etwa wenn die zuständige Strafverfolgungsbehörde über den Verdacht einer Straftat informiert werden soll.

Absatz 2 legt fest, dass der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person zu treffen hat, wenn eine Information der betroffenen Person nach Maßgabe des Absatzes 1 unterbleibt. Hierdurch werden die nach Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 erforderlichen Schutzmaßnahmen beachtet. Zu den geeigneten Maßnahmen zählt die Bereitstellung dieser Informationen für die Öffentlichkeit. Eine Veröffentlichung in allgemein zugänglicher Form kann etwa die Bereitstellung der Information auf einer allgemein zugänglichen Webseite des Verantwortlichen sein (Erwägungsgrund 58 Satz 2 der Verordnung (EU) 2016/679). Die Information hat in Entsprechung zu Artikel 12 Absatz 1 der Verordnung (EU) 2016/679 in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen.

Der Verantwortliche hat schriftlich zu fixieren, aus welchen Gründen er von einer Information abgesehen hat. Die Stichhaltigkeit der Gründe unterliegt der Kontrolle durch die zuständige Aufsichtsbehörde, die durch die Dokumentationspflicht ermöglicht wird. Die in Absatz 2 Satz 1 und 2 zum Schutz der berechtigten Interessen der betroffenen Person geforderten Maßnahmen des Verantwortlichen finden im Fall des Absatz 1 Nummer 4 und 5 keine Anwendung. Andernfalls könnten die in Satz 1 und 2 geforderten Maßnahmen zu einer Vereitelung oder ernsthaften Beeinträchtigung des – legitimen – Verarbeitungszwecks führen.

Absatz 3 bestimmt, dass der Verantwortliche die Information der betroffenen Person zeitnah nachzuholen hat, wenn die Ausschlussgründe des Absatzes 1 nur vorübergehend vorliegen.

Zu § 33 (Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden)

§ 33 Absatz 1 enthält in Ergänzung der in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 und § 29 Absatz 1 Satz 1 genannten Ausnahmen Einschränkungen der Informationspflicht des Verantwortlichen aus Artikel 14 Absatz 1, 2 und 4 der Verordnung (EU) 2016/679.

Absatz 1 Nummer 1, der nur für öffentliche Stellen gilt, ist eng angelehnt an die Ausnahmeregelungen des § 19a Absatz 3 i. V. m. § 19 Absatz 4 Nummer 1 und 2 BDSG a. F. Es wird auf die Begründung zu § 31 Absatz 1 Nummer 2 und 3 verwiesen.

Absatz 1 Nummer 2 gilt nur für nichtöffentliche Stellen. Nummer 2 Buchstabe a entspricht im Wesentlichen § 33 Absatz 2 Satz 1 Nummer 7b) BDSG a. F. Der Ausnahmetatbestand ist eng auszulegen; die Möglichkeit des Scheiterns einzelner Geschäfte des Verantwortlichen, etwa das Zustandekommen oder die Abwicklung eines Vertrags mit der betroffenen Person, begründen keine Ausnahme von der Informationspflicht. Notwendig ist vielmehr, dass die allgemein anerkannten Geschäftszwecke des Verantwortlichen insgesamt gefährdet werden. Für den Begriff „Geschäftszweck“ gilt dasselbe Verständnis wie bisher, die neu eingefügte Ergänzung „allgemein anerkannt“

dient der Eingrenzung. Einen Anwendungsfall können Datenverarbeitungen zur Verfolgung zivilrechtlicher Ansprüche darstellen (Artikel 23 Absatz 1 Buchstabe j der Verordnung (EU) 2016/679).

Absatz 1 Nummer 2 Buchstabe b ist an § 33 Absatz 2 Satz 1 Nummer 6 BDSG a. F. angelehnt. Die im konkreten Umfang (Artikel 23 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679) vorgesehene Beschränkung der Informationspflicht dient den Zielen der nationalen Sicherheit (Artikel 23 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679), der Landesverteidigung (Artikel 23 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679), der öffentlichen Sicherheit (Artikel 23 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679), der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (Artikel 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679) sowie sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder der Bundespublik Deutschland (Artikel 23 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679).

Absatz 2 entspricht § 32 Absatz 2 Satz 1 und 2. Auf die dortige Begründung wird verwiesen.

Absatz 3 betrifft den bislang in § 19a Absatz 3 i. V. m. § 19 Absatz 3 BDSG a. F. geregelten Fall der Informationserteilung bei Datenübermittlung durch öffentliche Stellen an die dort aufgeführten Behörden zu Zwecken der nationalen Sicherheit.

Zu § 34 (Auskunftsrecht der betroffenen Person)

§ 34 Absatz 1 enthält ergänzend zu den in § 27 Absatz 2, § 28 Absatz 2 und § 29 Absatz 1 Satz 2 genannten Ausnahmen Einschränkungen des Auskunftsrechts der betroffenen Person. Die Absätze 2 und 3 regeln, anknüpfend an die bisherige Regelung des § 19 Absatz 5 und 6 BDSG a. F., Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Person und weiten diese im Vergleich zur bisherigen Rechtslage aus.

Absatz 1 Nummer 1 verweist für das Auskunftsrecht auf die Beschränkungen des § 33 Absatz 1 und 3. Durch den Verweis werden die bislang bestehenden Einschränkungen des Auskunftsrechts der betroffenen Person aus § 19 Absatz 3 und 4 Nummer 1 und 2 sowie § 34 Absatz 7 i. V. m. § 33 Absatz 2 Satz 1 Nummer 6 und 7b BDSG a. F. modifiziert übernommen.

Absatz 1 Nummer 2 führt § 19 Absatz 2 und § 33 Absatz 2 Satz 1 Nummer 2 BDSG a. F. im Wesentlichen fort. In Erweiterung der bisherigen Rechtslage hat der Verantwortliche jedoch sicherzustellen, dass durch geeignete technische und organisatorische Maßnahmen eine Verwendung der Daten zu anderen Zwecken ausgeschlossen ist. Bei der Ermittlung des Aufwands hat der Verantwortliche die bestehenden technischen Möglichkeiten, gesperrte und archivierte Daten der betroffenen Person im Rahmen der Auskunftserteilung verfügbar zu machen, zu berücksichtigen. Werden die Daten ausschließlich aufgrund von Aufbewahrungsvorschriften gespeichert, ist die Verarbeitung der Daten einzuschränken (§ 35 Absatz 3).

Die Dokumentationspflicht und die Begründungspflicht nach Absatz 2 sind Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen im Sinne des Artikels 23 Absatz 2 Buchstaben c, d, g und h der Verordnung (EU) 2016/679. Hierdurch wird die betroffene Person in die Lage versetzt, die Ablehnung der Auskunftserteilung nachzuvollziehen und gegebenenfalls durch die zuständige Aufsichtsbehörde prüfen zu lassen. Ergänzend hierzu hat der Verantwortliche nach Artikel 12 Absatz 4 der Verordnung (EU) 2016/679 die betroffene Person auf die Möglichkeit der Beschwerde bei der zuständigen Aufsichtsbehörde und des gerichtlichen Rechtsschutzes hinzuweisen (bislang § 19 Absatz 5 Satz 2 BDSG a. F.). Satz 3 enthält die bisher in § 34 Absatz 5 BDSG a. F. enthaltene strenge Zweckbindung der zum Zweck der Auskunftserteilung und zu deren Vorbereitung gespeicherten Daten.

Absatz 3 entspricht § 19 Absatz 6 BDSG a. F. Die Beschränkung dient dem Schutz der öffentlichen Sicherheit (Artikel 23 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679) und der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten (Artikel 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679).

Absatz 4 führt die nach bisherigem Recht (§ 19 Absatz 1 Satz 3 BDSG a. F.) bestehende Einschränkung des Auskunftsrechts für personenbezogene Daten fort, die durch öffentliche Stellen weder automatisiert verarbeitet noch – ohne automatisiert verarbeitet zu werden – in einem Dateisystem gespeichert sind oder werden sollen. Diese Form der Datenverarbeitung ist zwar nach Artikel 2 Absatz 1 der Verordnung (EU) 2016/679 nicht von deren sachlichen Anwendungsbereich erfasst, jedoch gilt nach § 1 Absatz 8 die Verordnung (EU) 2016/679 – und mithin auch das Auskunftsrecht nach deren Artikel 15 – auch für diese Form der Datenverarbeitung. Unter Absatz 4 fallen insbesondere Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien

geordnet sind (vgl. Erwägungsgrund 15 Satz 3 der Verordnung (EU) 2016/679). Die Einschränkung liegt daher außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679.

Das Auskunftsrecht besteht nur unter der Voraussetzung, dass die betroffene Person Angaben macht, die dem Verantwortlichen das Auffinden der Daten ermöglichen. Ferner darf der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse stehen. Beide Voraussetzungen bestehen bereits im geltenden Recht (§ 19 Absatz 1 Satz 3 BDSG a. F.), dessen Schutzstandard erhalten bleibt.

Zu § 35 (Recht auf Löschung)

§ 35 schränkt das Recht der betroffenen Person auf Löschung und die damit korrespondierende Pflicht des Verantwortlichen aus Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 ein. Die in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen bleiben von der Vorschrift unberührt. Die Regelung gilt sowohl für öffentliche als auch nichtöffentliche Stellen. Die bisherige Rechtslage (§§ 20 Absatz 3, 35 Absatz 3 BDSG a. F.) wird weitgehend fortgeführt.

Unter den Voraussetzungen der Absätze 1 bis 3 tritt an die Stelle der Löschung die Einschränkung der Verarbeitung (Artikel 18 der Verordnung (EU) 2016/679).

Hierdurch wird die Beschränkung des Rechts auf bzw. der Pflicht zur Löschung personenbezogener Daten auf das erforderliche Ausmaß im Sinne des Artikel 23 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 begrenzt. Artikel 18 Absatz 2 und 3 sowie Artikel 19 der Verordnung (EU) 2016/679 vermitteln effektive Garantien gegen Missbrauch und unrichtige Übermittlung im Sinne des Artikels 23 Absatz 2 Buchstabe d der Verordnung (EU) 2016/679.

Absatz 1 Satz 1 und 2 entspricht der bisherigen Regelung des § 20 Absatz 3 Nummer 3 und § 35 Absatz 3 Nummer 3 BDSG a. F. Der vertretbare Aufwand für den Verantwortlichen bemisst sich nach dem jeweiligen Stand der Technik und erfasst insbesondere nicht oder nur mit unverhältnismäßig hohem Aufwand veränderbare oder löschbare Datenspeicher. Einschränkend gilt dies nach Satz 3 nicht für die Fallgruppe des Artikels 17 Buchstabe d der Verordnung (EU) 2016/679, da der Verantwortliche bei einer unrechtmäßigen Datenverarbeitung nicht schutzwürdig ist und sich nicht auf einen unverhältnismäßig hohen Aufwand der Löschung wegen der von ihm selbst gewählten Art der Speicherung berufen kann.

Absatz 2 Satz 1 sieht eine Beschränkung zur Wahrung schutzwürdiger Interessen der betroffenen Person vor (Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679). Die Ausnahme entspricht § 20 Absatz 3 Nummer 2 und § 35 Absatz 3 Nummer 2 BDSG a. F. Sie ergänzt in den Fällen, in denen der Verantwortliche die Daten der betroffenen Person nicht länger benötigt oder unrechtmäßig verarbeitet hat (Artikel 17 Absatz 1 Buchstabe a und d der Verordnung (EU) 2016/679) die Regelung des Artikel 18 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679. Nach Artikel 18 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 erfolgt die Einschränkung der Verarbeitung unrechtmäßig verarbeiteter Daten nur auf entsprechendes Verlangen der betroffenen Person. Artikel 18 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 lässt eine Einschränkung der Verarbeitung nicht länger benötigter Daten auf Verlangen der betroffenen Person nur zu, wenn die betroffene Person sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt. Absatz 2 sieht demgegenüber auch ohne entsprechendes Verlangen der betroffenen Person eine generelle Pflicht des Verantwortlichen zur Einschränkung der Verarbeitung vor, wenn er Grund zu der Annahme hat, dass durch die Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. Die Regelung ist notwendig, da der Verantwortliche nach Artikel 17 der Verordnung (EU) 2016/679 grundsätzlich verpflichtet ist, nicht mehr erforderliche oder unrechtmäßig verarbeitete Daten zu löschen.

Die Einschränkung der Verarbeitung anstelle der Löschung soll die betroffene Person in die Lage versetzen, ihr Verlangen auf Einschränkung der Verarbeitung gegenüber dem Verantwortlichen zu äußern oder sich für eine Löschung der Daten zu entscheiden. Dies wird durch die Unterrichtungspflicht nach Satz 2, welche zugleich eine Maßnahme zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person nach Artikel 23 Absatz 2 Buchstabe h der Verordnung (EU) 2016/679 darstellt, gewährleistet. In der Regel wird es sich daher nur um eine vorübergehende Beschränkung der Löschungspflicht des Verantwortlichen handeln (Artikel 23 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679).

Absatz 3 sieht eine Beschränkung für den Fall vor, dass einer Löschung nicht mehr erforderlicher Daten satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen. Die in § 20 Absatz 3 Nummer 1 und § 35 Absatz 3 Nummer 1 BDSG a. F. vorgesehene ergänzende Einschränkung der gesetzlichen Aufbewahrungsfrist ist in § 35 über die sich unmittelbar aus der Verordnung (EU) 2016/679 ergebende Ausnahme des Artikels 17 Absatz 3 Buchstabe b – Erfüllung einer rechtlichen Verpflichtung nach dem Recht der Union oder der Mitgliedstaaten – erfasst. Die Ausnahme schützt den Verantwortlichen vor einer Pflichtenkollision.

Zu § 36 (Widerspruchsrecht)

§ 36 schränkt das Recht auf Widerspruch nach Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 gegenüber einer öffentlichen Stelle ein, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet. § 36 setzt öffentliche Interessen des Verantwortlichen im Sinne des Artikel 23 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 voraus, die im konkreten Einzelfall zwingend sein und Vorrang vor den Interessen der betroffenen Person haben müssen. Darüber hinaus ist das Recht auf Widerspruch ausgeschlossen, wenn eine Rechtsvorschrift zur Verarbeitung verpflichtet. § 27 Absatz 2 und § 28 Absatz 4 enthalten spezifische Einschränkungen des Widerspruchsrechts für die Datenverarbeitung zu Forschungszwecken, statistischen Zwecken und im öffentlichen Interesse liegenden Archivzwecken.

Zu § 37 (Automatisierte Entscheidungen im Einzelfall einschließlich Profiling)

§ 37 trägt den spezifischen Belangen der Versicherungswirtschaft Rechnung. Absatz 1 erlaubt eine automatisierte Einzelentscheidung über die in Artikel 22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 genannten Fälle hinaus, wenn die Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht. Es müssen die in den Nummern 1 und 2 genannten alternativen Voraussetzungen erfüllt sein.

Die Regelung beruht auf Artikel 22 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679, welcher den Mitgliedstaaten die Möglichkeit einräumt, über nach Artikel 22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 hinausgehende Zulässigkeitstatbestände für automatisierte Entscheidungen im Einzelfall zu schaffen. Auch der spezialgesetzlich geregelte automatisierte Erlass von Verwaltungsakten (§ 35a VwVfG) im Rahmen vollautomatisierter Verwaltungsverfahren kann auf Artikel 22 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 gestützt werden.

Im Gegensatz zu Artikel 22 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 ist das Bestehen eines Vertragsverhältnisses zwischen der von der automatisierten Entscheidung betroffenen Person und dem Verantwortlichen keine zwingende Voraussetzung des Absatzes 1. Es genügt vielmehr, dass die automatisierte Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht.

Durch Absatz 1 Nummer 1 bleiben die bislang nach § 6a Absatz 2 Nummer 1 BDSG a. F. zulässigen automatisierten Einzelentscheidungen im Rahmen außervertraglicher Rechtsverhältnisse („sonstige Rechtsverhältnisse“) weiterhin möglich. Absatz 1 Nummer 1 ermöglicht insbesondere die automatisierte Schadensregulierung zwischen der Kfz-Haftpflichtversicherung des Schädigers und dem Geschädigten. Voraussetzung ist, dass dem Begehren des Antragstellers, der gleichzeitig datenschutzrechtlich die betroffene Person ist, entsprochen wird. In diesen Fällen ist eine Rechtsbeeinträchtigung der betroffenen Person nicht ersichtlich.

Absatz 1 Nummer 2 ermöglicht die automatisierte Entscheidung über Versicherungsleistungen der Privaten Krankenversicherung bei der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen. Auch wenn dem Begehren des Antragstellers als von der Entscheidung betroffener Person nicht oder nicht vollständig stattgegeben wird, ist die automatisierte Rechnungsprüfung durch die Private Krankenversicherung – wie bisher nach § 6a Absatz 2 Nummer 2 BDSG a. F. – zulässig, wenn der Verantwortliche angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft. Hierzu zählt zumindest das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung. Über diese Rechte ist die betroffene Person zu informieren. Die aufgeführten Maßnahmen entsprechen den Schutzmechanismen des Artikels 22 Absatz 3 der Verordnung (EU) 2016/679, so dass zwischen § 37 Absatz 1 Nummer 2 und den Zulässigkeitstatbeständen des Artikel 22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 ein harmonisiertes Konzept der Schutzmechanismen besteht.

Beantragt hingegen ein Versicherungsnehmer mit personenbezogenen Daten eines Dritten, namentlich eines im Rahmen der Privaten Krankenversicherung mitversicherten Angehörigen, eine Leistung, liegt keine Entscheidung

im Sinne des Artikels 22 Absatz 1 der Verordnung (EU) 2016/679 gegenüber der datenschutzrechtlich betroffenen Person – dem Dritten – vor. Vielmehr entscheidet die Versicherung ausschließlich automatisiert über Ansprüche aus dem Versicherungsvertrag mit dem Antragsteller als Versicherungsnehmer. Hierbei werden personenbezogene Daten des Dritten automatisiert verarbeitet, wofür es einer Rechtsgrundlage nach Artikel 6 Absatz 1 der Verordnung (EU) 2016/679, jedoch keiner Ausnahmeregelung vom grundsätzlichen Verbot der automatisierten Entscheidung im Einzelfall bedarf.

Absatz 2 Satz 1 erlaubt Versicherungsunternehmen im Rahmen automatisierter Entscheidungen nach Absatz 1 eine Verarbeitung von Gesundheitsdaten im Sinne des Artikel 4 Nummer 15 der Verordnung (EU) 2016/679. Dies ist insbesondere bei der automatisierten Abrechnung von Leistungsansprüchen durch die Private Krankenversicherung notwendig. Absatz 2 beruht auf Artikel 22 Absatz 4 in Verbindung mit Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679. Die Gewährleistung eines bezahlbaren und funktionsfähigen Krankenversicherungsschutzes in der Privaten Krankenversicherung ist als gewichtiges Interesse des Gemeinwohls anerkannt. Eine wirtschaftliche Leistungsbearbeitung im Massenverfahren setzt den Einsatz von automatisierten Verfahren voraus, insbesondere wenn es um die Anwendung gesetzlicher und somit standardisierter Gebührenordnungen (zum Beispiel GOÄ) geht.

Nach Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 muss die nationale Regelung in angemessenem Verhältnis zu dem verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen. Dem trägt der Verweis in Absatz 2 Satz 2 auf § 22 Absatz 2 Satz 2 Rechnung.

Zu § 38 (Datenschutzbeauftragte nichtöffentlicher Stellen)

§ 38 trifft unter Nutzung der durch Artikel 37 Absatz 4 Satz 1 Halbsatz 2 und Artikel 38 Absatz 5 der Verordnung (EU) 2016/679 vermittelten Gestaltungsspielräume Regelungen zur Benennungspflicht und zur Verschwiegenheitspflicht bzw. dem Zeugnisverweigerungsrecht von Datenschutzbeauftragten in nichtöffentlichen Stellen. Diese ergänzen die Vorgaben der Artikel 37 bis 39 der Verordnung (EU) 2016/679 zu der Benennung, der Stellung und den Aufgaben betrieblicher Datenschutzbeauftragter.

In Absatz 1 wird von der Öffnungsklausel des Artikels 37 Absatz 4 Satz 1 Halbsatz 2 der Verordnung (EU) 2016/679 Gebrauch gemacht.

Satz 1 ist inhaltlich an den bisherigen § 4f Absatz 1 Satz 4 BDSG a. F. angelehnt. Danach haben nichtöffentliche Stellen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu bestellen, wenn sie in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen. Satz 2 entspricht inhaltlich im Wesentlichen der bisherigen Regelung des § 4f Absatz 1 Satz 6 BDSG a. F.

Absatz 2 verweist für die betrieblichen Datenschutzbeauftragten, sofern aufgrund der Verordnung (EU) 2016/679 oder Absatz 1 eine Pflicht zur Benennung besteht, auf den besonderen Kündigungsschutz des § 6 Absatz 4. Die in § 6 Absatz 5 Satz 2 und Absatz 6 vorgesehenen Regelungen zur Verschwiegenheitspflicht und zum Zeugnisverweigerungsrecht, die auf Artikel 38 Absatz 5 der Verordnung (EU) 2016/679 beruhen, finden auch für betriebliche Datenschutzbeauftragte stets Anwendung.

Zu § 39 (Akkreditierung)

Artikel 43 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 sieht vor, dass die für die Zertifizierung von Verantwortlichen oder Auftragsverarbeitern zuständigen Zertifizierungsstellen durch die Aufsichtsbehörden und/oder die gemäß Verordnung (EG) 765/2008 benannten nationalen Akkreditierungsstellen akkreditiert werden. Die Mitgliedstaaten haben sicherzustellen, dass die Akkreditierung durch eine oder beide dieser Institutionen erfolgt. Die Deutsche Akkreditierungsstelle (DAkkS) ist die gemäß der Verordnung (EG) 765/2008 benannte nationale Akkreditierungsstelle.

§ 39 sieht in Ausübung des durch Artikel 43 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 eröffneten mitgliedstaatlichen Gestaltungsspielraums eine Akkreditierung der Zertifizierungsstellen auf der Grundlage des Akkreditierungsgesetzes vor. Die Akkreditierung durch die DAkkS ist sachgerecht, weil die DAkkS über hohe Kompetenz und Erfahrung bei der Akkreditierung und über eine etablierte und erprobte Akkreditierungsinfrastruktur verfügt. Die Regelung stellt ein bundeseinheitliches Akkreditierungsverfahren sicher, dass eine europaweite und im Rahmen von Gegenseitigkeitsabkommen auch internationale Anerkennung der Akkreditierungen sicherstellt.

Um die gebotene Einwirkungsmöglichkeit der zuständigen Aufsichtsbehörde in die Akkreditierungsentscheidung der DAkkS zu gewährleisten, erhalten die Aufsichtsbehörden des Bundes und der Länder durch Satz 1 die Zuständigkeit als Befugnis erteilende Behörde im Sinne des § 1 Absatz 2 Satz 1 des Akkreditierungsstellengesetzes. Durch Satz 2 werden diejenigen Normen des Akkreditierungsstellengesetzes für entsprechend anwendbar erklärt, die die gebotene Beteiligung und Mitsprache der Aufsichtsbehörden an der Akkreditierungsentscheidung durch die DAkkS gewährleisten. Danach trifft die DAkkS die Akkreditierungsentscheidung im Einvernehmen mit der zuständigen Aufsichtsbehörde (§ 4 Absatz 3 Akkreditierungsstellengesetz).

Zu § 40 (Aufsichtsbehörden der Länder)

§ 40 regelt die Zuständigkeit und in Ergänzung und Konkretisierung des Artikels 58 Absatz 6 der Verordnung (EU) 2016/679 die Befugnisse der Aufsichtsbehörden der Länder über die nichtöffentlichen Stellen. Die Regelung orientiert sich weitgehend an der bisherigen Regelung des § 38 BDSG a. F. Die Regelungen zur Amtshilfe (§ 38 Absatz 1 Satz 5 BDSG a. F.), zum Beschwerderecht (§ 38 Absatz 1 Satz 8 erste Alternative BDSG a. F.), zur Registerführung meldepflichtiger Datenverarbeitungen (§ 38 Absatz 2 BDSG a. F.), zum Einsichtsrecht geschäftlicher Unterlagen (§ 38 Absatz 4 Satz 2 BDSG a. F.) und zu den Anordnungs- und Beseitigungsverfügungen (§ 38 Absatz 5 Satz 1 und 2 BDSG a. F.) waren aufgrund unmittelbar geltender Vorgaben der Verordnung (EU) 2016/679 zu streichen. Ebenso wurde die überkommene Regelung der Bestimmung der zuständigen Aufsichtsbehörden durch die Landesregierungen (§ 38 Absatz 6 BDSG a. F.) nicht übernommen.

Zu § 41 (Anwendung der Vorschriften über das Bußgeld- und Strafverfahren)

Gemäß § 2 Absatz 2 Satz 2 des Gesetzes über Ordnungswidrigkeiten gilt das Gesetz für Ordnungswidrigkeiten nach Bundes- und Landesrecht. Davon abweichend erstreckt § 41 Absatz 1 das Gesetz über Ordnungswidrigkeiten grundsätzlich auch auf Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679.

§ 41 geht davon aus, dass von den in den Absätzen 4 und 5 des Artikels 83 der Verordnung (EU) 2016/679 genannten „Verstößen gegen die folgenden Bestimmungen“ auch dann gesprochen werden kann, wenn die Mitgliedstaaten bezüglich der in den Absätzen 4 und 5 der Verordnung genannten Bestimmungen nationale Regelungen aufgrund von Öffnungsklauseln erlassen haben. Dass „Verstöße gegen diese Verordnung“ auch Verstöße gegen solche nationalen Bestimmungen erfasst, ergibt sich ausdrücklich im Bereich des Schadensersatzes aus Erwägungsgrund 146 Satz 5 der Verordnung und im Bereich der Strafvorschriften aus Erwägungsgrund 149 Satz 1.

Gemäß Absatz 1 Satz 2 finden §§ 17, 35 und 36 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung. § 17 des Gesetzes über Ordnungswidrigkeiten kommt nicht zur Anwendung, da die Verordnung (EU) 2016/679 die Bußgeldhöhe abschließend regelt. §§ 35 und 36 des Gesetzes über Ordnungswidrigkeiten werden nicht angewendet, da sich bereits aus Artikel 83 der Verordnung (EU) 2016/679 ergibt, dass die Aufsichtsbehörden für die Verhängung von Geldbußen zuständig sind.

Die Verordnung selbst regelt das Bußgeld- und Strafverfahren nicht. An den bisherigen Grundzügen des datenschutzrechtlichen Bußgeld- und Strafverfahrens wird festgehalten, da insbesondere Artikel 83 Absatz 8 Verordnung (EU) 2016/679 ausdrücklich fordert, dass die Mitgliedstaaten angemessene Verfahrensgarantien vorsehen. § 41 Absatz 2 Satz 1 regelt, dass die Vorschriften des Gesetzes über Ordnungswidrigkeiten und der allgemeinen Gesetze über das Strafverfahren grundsätzlich Anwendung finden.

Gemäß Absatz 2 Satz 2 finden §§ 56 bis 58, 87, 88, 99, 100 des Gesetzes über Ordnungswidrigkeiten keine Anwendung. Die Anwendung der §§ 56 bis 58 des Gesetzes über Ordnungswidrigkeiten ist ausgeschlossen, da die Verwarnung bereits in Artikel 58 Absatz 2 Buchstabe b Verordnung (EU) 2016/679 geregelt ist. Indem die §§ 87, 88, 99, 100 für nicht anwendbar erklärt werden, ist die Anwendung einzelner Vorschriften zu Geldbußen gegen eine juristische Person und zu Nebenfolgen sowie zur Vollstreckung von Bußgeldentscheidungen ausgeschlossen.

Absatz 2 Satz 3 bestimmt, dass die Staatsanwaltschaft im Zwischenverfahren das Verfahren nur mit Zustimmung der Aufsichtsbehörde einstellen kann, die den Bußgeldbescheid erlassen hat, wird der Bedeutung der Geldbußen in der Verordnung (EU) 2016/679 und der Unabhängigkeit der Datenschutzaufsicht Rechnung getragen. Im Gegensatz zu anderen Behörden ist die Unabhängigkeit der Datenschutzaufsicht primärrechtlich verankert und durch die Rechtsprechung des EuGH bestätigt worden.

Zu § 42 (Strafvorschriften)

Artikel 84 Absatz 1 der Verordnung (EU) 2016/679 berechtigt und verpflichtet die Mitgliedstaaten, „andere Sanktionen“ für Verstöße gegen die Verordnung festzulegen. Artikel 84 ist damit insbesondere eine Öffnungsklausel, um neben Geldbußen im Sinne des Artikels 83 mitgliedstaatlich strafrechtliche Sanktionen vorzusehen. Hiervon macht § 42 Gebrauch.

Mit Blick auf Straftaten, die vor Geltung der Verordnung (EU) 2016/679 begangen wurden, ist klarstellend insbesondere auf Artikel 49 Absatz 1 Satz 3 der Charta der Grundrechte der Europäischen Union hinzuweisen, wonach dann, wenn nach Begehung einer Straftat durch Gesetz eine mildere Strafe eingeführt wird, diese zu verhängen ist.

Absatz 3 entspricht § 44 Absatz 2 BDSG a. F.

Absatz 4 dient dem verfassungsrechtlichen Verbot einer Selbstbezichtigung und ist § 42a Satz 6 BDSG a. F. entlehnt. Die Regelung kann auf die Öffnungsklausel des Artikels 84 Absatz 1 der Verordnung (EU) 2016/679 gestützt werden, wonach die Mitgliedstaaten Vorschriften für Verstöße gegen diese Verordnung festlegen und alle zu deren Anwendung erforderlichen Maßnahmen treffen.

Zu § 43 (Bußgeldvorschriften)

Absatz 1 gibt die Bußgeldtatbestände des § 43 Absatz 1 Nummer 7a und b BDSG a. F. wieder; mit diesen Tatbeständen war Artikel 9 der Verbraucherkreditrichtlinie 2008/48/EG umgesetzt worden.

Absatz 2 behält den bisherigen Bußgeldrahmen (§ 43 Absatz 3 Satz 1 BDSG a. F.) bei.

Mit Absatz 3 wird von der Öffnungsklausel des Artikels 83 Absatz 7 der Verordnung (EU) 2016/679 Gebrauch gemacht, national zu regeln, ob und in welchem Umfang gegen Behörden und sonstige öffentliche Stellen Geldbußen verhängt werden können. Absatz 2 verweist nicht auf öffentliche Stellen im Sinne des § 2 Absatz 5, denn öffentliche Stellen, die im Rahmen ihrer Tätigkeit im Wettbewerb mit anderen Verarbeitern stehen, sollen bei der Verhängung von Geldbußen gegenüber ihren Wettbewerbern nicht bessergestellt werden.

Absatz 4 dient dem verfassungsrechtlichen Verbot einer Selbstbezichtigung und ist § 42a Satz 6 BDSG a. F. entlehnt. Die Regelung kann auf die Öffnungsklausel des Artikels 83 Absatz 8 der Verordnung (EU) 2016/679 gestützt werden, wonach angemessene Verfahrensgarantien geschaffen werden müssen.

Zu § 44 (Klagen gegen einen Verantwortlichen oder Auftragsverarbeiter)

§ 44 Absatz 1 dient der Durchführung von Artikel 79 Absatz 2 Verordnung (EU) 2016/679. Danach können Klagen wegen eines Verstoßes gegen die Regelungen der Verordnung (EU) 2016/679 vor den Gerichten des Mitgliedstaats erhoben werden, in dem der beklagte Verantwortliche oder Auftragsverarbeiter seine Niederlassung hat oder – sofern die Beklagte nicht als Behörde in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist – vor den Gerichten des Mitgliedstaats, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat.

Artikel 79 Absatz 2 Verordnung (EU) 2016/679 regelt nur die internationale Zuständigkeit und geht insoweit der Verordnung (EU) 1215/2012 vor (vgl. Erwägungsgrund 147 Verordnung (EU) 2016/679 und Artikel 67 Verordnung (EU) 1215/2012). Artikel 79 Absatz 2 der Verordnung regelt aber nicht die örtliche Zuständigkeit. Diese richtet sich bei zivilrechtlichen Ansprüchen grundsätzlich nach den §§ 12 ff. der Zivilprozessordnung (ZPO). Es sind zur Durchführung der Verordnung (EU) 2016/679 ergänzende Regelungen der örtlichen Zuständigkeit erforderlich.

Zum einen ist der Gerichtsstand der Niederlassung (§ 21 Absatz 1 ZPO) auf Klagen beschränkt, die einen Bezug zum Geschäftsbetrieb der Niederlassung haben; Artikel 79 Absatz 2 Satz 1 Verordnung (EU) 2016/679 enthält diese Beschränkung nicht. Dies wird umgesetzt durch die Schaffung eines besonderen Gerichtsstands der Niederlassung in § 44 Absatz 1 Satz 1.

Zum anderen wäre nicht in allen Fällen nach der ZPO eine örtliche Zuständigkeit in Deutschland begründet, wenn der Betroffene hier seinen gewöhnlichen Aufenthaltsort hat. Eine örtliche Zuständigkeit nach den §§ 12 ff. ZPO fehlt etwa, wenn der Beklagte keine Niederlassung in Deutschland hat, kein Gerichtsstand des Vermögens nach § 23 ZPO begründet ist und auch ein Gerichtsstand aus unerlaubter Handlung gemäß § 32 ZPO nicht begründet ist, weil die rechtswidrige Datenverarbeitung keine Auswirkungen im Inland hat. § 44 Absatz 1 Satz 2 schafft daher kumulativ einen besonderen Gerichtsstand am Ort des gewöhnlichen Aufenthalts der betroffenen Person.

Eine Ausnahme von den örtlichen Gerichtsständen des Absatzes 1 sieht § 44 Absatz 2 für Klagen gegen Behörden vor, die in Ausübung hoheitlicher Befugnisse tätig geworden sind. Diese Ausnahme entspricht zum einen Artikel 79 Absatz 2 Verordnung (EU) 2016/679 und berücksichtigt zum anderen, dass sich die örtliche Zuständigkeit für Klagen gegen Behörden, die in Ausübung hoheitlicher Befugnisse tätig geworden sind, nach den Verfahrensordnungen der zuständigen Fachgerichte richtet.

Inhaltlich erfasst die örtliche Zuständigkeit nach § 44 Absatz 1 alle Klagen, die auf datenschutzrechtlichen Vorschriften im Anwendungsbereich der Verordnung (EU) 2016/679 basieren. Datenschutzrechtliche Regelungen sind alle Vorschriften, die dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten dienen (vgl. Artikel 1 Absatz 1 Verordnung (EU) 2016/679). Erfasst werden hiervon neben den Regelungen der Verordnung (EU) 2016/679 auch delegierte Rechtsakte und Durchführungsrechtsakte und andere Beschlüsse der Europäischen Kommission, die auf der Basis der Verordnung (EU) 2016/679 oder der Richtlinie 95/46/EG erlassen worden sind oder erlassen werden, sowie mitgliedstaatliche Regelungen im Anwendungsbereich der Verordnung (EU) 2016/679, die z.B. im Rahmen der Öffnungsklauseln der Konkretisierung der Vorgaben der Verordnung (EU) 2016/679 dienen. Erfasst sind sowohl Klagen wegen Verstößen gegen datenschutzrechtliche Bestimmungen als auch auf Erfüllung von darin enthaltenen Rechten der betroffenen Person (z. B. auf Auskunft oder Berichtigung).

Gemäß Artikel 27 Absatz 1 Verordnung (EU) 2016/679 ist ein Verantwortlicher oder Auftragsverarbeiter, der gemäß Artikel 3 Absatz 2 Verordnung (EU) 2016/679 in deren Anwendungsbereich fällt, also keine Niederlassung in der Europäischen Union hat, verpflichtet, einen Vertreter in der Europäischen Union zu benennen. Dieser dient gemäß Artikel 27 Absatz 4 Verordnung (EU) 2016/679 den betroffenen Personen sowie den Aufsichtsbehörden als Anlaufstelle. Es ist daher sachgerecht, ihn auch als bevollmächtigt anzusehen, Zustellungen in Zivilgerichtsverfahren vor deutschen Gerichten gemäß § 171 ZPO für den Verantwortlichen oder Auftragsverarbeiter entgegenzunehmen. Hierdurch werden insbesondere die praktischen Schwierigkeiten bei der grenzüberschreitenden Zustellung einer Klage vermieden. Es bleibt dem zuständigen Gericht allerdings unbenommen, einen in einem Drittstaat ansässigen Verantwortlichen oder Auftragsverarbeiter – insbesondere bei unklarer Sach- und Rechtslage – ausdrücklich aufzufordern, einen Zustellungsbevollmächtigten im Inland gemäß § 184 Absatz 1 ZPO zu benennen. Diese Möglichkeit besteht bei Beklagten in einem Mitgliedstaat der Europäischen Union nicht.

Zu § 45 (Anwendungsbereich)

Der Dritte Teil dient im Wesentlichen der Umsetzung der Richtlinie (EU) 2016/680. § 45 regelt den Anwendungsbereich des Dritten Teils. Er gilt nur für Verarbeitungen durch öffentliche Stellen und, vgl. Artikel 3 Absatz 7 Buchstabe b der Richtlinie (EU) 2016/680 und § 2 Absatz 4 BDSG, insoweit, als öffentliche Stellen geltende Beliehene, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit zuständig sind und auch nur, soweit sie zu diesen Zwecken Daten verarbeiten. Dies sind insbesondere die Polizeibehörden, die Staatsanwaltschaften sowie der Zoll und die Steuerfahndung, soweit sie die Daten zu den genannten Zwecken verarbeiten. Dies schließt Gefahrenabwehrzwecke ein.

Für die Eröffnung des Anwendungsbereichs des Dritten Teils und damit auch der Richtlinie (EU) 2016/680 genügt also eine Verarbeitung zu den o. g. Zwecken allein nicht; daneben muss auch eine grundsätzliche Befugnis- und Aufgabenzuweisung (Zuständigkeit) für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit vorliegen.

Die Ermittlung, Verfolgung, Ahndung und Vollstreckung von Ordnungswidrigkeiten ist vom Anwendungsbereich umfasst; dies wird durch Erwägungsgrund 13 der Richtlinie (EU) 2016/680 unterstützt. Hierdurch wird insbesondere erreicht, dass die polizeiliche Datenverarbeitung einheitlichen Regeln folgt, unabhängig davon, ob eine Straftat oder eine Ordnungswidrigkeit in Rede steht. Aus dem Ziel, dem Ordnungswidrigkeitenverfahren einheitliche datenschutzrechtliche Regeln gegenüberzustellen, folgt, dass somit auch in Bezug auf die Datenverarbeitung durch Behörden, die nicht Polizeibehörden sind, soweit sie aber Ordnungswidrigkeiten verfolgen, ahnden und vollstrecken, der Teil 3 des vorliegenden Gesetzes gilt und die Datenverarbeitung auch sonst Regeln folgen muss, welche die Richtlinie (EU) 2016/680 umsetzen. Daraus folgt, dass die Datenverarbeitung bei Verwaltungsbehörden wie z. B. Waffen-, Hygiene- oder Passbehörden, deren Aufgabenzuweisung nicht mit den in § 45 genannten Zwecken übereinstimmt, grundsätzlich solange und soweit nicht in den Anwendungsbereich der Richtlinie und

damit des Dritten Teils dieses Gesetzes fällt, wie die von ihnen geführten Verfahren nicht in ein konkretes Ordnungswidrigkeitenverfahren übergehen.

Auftragsverarbeiter – ob öffentliche oder nichtöffentliche Stellen – , deren Tätigkeit sich grundsätzlich dadurch auszeichnet, dass sie Daten zur Erfüllung einer Auftragsverarbeitungsvereinbarung und nicht aufgrund eigener Aufgabenzuschreibung verarbeiten, sind durch die Regelungen des Dritten Teils nur adressiert, sofern sie konkret angesprochen sind. Die von ihnen durchgeführten Verarbeitungen richten sich im Übrigen nach den Regelungen der Verordnung (EU) 2016/679 bzw. dem diese ausformenden Teilen 1 und 2 dieses Gesetzes. Das schließt nicht aus, dass durch den Dritten Teil angesprochene Verantwortliche auch als Auftragsverarbeiter tätig sein können.

Zu § 46 (Begriffsbestimmungen)

Die Begriffsbestimmungen in den Nummern 1 bis 15 sind zum Zweck der Umsetzung der Richtlinie (EU) 2016/680 aufgenommen worden. Sie schließen an die Begriffsbestimmungen in Artikel 3 der Richtlinie (EU) 2016/680 an. Zum Zweck der Übersichtlichkeit wurde die in Artikel 10 der Richtlinie (EU) 2016/680 enthaltene Definition besonderer personenbezogener Daten als Nummer 14 aufgenommen. Zudem wurde die in § 51 angesprochene Einwilligung unter Übernahme der Definition aus der Verordnung (EU) 2016/679 in Nummer 17 aufgenommen.

Zu § 47 (Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten)

§ 47 dient der Umsetzung von Artikel 4 Absatz 1 der Richtlinie (EU) 2016/680 und führt einige allgemeine Verarbeitungsgrundsätze, die in Teilen an späterer Stelle noch einmal aufgenommen werden, an zentraler Stelle zusammen.

Zu § 48 (Verarbeitung besonderer Kategorien personenbezogener Daten)

§ 48 dient der Umsetzung von Artikel 10 der Richtlinie (EU) 2016/680. Absatz 1 legt fest, dass die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig ist, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist und schafft damit eine eigene Rechtsgrundlage für diese Verarbeitungen. Das kann auch die Verarbeitung in den in Artikel 10 Buchstaben b) und c) genannten Zusammenhängen, d. h. zur Wahrung lebenswichtiger Interessen der betroffenen oder eines Dritten oder wenn Daten verarbeitet werden sollen, die die betroffene Person offensichtlich öffentlich gemacht hat, umfassen. In Absatz 2 wird in Satz 1 klargestellt, dass bei der Verarbeitung geeignete Garantien für die Rechtsgüter der betroffenen Personen beachtet werden müssen. In Satz 2 werden Aussagen zu möglichen Maßnahmen zur Umsetzung dieser Vorgabe getroffen. Die Aufzählung gibt unverbindliche Beispielsfälle wieder, wie geeignete Garantien aussehen können. Die konkrete Ausgestaltung der Maßnahmen kann also von Einzelfall zu Einzelfall variieren.

Zu § 49 (Verarbeitung zu anderen Zwecken)

Satz 1 setzt Artikel 4 Absatz 2 der Richtlinie (EU) 2016/680 um. Somit wird klargestellt, dass Verantwortliche Daten so lange und so weit zu anderen Zwecken, als zu denen sie ursprünglich erhoben wurden, verarbeiten dürfen, so lange es sich bei diesen anderen Zwecken um einen der in § 45 genannten Zwecke handelt und diese Verarbeitung erforderlich und verhältnismäßig ist. Grundsätzlich eröffnet Artikel 4 Absatz 2 der Richtlinie (EU) 2016/680 stets die Möglichkeit, die Daten für einen der in § 45 genannten Zwecke zu verarbeiten und innerhalb der Palette der genannten Zwecke auch Zweckänderungen vorzunehmen, wobei der EU-Gesetzgeber offen lässt, ob in diesen Fällen überhaupt eine Zweckänderung vorliegt. Zusätzliche Anforderungen an die Zweckänderung innerhalb der in § 45 genannten Zwecke aufgrund nationalen Verfassungsrechts (so etwa der Grundsatz der hypothetischen Datenneuerhebung, vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 und 1 BvR 1140/06) werden in den Fachgesetzen umgesetzt.

Satz 2 betrifft die Weiterverarbeitung von zu Zwecken des § 45 erhobenen Daten zu anderen als in § 45 genannten Zwecken. Eine solche ist zulässig, wenn dies in einer Rechtsvorschrift vorgesehen ist. Eine solche findet sich beispielsweise für einen typischen Fall einer solchen Weiterverarbeitung durch Datenübermittlung an nicht für Zwecke der Richtlinie zuständige Behörden in § 25.

Zu § 50 (Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken)

§ 50 greift Artikel 4 Absatz 3 der Richtlinie (EU) 2016/680 auf, wonach Verantwortliche Daten auch zu wissenschaftlichen, statistischen und historischen Zwecken verarbeiten dürfen, solange diese Verarbeitung unter die in § 45 genannten Zwecke gefasst werden kann. Als Beispiel kann hier die im Bundeskriminalamt durchgeführte kriminologische oder kriminaltechnische Forschung angeführt werden. Voraussetzung hierfür ist das Vorliegen

geeigneter Vorkehrungen zugunsten der Rechtsgüter der betroffenen Person; hierzu können insbesondere die gemessen am konkreten Forschungszweck so zeitnah wie möglich erfolgende Anonymisierung von Daten oder die räumliche und organisatorische Abtrennung der Forschung betreibenden Stellen gehören. Diese Vorkehrungen werden im einschlägigen Fachrecht, etwa in § 21 Bundeskriminalamtgesetz, weiter ausdifferenziert.

Zu § 51 (Einwilligung)

In § 51 finden sich die Voraussetzungen für eine wirksame Einwilligung. Hierbei wurden Elemente aus Artikel 7 der Verordnung (EU) 2016/679 mit dort nicht enthaltenen Elementen des § 4a BDSG a. F. kombiniert.

Absatz 1 entspricht Artikel 7 Absatz 1, Absatz 2 Artikel 7 Absatz 2 und Absatz 3 Artikel 7 Absatz 3 der Verordnung (EU) 2016/679. In Absatz 4 wurde der Ansatz aus § 4a Absatz 1 BDSG a. F. mit dem Gedanken aus Artikel 7 Absatz 4 der Verordnung (EU) 2016/679 angereichert, wonach für die Beurteilung der Frage, ob die Freiwilligkeit der Einwilligung vorliegt, wesentlich auf die Umstände der Erteilung abzustellen ist.

Absatz 5 entspricht § 4a Absatz 3 BDSG a. F.

Zu § 52 (Verarbeitung auf Weisung des Verantwortlichen)

§ 52 setzt Artikel 23 der Richtlinie (EU) 2016/680 um.

Zu § 53 (Datengeheimnis)

§ 53 greift die Regelung des § 5 BDSG a. F. auf.

Zu § 54 (Automatisierte Einzelentscheidung)

§ 54 setzt Artikel 11 der Richtlinie (EU) 2016/680 um und regelt das Verbot automatisierter, insbesondere auf Profiling basierender Einzelentscheidungen. Um eine in Absatz 1 genannte, nur unter bestimmten Umständen zulässige, „Entscheidung, die eine nachteilige Rechtsfolge für die betroffene Person hat“, zu sein, muss es sich bei einer solchen Entscheidung um einen Rechtsakt mit Außenwirkung gegenüber der betroffenen Person – regelmäßig einen Verwaltungsakt – handeln. Interne Zwischenfestlegungen oder -auswertungen, die Ausfluss automatisierter Prozesse sind, fallen nicht hierunter.

Zu § 55 (Allgemeine Informationen zu Datenverarbeitungen)

§ 55 dient der Umsetzung von Artikel 13 Absatz 1 der Richtlinie (EU) 2016/680. Es geht hier um aktive Informationspflichten des Verantwortlichen gegenüberbetroffenen Personen unabhängig von der Geltendmachung von Betroffenenrechten. Dieser Informationspflicht sollen Verantwortliche in allgemeiner Form nachkommen können. Durch die explizit in Erwägungsgrund 42 der Richtlinie (EU) 2016/680 aufgenommene Möglichkeit der Information über die Internetseite des Verantwortlichen wird im Zusammenhang der Sinn und Zweck der Regelung klargestellt: Betroffene Personen sollen sich unabhängig von der Datenverarbeitung im konkreten Fall in leicht zugänglicher Form einen Überblick über die Zwecke der beim Verantwortlichen durchgeführten Verarbeitungen verschaffen können und eine Übersicht über die ihnen zu Gebote stehenden Betroffenenrechte bekommen.

Zu § 56 (Benachrichtigung betroffener Personen)

§ 56 betrifft Fälle, in denen in fachgesetzlichen Regelungen eine aktive Benachrichtigung betroffener Personen vorgesehen ist. Eine Festlegung dieser in Artikel 13 Absatz 2 der Richtlinie (EU) 2016/680 so bezeichneten „besonderen Fälle“ ist nicht verallgemeinernd auf Ebene des Bundesdatenschutzgesetzes möglich und muss somit im Fachrecht geleistet werden. Leitend für die Entscheidung, ob eine Benachrichtigung unabhängig von der Geltendmachung eines Betroffenenrechts angezeigt ist, dürfte z. B. sein, ob die Verarbeitung mit oder ohne Wissen der betroffenen Person, ggf. in Verbindung mit einer erhöhten Eingriffstiefe, erfolgt. In letztgenannten Fällen ist eine aktive, ggf. nachträgliche Benachrichtigung die einzige Möglichkeit für die betroffene Person, von der Verarbeitung Kenntnis zu erlangen und ggf. deren Rechtmäßigkeit mithilfe der Geltendmachung von Betroffenenrechten zu prüfen.

Absatz 1 stellt klar, welche Informationen betroffenen Personen von dem Verantwortlichen in diesen Fällen aktiv übermittelt werden müssen und dient dabei der Umsetzung von Artikel 13 Absatz 2 der Richtlinie (EU) 2016/680.

Absatz 2 ermöglicht es in Umsetzung von Artikel 13 Absatz 3 der Richtlinie (EU) 2016/680, zu den dort genannten Zwecken von der Bereitstellung der in Absatz 1 genannten Informationen abzusehen, sie einzuschränken oder sie aufzuschieben. Die Vorschrift geht zum Schutz der betroffenen Person über das durch die Richtlinie (EU) 2016/680 Gebotene hinaus, indem tatbestandlich jeweils eine Gefährdung – gegenüber einer in der Richtlinie

angesprochenen Beeinträchtigung – der genannten Rechtsgüter oder Zwecke vorausgesetzt wird. Den Ausnahmen ist der Gedanke gemein, dass die Auskunftserteilung nicht zur Gefährdung der ordnungsgemäßen Erfüllung der Aufgaben des Verantwortlichen führen soll.

Absatz 3 statuiert ein § 19 Absatz 3 BDSG a. F. entnommenes Zustimmungserfordernis der dort genannten Stellen, wenn sich die Benachrichtigung auf die Übermittlung an diese Stellen (nach Absatz 1 Satz 1 Nummer 4) bezieht. Insofern besteht ein der Situation der aktiven Geltendmachung von Betroffenenrechten vergleichbarer Sachverhalt, weshalb die Übernahme geboten ist. Die Nutzung der Möglichkeit, von der Bereitstellung der in Absatz 1 genannten Informationen abzusehen, sie einzuschränken oder aufzuschieben, muss Verhältnismäßigkeitsgrundsätzen genügen, mithin in ein angemessenes Verhältnis zur Bedeutung der Betroffeneninformation für die spätere Geltendmachung von Betroffenenrechten gebracht werden. So hat der Verantwortliche im Einzelfall zu prüfen, ob die Bereitstellung etwa nur teil- oder zeitweise eingeschränkt werden kann („solange und soweit“).

Zu § 57 (Auskunftsrecht)

§ 57 thematisiert das Auskunftsrecht als zentrales Betroffenenrecht und normiert gleichzeitig dessen Einschränkungen. Die Vorschrift dient mithin der Umsetzung der Artikel 14 (Bestehen des Auskunftsrechts) und 15 (Ausnahmen) der Richtlinie (EU) 2016/680. Das Auskunftsrecht setzt – im Gegensatz zu in § 56 angesprochenen aktiven Benachrichtigungspflichten – einen entsprechenden Antrag der betroffenen Person voraus.

Absatz 1 legt den Umfang des der betroffenen Person zustehenden Auskunftsrechts fest. Der in den Nummern 1 und 4 genannte Begriff „Kategorie“ ermöglicht dem Verantwortlichen eine angemessene Generalisierung der Angaben zu den verarbeiteten personenbezogenen Daten sowie zu den Übermittlungsempfängern. Die Angaben nach Nummer 1 zu den verarbeiteten personenbezogenen Daten können im Sinne einer zusammenfassenden Übersicht in verständlicher Form gemacht werden. Die Angaben müssen also nicht in einer Form gemacht werden, welche Aufschluss über die Art und Weise der Speicherung oder Sichtbarkeit der Daten beim Verantwortlichen (im Sinne einer Kopie) zulässt. Ebenso bedeutet die Pflicht zur Angabe der verfügbaren Informationen zur Datenquelle nicht, dass die Identität natürlicher Personen oder gar vertrauliche Informationen preisgegeben werden müssen. Der Verantwortliche muss sich bei der Angabe zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, letztlich von dem gesetzgeberischen Ziel leiten lassen, bei der betroffenen Person ein Bewusstsein über Umfang und Art der verarbeiteten Daten zu erzeugen und es ihr zu ermöglichen, aufgrund dieser Informationen zu ermessen, ob die Verarbeitung rechtmäßig ist und – wenn Zweifel hieran bestehen – ggf. die Geltendmachung weitere Betroffenenrechte auf diese Informationen stützen zu können.

Absatz 2 überführt den Rechtsgedanken des § 19 Absatz 2 BDSG a. F. in das BDSG und sorgt darüber hinaus für einen Gleichlauf mit § 33 Absatz 1 Nummer 2.

Absatz 3 überführt die Regelung des § 19 Absatz 1 Satz 3 BDSG a. F.

Absatz 4 normiert, zu welchen Zwecken das Auskunftsrecht durch den Verantwortlichen vollständig oder teilweise eingeschränkt werden darf. Die Vorschrift geht zum Schutz der betroffenen Person über das durch die Richtlinie (EU) 2016/680 Gebotene hinaus, indem tatbestandlich jeweils eine Gefährdung – gegenüber einer in der Richtlinie angesprochenen Beeinträchtigung – der genannten Rechtsgüter oder Zwecke vorausgesetzt wird. Den Ausnahmen ist der Gedanke gemein, dass die Auskunftserteilung nicht zur Gefährdung der ordnungsgemäßen Erfüllung der Aufgaben des Verantwortlichen führen soll. Die Nutzung der Möglichkeit, von der Auskunftserteilung vollständig oder teilweise abzusehen, muss Verhältnismäßigkeitsgrundsätzen genügen und ihr muss eine nachvollziehbare Interessenabwägung vorausgehen. Die durch das teilweise oder vollständige Absehen von der Auskunftserteilung geschützten Rechtsgüter müssen mithin in ein angemessenes Verhältnis zur Bedeutung der Auskunftserteilung für die spätere Geltendmachung weiterer Betroffenenrechte gebracht werden. So hat der Verantwortliche im Einzelfall zu prüfen, ob die Auskunft etwa nur teilweise eingeschränkt oder zu einem späteren Zeitpunkt erteilt werden kann.

Absatz 5 nimmt § 19 Absatz 3 BDSG a. F. auf.

Absatz 6 Sätze 1 und 2 dient der Umsetzung von Artikel 15 Absatz 3 Sätze 1 und 2 der Richtlinie (EU) 2016/680. Hierdurch wird dem Verantwortlichen – auch gemeinsam mit der sich aus Absatz 4 ergebenden Variante, die Frage nach dem „Ob“ der Verarbeitung nicht zu beantworten, die Möglichkeit gegeben, das Auskunftsverlangen

unbeantwortet zu lassen („neither confirm nor deny“). Satz 3 nimmt in Bezug auf das Absehen von einer Begründung der Auskunftsverweigerung zusätzlich einen aus § 19 Absatz 5 Satz 1 BDSG a. F. entnommenen Gedanken auf.

Absatz 7 thematisiert die Möglichkeiten, die der betroffenen Person im Fall des Absehens von einer Begründung für die vollständige oder teilweise Einschränkung des Auskunftsrechts oder im Fall der überhaupt ausbleibenden Beantwortung des Auskunftsverlangens bleiben. Nach Satz 1 kann die betroffene Person ihr Auskunftsrecht nach Auskunftsverweigerung durch den Verantwortlichen über die oder den Bundesbeauftragten ausüben. Dies dient der Umsetzung von Artikel 17 Absatz 1 der Richtlinie (EU) 2016/680 und kommt einer deklaratorischen Wiederholung des im BDSG a. F. und nun auch in § 60 enthaltenen Grundsatzes gleich, wonach betroffene Personen jederzeit die Bundesbeauftragte oder den Bundesbeauftragten anrufen können. Satz 2 sieht in Umsetzung von Artikel 17 Absatz 2 der Richtlinie (EU) 2016/680 eine entsprechende Unterrichtung durch den Verantwortlichen vor, die allerdings nicht auf Fälle Anwendung findet, in denen der Verantwortliche nach Absatz 6 berechtigt ist, von einer Information des Antragstellers ganz abzusehen. Satz 3 nimmt § 19 Absatz 6 Satz 1 BDSG a. F. auf. Sätze 4 und 5 betreffen den Inhalt der betroffenen Person seitens der oder dem Bundesbeauftragten zur Verfügung gestellten Informationen im Ergebnis der dort durchgeführten Prüfung; hier wird Artikel 17 Absatz 3 Satz 1 der Richtlinie (EU) 2016/680 umgesetzt und zur Stärkung der Betroffenenrechte in Satz 5 über das von der Richtlinie Geforderte hinausgegangen, indem die Mitteilung die Information enthalten darf, ob datenschutzrechtliche Verstöße festgestellt wurden, mithin die Auskunftsverweigerung oder teilweise Einschränkung der Auskunft rechtmäßig war. Satz 6 und 7 nimmt § 19 Absatz 6 Satz 2 BDSG a. F. auf. Satz 8 setzt Artikel 17 Absatz 3 Satz 2 der Richtlinie (EU) 2016/680 um.

Absatz 8 setzt Artikel 15 Absatz 4 der Richtlinie (EU) 2016/680 um.

Zu § 58 (Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung)

In § 58 werden die Betroffenenrechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung und deren Ausnahmen zusammengeführt. § 58 dient der Umsetzung von Artikel 16 der Richtlinie (EU) 2016/680 in seiner Ausformung als Betroffenenrecht.

Absatz 1 betrifft das Recht auf Berichtigung unrichtiger bzw. auf Vervollständigung unvollständiger Daten. Hier wird Artikel 16 Absatz 1 der Richtlinie (EU) 2016/680 umgesetzt. In Satz 2 wird ein in Erwägungsgrund 47 der Richtlinie (EU) 2016/680 enthaltener Gedanke aufgenommen, wonach zur Vorbeugung massenhafter und nicht erfolgversprechender Anträge klargestellt wird, dass sich die Berichtigung auf die betroffene Person betreffende Tatsachen bezieht und nicht etwa auf den Inhalt von Zeugenaussagen; Gleiches gilt etwa für polizeifachliche Bewertungen. In Satz 3 wird Artikel 16 Absatz 3 Satz 1 Buchstabe a der Richtlinie (EU) 2016/680 umgesetzt. Zwar sieht der Richtlinientext im beschriebenen Fall die Verarbeitungseinschränkung als Alternative zur Löschung vor. Da die Richtlinie allerdings im Fall der Verarbeitung unrichtiger Daten deren Berichtigung, aber nicht deren Löschung vorsieht, wird der in der Richtlinie beschriebene Sachverhalt systematisch korrekt in Absatz 1 verortet, indem für Fälle, in denen nach Bestreiten der Richtigkeit der Daten deren Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, an die Stelle der Berichtigung eine Verarbeitungseinschränkung tritt. Für das Bestreiten der Richtigkeit der beim Verantwortlichen verarbeiteten Daten durch die betroffene Person reicht die reine Behauptung der Unrichtigkeit nicht aus; vielmehr müssen die Zweifel an der Unrichtigkeit durch Beibringung geeigneter Tatsachen substantiiert werden. Dies dient dem Schutz der polizeifachlichen Arbeit und der Vermeidung unverhältnismäßigen Prüfaufwands.

Absatz 2 statuiert das Betroffenenrecht auf Löschung und dient der Umsetzung von Artikel 16 Absatz 2 der Richtlinie (EU) 2016/680, in dem sowohl die unabhängig von der Geltendmachung des Betroffenenrechts durch die betroffene Person bestehende Löschungspflicht des Verantwortlichen als auch das entsprechende Betroffenenrecht angesprochen sind.

Absatz 3 betrifft die Voraussetzungen, unter denen an die Stelle einer Löschung nach Absatz 2 eine Verarbeitungseinschränkung treten kann. Es werden Elemente aus dem bisherigen § 20 Absatz 3 BDSG a. F. (Absatz 3 Satz 1 Nummern 1 und 3), ergänzt um Artikel 16 Absatz 3 Satz 1 Buchstabe b der Richtlinie (EU) 2016/680 (Absatz 3 Satz 1 Nummer 2) aufgenommen. Absatz 3 Satz 1 Nummer 1 übernimmt zudem einen in Erwägungsgrund 47 Satz 4 der Richtlinie (EU) 2016/680 enthaltenen Gedanken. Die Möglichkeit, von der Löschung wegen unverhältnismäßigen Aufwands abzusehen, ist als restriktiv auszulegende Ausnahmeregelung anzusehen. Im

Grundsatz sollte die bei Verantwortlichen zum Einsatz kommende IT-Infrastruktur darauf ausgelegt sein, eine Löschungsverpflichtung auch technisch nachvollziehen zu können.

Satz 2 nimmt einen in § 32 Absatz 2 Satz 3 BKAG enthaltenen Gedanken zur Möglichkeit der Verarbeitung in ihrer Verarbeitung eingeschränkter Daten auf.

Absatz 4 fordert, dass die Verarbeitungseinschränkung im Kontext automatisierter Verarbeitung erkennbar sein muss.

Die in Absatz 5 enthaltene Verpflichtung zur Meldung der Berichtigung an Stellen, von denen die unrichtigen Daten stammen, setzt Artikel 16 Absatz 5 der Richtlinie (EU) 2016/680 um. Eine spiegelbildliche Verpflichtung ist in § 75 Absatz 1 für Fälle enthalten, in denen der Verantwortliche von sich aus, also unabhängig von der Geltendmachung eines Betroffenenrechts, eine Berichtigung durchführt. Darüber hinausverweist Absatz 5 Satz 3 im Hinblick auf die Benachrichtigung von Stellen, an die Daten übermittelt wurden, über die Berichtigung, Löschung oder Verarbeitungseinschränkung auf § 72 Absatz 4.

Absatz 6 dient der Umsetzung von Artikel 16 Absatz 4 der Richtlinie (EU) 2016/680 und betrifft das zur Anwendung kommende Verfahren, wenn der Verantwortliche einem Antrag auf Berichtigung oder Löschung nicht oder nur eingeschränkt nachkommt. Die Vorschrift ist § 57 Absatz 6 nachgebildet; folgerichtig wird – so auch in Absatz 7 – weitgehend auf die entsprechenden Vorschriften in § 57 zur vollständigen oder teilweisen Einschränkung des Auskunftsrechts verwiesen.

Zu § 59 (Verfahren für die Ausübung der Rechte der betroffenen Person)

In § 59 werden Elemente des Artikels 12 der Richtlinie (EU) 2016/680 umgesetzt.

Absatz 1 setzt Artikel 12 Absatz 1, Absatz 2 setzt Artikel 12 Absatz 3, Absatz 3 setzt Artikel 12 Absatz 4 und Absatz 4 setzt Artikel 12 Absatz 5 der Richtlinie (EU) 2016/680 um.

Wenngleich es Absatz 5 der Richtlinie (EU) 2016/680 dem Verantwortlichen in begründeten Zweifelsfällen ermöglicht, zusätzliche Informationen zur Identitätsklärung anzufordern, ist hierdurch keine Änderung der bisherigen verbreiteten Praxis angezeigt, den Nachweis der Identität auch weiterhin als Grundvoraussetzung für die Antragsstellung anzusehen.

Zu § 60 (Anrufung der oder des Bundesbeauftragten)

§ 60 stellt auch für den Bereich der Verarbeitung durch Verantwortliche zu den in § 45 genannten Zwecken klar, dass sich Betroffene mit Beschwerden über die bei Verantwortlichen durchgeführte Verarbeitung an die oder den Bundesbeauftragten wenden können. Insbesondere mit Absatz 1 dieser Vorschrift werden gleichzeitig Artikel 52 der Richtlinie (EU) 2016/680 umgesetzt als auch § 21 BDSG a. F. in das BDSG überführt. Absatz 2 setzt Artikel 52 Absatz 2 der Richtlinie (EU) 2016/680 um.

Zu § 61 (Rechtsschutz gegen Entscheidungen der oder des Bundesbeauftragten oder bei deren oder dessen Untätigkeit)

§ 61 setzt Artikel 53 Absatz 1 der Richtlinie (EU) 2016/680 um und bestimmt, dass Adressaten von verbindlichen Entscheidungen der oder des Bundesbeauftragten Rechtsschutz gegen diese suchen können. In Erwägungsgrund 86 der Richtlinie (EU) 2016/680 wird betont, dass sich der Rechtsschutz insbesondere auf die Ausübung von Untersuchungs-, Abhilfe und Genehmigungsbefugnissen oder die Ablehnung oder Abweisung von Beschwerden bezieht durch die oder den Bundesbeauftragten bezieht; für reine Stellungnahmen oder Empfehlungen hingegen soll der Anwendungsbereich nicht eröffnet sein. Auf die sich aus seiner systematischen Stellung ergebene Anwendbarkeit von § 20 in Bezug auf das Rechtsschutzverfahren wird hingewiesen. In Absatz 2 wird – im Umsetzung von Artikel 53 Absatz 2 der Richtlinie (EU) 2016/680 – der Rechtsschutz auf Fälle der Untätigkeit der oder des Bundesbeauftragten ausgedehnt.

Zu § 62 (Auftragsverarbeitung)

§ 62 dient der Umsetzung von Artikel 22 der Richtlinie (EU) 2016/680 und stellt Anforderungen auf, wenn der Verantwortliche Auftragsverarbeitungsverhältnisse eingehen will. Gleichzeitig werden Elemente des § 11 BDSG a. F. überführt. Am bisherigen Regelungsansatz, wonach der Verantwortliche für die Datenübermittlung an den Auftragsverarbeiter keiner gesonderten Rechtsgrundlage bedarf, ändert sich durch die Richtlinienumsetzung nichts.

Absatz 1 greift die Regelung des § 11 Absatz 1 BDSG a. F. auf.

Absatz 2 beschreibt an den Auftragsverarbeiter zu stellende Anforderungen und setzt Artikel 22 Absatz 1 der Richtlinie (EU) 2016/680 um.

In Absatz 3 werden Voraussetzungen für die Eingehung von Unterauftragsverarbeitungsverhältnissen normiert und dadurch Artikel 22 Absatz 2 der Richtlinie (EU) 2016/680 umgesetzt.

In Absatz 4 wird in Übernahme von Elementen aus Artikel 28 Absatz 4 der Verordnung (EU) 2016/679 die Überführung von den Auftragsverarbeiter treffenden Pflichten auf einen Unterauftragnehmer thematisiert.

In Absatz 5 werden die erforderlichen Inhalte einer der Auftragsverarbeitung zugrundeliegenden Vereinbarung niedergelegt. Diese Inhalte sind sowohl Artikel 22 Absatz 3 der Richtlinie (EU) 2016/680, Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 als auch § 11 Absatz 2 und 3 BDSG a. F. entnommen; so werden in Satz 2 Nummer 1 Elemente aus Artikel 28 Absatz 3 Buchstabe a der Verordnung (EU) 2016/679 und § 11 Absatz 3 Satz 2 BDSG a. F., in Nummer 5 Elemente aus Artikel 28 Absatz 3 Buchstabe h, in Nummer 7 Elemente aus Artikel 28 Absatz 3 Buchstabe c und in Nummer 8 Elemente aus Artikel 28 Absatz 3 Buchstabe f der Verordnung (EU) 2016/679 aufgenommen.

Absatz 6 trifft in Umsetzung von Artikel 22 Absatz 4 der Richtlinie (EU) 2016/680 Aussagen zur Form der Vereinbarung. Absatz 7 dient der Umsetzung von Artikel 22 Absatz 5 der Richtlinie (EU) 2016/680.

Zu § 63 (Gemeinsam Verantwortliche)

§ 63 dient der Umsetzung von Artikel 21 der Richtlinie (EU) 2016/680. Zur beispielhaften Konkretisierung der infrage kommenden Fälle wird zudem eine Formulierung aus § 6 Absatz 2 BDSG a. F. übernommen.

Zu § 64 (Anforderungen an die Sicherheit der Datenverarbeitung)

§ 64 dient der Umsetzung von Artikel 29 der Richtlinie (EU) 2016/680. Er verpflichtet den Verantwortlichen dazu, erforderliche technisch-organisatorische Maßnahmen zu treffen. Gleichzeitig wird klargestellt, dass die Ausgestaltung der Maßnahmen Ergebnis eines Abwägungsprozesses sein soll, in den insbesondere der Stand der verfügbaren Technik, die entstehenden Kosten, die näheren Umstände der Verarbeitung und die in Aussicht zu nehmende Gefährdung für die Rechtsgüter der betroffenen Person einzustellen sind. Weiterhin wird klarstellend geregelt, dass bei der Festlegung der technisch-organisatorischen Maßnahmen die einschlägigen Standards und Empfehlungen, insbesondere Technische Richtlinien, des Bundesamts für Sicherheit in der Informationstechnik zu berücksichtigen sind.

Absatz 1 liegt der schon in § 9 Satz 2 BDSG a. F. enthaltene Gedanke zugrunde, wonach die Erforderlichkeit der Maßnahmen daran zu bemessen ist, ob ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht, aufgenommen.

In Absatz 2 werden Inhalte aus Artikel 32 Absatz 1 Buchstaben a bis c Verordnung (EU) 2016/679 übernommen.

Absatz 3 nimmt den wesentlichen Inhalt von § 9 BDSG a. F. und dem Anhang zu § 9 Satz 1 BDSG a. F. auf und überführt ihn in das BDSG. Er benennt die Ziele, die im Hinblick auf automatisierte Verarbeitungen durch die Etablierung geeigneter technisch-organisatorischer Maßnahmen verfolgt und erreicht werden sollen. Satz 2 nimmt den in Satz 3 der Anlage zu § 9 Satz 1 BDSG a. F. enthaltenen Gedanken auf.

Zu § 65 (Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Bundesbeauftragten)

§ 65 dient der Umsetzung von Artikel 30 der Richtlinie (EU) 2016/680 und legt den Umfang und die Modalitäten der Meldung von „Verletzungen des Schutzes personenbezogener Daten“ nach § 46 Nummer 10 an die oder den Bundesbeauftragten fest. Ansatzpunkt der Meldung sind, wie sich auch aus der systematischen Stellung der Vorschrift im Bereich Sicherheit der Verarbeitung ergibt, Vorfälle wie etwa Datenabflüsse.

Die in Absatz 5 geforderte Dokumentation muss in Qualität und Quantität so beschaffen sein, dass sie der oder dem Bundesbeauftragten die Überprüfung der Einhaltung der gesetzlichen Vorgaben ermöglicht.

In Absatz 7 wird durch einen Verweis auf § 43 Absatz 2 der in § 42a Satz 6 BDSG a. F. enthaltene Gedanke überführt, wonach die Motivation zur Meldung einer Verletzung des Schutzes personenbezogener Daten nicht

dadurch verringert werden soll, dass die durch die Meldung verfügbar werdenden Informationen zur Verarbeitung zur Einleitung eines Strafverfahrens führen können.

Absatz 8 stellt klar, dass die in § 61 enthaltene Meldepflicht an die oder den Bundesbeauftragten andere Meldepflichten, etwa solche an das Bundesamt für Sicherheit in der Informationstechnik als Meldestelle des Bundes für IT-Sicherheitsvorfälle (vgl. § 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik), nicht ausschließt bzw. diesen nicht vorgeht.

Zu § 66 (Benachrichtigung betroffener Personen bei Verletzung des Schutzes personenbezogener Daten)

§ 66 setzt Artikel 31 der Richtlinie (EU) 2016/680 um. In Absatz 6 wird – parallel zu § 65 Absatz 7 – durch einen Verweis auf § 43 Absatz 2 der in § 42a Satz 6 BDSG a. F. enthaltene Gedanke überführt, wonach auch bei einer Benachrichtigung der betroffenen Person die Motivation zu dieser Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten nicht dadurch verringert werden soll, dass die durch die Meldung verfügbar werdenden Informationen zur Verarbeitung zur Einleitung eines Strafverfahrens führen können.

Zu § 67 (Durchführung einer Datenschutz-Folgenabschätzung)

§ 67 dient der Umsetzung von Artikel 27 der Richtlinie (EU) 2016/680. Die Datenschutz-Folgenabschätzung ist ein zentrales Element der strukturellen Stärkung des Datenschutzes. Die Voraussetzungen zur Durchführung einer Datenschutz-Folgenabschätzung können nur unvollkommen gesetzlich konkret ausgestaltet werden. So lässt sich dennoch feststellen, dass hinsichtlich des Umfangs der Verarbeitung nicht eine Einzelverarbeitung, sondern lediglich die Verwendung maßgeblicher Systeme und Verfahren zur Verarbeitung personenbezogener Daten mithilfe einer Datenschutz-Folgenabschätzung vorab in den Blick genommen werden müssen. Insoweit lässt sich – abseits der prozeduralen Verbindung – eine Vergleichbarkeit mit den Voraussetzungen der Durchführung einer Anhörung der oder des Bundesbeauftragten begründen. Kriterien für die Entscheidung, ob die vorgesehene Verarbeitung qualitativ erhöhte Gefahren für die Rechtsgüter der betroffenen Person in sich birgt, können beispielsweise der Kreis der betroffenen Personen, die Art der zur Datenerhebung eingesetzten Mittel oder der Kreis der zugriffsberechtigten Personen, mithin die Eingriffsintensität der mit der Verarbeitung verbundenen Maßnahmen im Sinne einer Gesamtwürdigung sein.

Die Konkretisierung der in Absatz 1 genannten Voraussetzungen obliegt letztlich der Praxis. Bei diesem Konkretisierungsvorgang wird allerdings zu beachten sein, dass die entstehenden Aufwände angemessen und beherrschbar bleiben müssen. Ferner ist festzuhalten, dass das Erfordernis einer Datenschutz-Folgenabschätzung nur für neue Verarbeitungssysteme oder wesentliche Veränderungen an bestehenden gilt.

Absatz 2 nimmt Artikel 35 Absatz 1 Nummer 2, Absatz 3 Artikel 35 Absatz 2 der Verordnung (EU) 2016/679 auf. Absatz 4 legt den Inhalt der Folgenabschätzung fest und konkretisiert die in Artikel 27 Absatz 2 enthaltenen allgemeinen Angaben unter Übernahme der Angaben aus Artikel 35 Absatz 7 der Verordnung (EU) 2016/679 enthaltenen Punkte. Absatz 5 nimmt Artikel 35 Absatz 11 der Verordnung (EU) 2016/679 auf.

Zu § 68 (Zusammenarbeit mit der oder dem Bundesbeauftragten)

§ 68 setzt Artikel 26 der Richtlinie (EU) 2016/680 um. Die hier angesprochene Pflicht des Verantwortlichen zur Zusammenarbeit mit der oder dem Bundesbeauftragten fasst die ohnehin sich aus anderen Vorschriften ergebenden Kooperationsverpflichtungen und Kooperationsbeziehungen zwischen Verantwortlichem und der oder dem Bundesbeauftragten zusammen.

Zu § 69 (Anhörung der oder des Bundesbeauftragten)

§ 69 dient der Umsetzung von Artikel 28 der Richtlinie (EU) 2016/680. Die Vorkonsultation – hier als Anhörung bezeichnet – der oder des Bundesbeauftragten dient der datenschutzrechtlichen Absicherung in Bezug auf beabsichtigte Verarbeitungen in neu anzulegenden Dateisystemen, die ein erhöhtes Gefährdungspotential für Rechtsgüter der betroffenen Personen in sich bergen. Insofern besteht eine enge inhaltliche Verbindung zum Instrument der Datenschutz-Folgenabschätzung (§ 67). Prozedural wird diese Verbindung dadurch hergestellt, dass nach Absatz 1 Nummer 1 eine Anhörung durchzuführen ist, wenn im Ergebnis einer Datenschutz-Folgenabschätzung eine erhöhte Gefährdung angenommen wird und der Verantwortliche hierauf nicht mit Maßnahmen zur Gefährdungsminimierung reagiert.

Der Umfang der der oder dem Bundesbeauftragten vorzulegenden Unterlagen wird in Absatz 2 durch Zusammenführung der Vorgaben aus Artikel 28 Absatz 4 der Richtlinie (EU) 2016/680 und Artikel 36 Absatz 3 der Verordnung (EU) 2016/679 angeglichen.

Artikel 28 der Richtlinie (EU) 2016/680 knüpft an die Einleitung der Konsultation an, setzt aber nicht voraus, dass diese zwingend abgeschlossen sein muss, bevor personenbezogene Daten entsprechend verarbeitet werden. Zwar wird man im Regelfall den Abschluss der Konsultation im Interesse der Betroffenen abwarten. Im Ausnahmefall können jedoch Abweichungen geboten sein. Die in Absatz 4 vorgesehene Eilfallregelung trägt solchen operativen und (polizei-)fachlichen Erfordernissen in Abweichung von Absatz 3 Satz 1 Rechnung. Die Nutzung der Eilfallregelung entbindet den Verantwortlichen gleichwohl nicht davon, die Empfehlungen der oder des Bundesbeauftragten nach pflichtgemäßem Ermessen zu prüfen und die Verarbeitung gegebenenfalls daraufhin anzupassen. Weiterhin schmälert die Eilfallregelung nicht die der oder dem Bundesbeauftragten zur Verfügung stehenden Befugnisse.

Zu § 70 (Verzeichnis von Verarbeitungstätigkeiten)

§ 70 dient der Umsetzung von Artikel 24 der Richtlinie (EU) 2016/680 und verpflichtet den Verantwortlichen zur Führung eines Verzeichnisses über bei ihm durchgeführte Kategorien von Datenverarbeitungstätigkeiten. Dieses Verzeichnis dient vor allem der oder dem Bundesbeauftragten dazu, einen Überblick über die beim Verantwortlichen durchgeführten Datenverarbeitungen zu erhalten. Das Zusammenspiel von Anhörung der Datenschutzaufsicht (§ 69), Einsicht in das Verzeichnis (§ 70 Absatz 3) und Zurverfügungstellung von Protokolldaten (§ 76 Absatz 5) gewährt der oder dem Bundesbeauftragten ein umfassendes Bild über die beim Verantwortlichen durchgeführten Datenverarbeitungen. Dies ermöglicht es ihr oder ihm, ihre oder seine Aufgaben und Befugnisse im Hinblick auf den jeweiligen Verantwortlichen zielgerichtet, effizient und verhältnismäßig auszurichten und zu nutzen. Die Beteiligung der oder des Bundesbeauftragten wird arrondiert und ergänzt durch die interne Beratungs- und Kontrolltätigkeit des oder der Beauftragten für den Datenschutz gemäß § 7 und die in § 16 Absatz 4 enthaltene Regelung zum umfassenden Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen. Das durch § 70 eingeführte Verzeichnis ist von dem System der Errichtungsanordnungen für Dateien zu unterscheiden und muss diese fachgesetzlich in einigen Bereichen vorgesehene Möglichkeit der Vorbereitung, Planung und Vorprüfung vorgesehener Verarbeitungen nicht.

In Absatz 1 werden die in das Verzeichnis aufzunehmenden Angaben benannt. Die Begrifflichkeit „Kategorien von Datenverarbeitungstätigkeiten“ stellt hierbei klar, dass sich das Verzeichnis nicht auf einzelne Datenverarbeitungsvorgänge, sondern auf sinnvoll abgrenz- und kategorisierbare Teile der beim Verantwortlichen durchgeführten Datenverarbeitungen bezieht. Es kann sich anbieten, die nach Satz 1 Nummer 2 aufzunehmenden Angaben zu den Zwecken der Verarbeitung an den gesetzlichen Aufgabenzuschreibungen der betreffenden öffentlichen Stelle auszurichten.

Absatz 2 verpflichtet den Verantwortlichen, ein Verzeichnis, wenngleich in geringerem Umfang, auch für Verarbeitungen zu führen, wenn er personenbezogene Daten im Auftrag verarbeitet.

In Absatz 3 werden Aussagen zur Form des Verzeichnisses getroffen.

Nach Absatz 4 wird das Verzeichnis und seine Aktualisierungen der oder dem Bundesbeauftragten auf Anfrage zur Verfügung gestellt.

Zu § 71 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen)

Durch § 71 soll Artikel 20 der Richtlinie (EU) 2016/680 umgesetzt werden, der generische Anforderungen an die datenschutzfreundliche Gestaltung von Datenverarbeitungssystemen (Privacy by Design) und die Implementierung datenschutzfreundlicher Grundeinstellungen (Privacy by Default) formuliert. Der Norm liegt der Gedanke zugrunde, dass der Aufwand zur Verfolgung der hier formulierten Ziele und Anforderungen im Sinne effizienten Mitteleinsatzes in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen sollte. Zur Konkretisierung und Handhabbarmachung der Vorgaben wurden in Absatz 1 Elemente des § 3a BDSG a. F. aufgenommen.

Die in Absatz 2 angesprochene Anforderung, die automatisierte umfassende Zugänglichmachung personenbezogener Daten zu verhindern, mündet letztlich in die Anforderung, eine solche Zugänglichmachung stets durch menschliches Zutun einer Prüfung zu unterziehen.

Zu § 72 (Unterscheidung zwischen verschiedenen Kategorien betroffener Personen)

§ 72 dient der Umsetzung von Artikel 6, bei Absatz 2 der Umsetzung von Artikel 7 Absatz 1 der Richtlinie (EU) 2016/680. Die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung, etwa der Unterscheidung entsprechende Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besondere Maßnahmen der Datensicherheit werden dem Fachrecht überlassen.

Zu § 73 (Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen)

§ 73 dient der Umsetzung von Artikel 7 Absatz 1 der Richtlinie (EU) 2016/680. Die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung, etwa der Unterscheidung entsprechende Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besondere Maßnahmen der Datensicherheit werden dem Fachrecht überlassen.

Zu § 74 (Verfahren bei Übermittlungen)

Absatz 1 dient der Umsetzung von Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680. Im Hinblick auf die Vervollständigung unvollständiger Daten als möglichem Sinn und Zweck einer Datenübermittlung wurden die in der Richtlinie (EU) 2016/680 enthaltene Vermeidung der Übermittlung „unvollständiger“ Daten nicht übernommen. Ferner ist bei der Anwendung und Auslegung der Anforderungen des § 74 zu beachten, dass die Frage nach der „Aktualität“ von Daten und der damit verbundenen Vorgabe, keine „nicht mehr aktuellen“ Daten zu übermitteln bzw. bereitzustellen, stets nur im konkreten Ermittlungszusammenhang und unter Beachtung des konkreten Verarbeitungszwecks beantworten lässt. In bestimmten Ermittlungszusammenhängen kann auch die Übermittlung nicht (mehr) aktuelle Daten wie alte Meldeadressen, alte (Geburts-)namen etc. bedeutsam und für die Aufgabenerfüllung erforderlich sein.

Absatz 2 wiederum setzt Artikel 9 Absatz 3 der Richtlinie (EU) 2016/680 um. Beispiele für die im Fachrecht vorgesehene Mitgabe besonderer Bedingungen können Zweckbindungsregelungen bei der Weiterverarbeitung durch den Empfänger, das Verbot der Weiterübermittlung ohne Genehmigung oder Konsultationserfordernisse vor der Beauskunftung betroffener Personen durch den Empfänger sein.

Absatz 3 Setzt Artikel 9 Absatz 4 der Richtlinie (EU) 2016/680 um.

Zu § 75 (Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung)

§ 75 dient der Umsetzung von Artikel 16 der Richtlinie (EU) 2016/680 in seiner Ausformung als Pflicht des Verantwortlichen. Systematisch werden in § 75 Pflichten des Verantwortlichen zur Berichtigung und Löschung personenbezogener Daten sowie zur Einschränkung ihrer Verarbeitung thematisiert, die unabhängig davon bestehen, ob eine betroffene Person darum nachsucht. Die spiegelbildlich bestehenden Rechte der betroffenen Person auf Berichtigung, Löschung personenbezogener Daten sowie auf Einschränkung der Verarbeitung durch den Verantwortlichen finden sich in § 58.

In Absatz 1 wird neben der Pflicht des Verantwortlichen zur Berichtigung Artikel 16 Absatz 5 der Richtlinie (EU) 2016/680 umgesetzt.

Absatz 2 dient der Umsetzung von Artikel 16 Absatz 2 der Richtlinie (EU) 2016/680, in dem gleichzeitig das Betroffenenrecht auf Löschung als auch die unabhängig davon bestehende Pflicht des Verantwortlichen zur Löschung erwähnt wird. Die Erweiterung des Katalogs der Tatbestände, bei deren Vorliegen eine Verarbeitungseinschränkung an die Stelle einer Löschung treten kann, um Satz 2 Nummer 2 nimmt ein entsprechendes Element aus Artikel 16 Absatz 3 Buchstabe b der Richtlinie (EU) 2016/680 auf und versteht den dort verwendeten Begriff „Beweiszwecke“ im Sinne von „Zwecke eines gerichtlichen Verfahrens“. Im Übrigen wird auf die Ausführungen zu § 58 Absatz 3 verwiesen.

Absatz 3 dient der Umsetzung von Artikel 5 der Richtlinie (EU) 2016/680.

Absatz 4 dient der Umsetzung von Artikel 16 Absatz 6 und Artikel 7 Absatz 3 der Richtlinie (EU) 2016/680.

Zu § 76 (Protokollierung)

§ 76 dient der Umsetzung von Artikel 25 der Richtlinie (EU) 2016/680 und statuiert in Absatz 1 eine umfassende Pflicht des Verantwortlichen zur Protokollierung der unter seiner Verantwortung durchgeführten Datenverarbeitungen.

Absatz 2 enthält konkrete Vorgaben an den Inhalt der Protokolle, Absatz 3 Verwendungsbeschränkungen, wobei von der durch die Richtlinie (EU) 2016/680 eröffneten Möglichkeit, die Protokolldaten über die Datenschutzkontrolle, Eigenüberwachung und Aufrechterhaltung der Datensicherheit hinaus auch im Zusammenhang mit der Verhütung oder Verfolgung von Straftaten Gebrauch gemacht.

In Absatz 4 wird eine Löschfrist für die Protokolldaten generiert.

In Absatz 5 wird festgelegt, dass die Protokolle dem Datenschutzbeauftragten und der oder dem Bundesbeauftragten zum Zweck der Datenschutzkontrolle zur Verfügung stehen müssen.

Zu § 77 (Vertrauliche Meldung von Verstößen)

§ 77 dient der Umsetzung von Artikel 48 der Richtlinie (EU) 2016/680. Der Verantwortliche hat im Zusammenhang mit der Meldung von Verstößen sowohl verantwortlicheninterne Meldungen als auch Hinweise von betroffenen Personen oder sonstigen Dritten in den Blick zu nehmen. Für beide Stränge bietet sich als Kontakt- und Beratungsstelle der Datenschutzbeauftragte an.

Zu § 78 (Allgemeine Voraussetzungen)

§ 78 dient der Umsetzung von Artikel 35 der Richtlinie (EU) 2016/680 und statuiert Voraussetzungen, die bei jeder Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen vorliegen müssen. Darüber hinaus enthält die Vorschrift zusätzliche Anforderungen an die Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen – auch an die insbesondere nach den §§ 79 bis 81 erforderliche Abwägungsentscheidung – aufgrund der Rechtsprechung des Bundesverfassungsgerichts (so etwa in BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 u. 1 BvR 1140/06). In besonderer Ausprägung dessen fordert Absatz 2 ein Unterbleiben der Übermittlung, wenn im Einzelfall Anlass zur Besorgnis besteht und diese Besorgnis auch nach einer Prüfung durch den Verantwortlichen weiter besteht, dass ein elementaren rechtsstaatlichen Grundsätzen genügender Umgang mit den übermittelten Daten nicht gesichert ist; hierbei ist – unter Übernahme eines Gedanken aus § 14 Absatz 7 BKAG a. F. – besonders zu berücksichtigen, wenn der Empfänger einen angemessenen Schutz der Daten garantiert.

Zu § 79 (Datenübermittlung bei geeigneten Garantien)

§ 79 dient der Umsetzung von Artikel 37 der Richtlinie (EU) 2016/680. In § 79 werden § 78 ergänzende Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten, zu denen die Europäische Kommission keinen Angemessenheitsbeschluss gemäß Artikel 36 gefasst hat, formuliert. Bei solchen Konstellationen kommt dem Verantwortlichen – insbesondere nach § 79 Absatz 1 Absatz 1 Nummer 2 – die Aufgabe zu, das Vorliegen geeigneter Garantien für den Schutz personenbezogener Daten beim Empfänger zu beurteilen. Die etwa beim Bundeskriminalamt bestehende Praxis, nach einer solchen Beurteilung die Datenübermittlung mit der Mitgabe von Verarbeitungsbedingungen – etwa Löschverpflichtungen nach Zweckerreichung, Weiterübermittlungsverbote, Zweckbindungen – zu verbinden, ist dazu geeignet, diese Beurteilung zu dokumentieren und ihr Ergebnis zu sichern. Im Zusammenhang mit dem auch hier anwendbaren § 78 Absatz 2 entfaltet der dort erwähnte Gesichtspunkt der Einzelfallgarantie des Empfängerstaats bei der Prüfung des Vorhandenseins geeigneter Garantien besondere Bedeutung.

Absatz 2 dient der Umsetzung von Artikel 37 Absatz 3 der Richtlinie (EU) 2016/680 zur Dokumentation der Übermittlungen nach § 79.

Absatz 3 dient der Umsetzung von Artikel 37 Absatz 2 der Richtlinie (EU) 2016/680, der die Unterrichtung der oder des Bundesbeauftragten über Kategorien von Übermittlungen vorsieht, die ohne Vorliegen eines Angemessenheitsbeschlusses der Kommission, aber wegen Bestehens geeigneter Garantien für den Schutz personenbezogener Daten im Drittstaat nach entsprechender Beurteilung durch den übermittelnden Verantwortlichen erfolgen.

Zu § 80 (Datenübermittlung ohne geeignete Garantien)

§ 80 dient der Umsetzung von Artikel 38 der Richtlinie (EU) 2016/680 und beleuchtet Konstellationen, in denen weder ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt noch die in § 79 erwähnten Garantien in Form eines rechtsverbindlichen Instruments oder nach Beurteilung durch den übermittelnden Verantwortlichen bestehen.

Zu § 81 (Sonstige Datenübermittlung an Empfänger in Drittstaaten)

§ 81 dient der Umsetzung von Artikel 39 der Richtlinie (EU) 2016/680. Die hier geregelte Konstellation zeichnet sich dadurch aus, dass der Kreis der möglichen Empfänger über öffentliche Stellen, die im Rahmen der Strafverfolgung tätig sind, hinaus auf sonstige öffentliche Stellen und Private ausgeweitet wird. Abgebildet werden etwa Ersuchen an Finanzinstitutionen oder Telekommunikationsdienstleister, die notwendigerweise mit der Übermittlung personenbezogener Daten verbunden sind. Für solche Übermittlungen „im besonderen Einzelfall“ gelten die in § 81 Absatz 1 genannten strengen Voraussetzungen. In Absatz 4 ist eine verstärkte Zweckbindung der gemäß § 81 übermittelten Daten vorgesehen.

Zu § 82 (Gegenseitige Amtshilfe)

§ 82 dient der Umsetzung des Artikels 50 der Richtlinie (EU) 2016/680.

Zu § 83 (Schadensersatz und Entschädigung)

Die Vorschrift setzt Artikel 56 der Richtlinie (EU) 2016/680 um.

Zu § 84 (Strafvorschriften)

Die Vorschrift setzt Artikel 57 der Richtlinie (EU) 2016/680 um. Durch § 81 wird keine dem deutschen Recht grundsätzlich fremde Strafbarkeit öffentlicher Stellen eingeführt.

Um das gesetzgeberische Ziel des Gleichlaufs der Sanktionsmöglichkeiten gegenüber öffentlichen Stellen bzw. deren Bediensteten und der bei diesen Stellen Beschäftigten unabhängig vom mit der Verarbeitung verfolgten Zweck herzustellen, wird auch für den Dritten Teil dieses Gesetzes mit § 41 Absatz 2 davon ausgegangen, dass gegen Behörden keine Geldbußen verhängt werden. Im Hinblick auf die Strafbarkeit von Handlungen wird – ebenso von dem o. g. Ziel eines Gleichlaufs geleitet – auf den für den Zweiten Teil maßgeblichen § 42 abgestellt.

Zu § 85 (Verarbeitung personenbezogener Daten im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten)

Die Vorschrift enthält spezifischere Regelungen für Verarbeitungen personenbezogener Daten im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten.

Absatz 1 enthält eine dem bisherigen § 4b Absatz 2 BDSG a. F. entsprechende Übermittlungsvorschrift an Drittstaaten und über- und zwischenstaatliche Stellen ausschließlich zur Erfüllung der in der Vorschrift genannten Zwecke. Durch den Regelungszusammenhang mit § 1 Absatz 8 i. V. m. Absatz 2 BDSG wird klargestellt, dass diese Ausnahmeregelung für alle nicht spezialgesetzlich geregelten Datenübermittlungen gilt, die nicht unter die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallen.

Absatz 2 entspricht der Regelung des § 24 Absatz 4 Satz 4 BDSG a. F. Sie findet nur Anwendung für Dienststellen im Geschäftsbereich des Bundesministeriums der Verteidigung. Für das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst und den Militärischen Abschirmdienst sind vergleichbare bereichsspezifische Regelungen in den jeweiligen Spezialgesetzen aufgenommen.

Absatz 3 Satz 1 enthält einen speziellen Ausschluss von den Informationspflichten gemäß Artikel 13 Absatz 1 und 2 der Verordnung (EU) 2016/679, der nur für öffentliche Stellen gilt, die nicht in den Anwendungsbereich der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallen, soweit keine spezialgesetzliche Regelung besteht. Der Ausschluss ist notwendig, um bei Verarbeitungen personenbezogener Daten im Bereich der nationalen Sicherheit und der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung, die nicht spezialgesetzlich geregelt sind, die bisherigen Ausnahmen von den Informationspflichten aus § 19a Absatz 3 i. V. m. § 19 Absatz 4 BDSG a. F. zu erhalten. Nach Satz 2 ist das Recht auf Auskunft ausgeschlossen, wenn eine Informationspflicht nicht besteht. Satz 3 bestimmt, dass die Regelungen nach § 32 Absatz 2 und § 33 Absatz 2 BDSG bei Unterbleiben der Informierung bzw. Auskunft bei Verarbeitungen nach Satz 1 keine Anwendung finden.

Zu Artikel 2 (Änderung des Bundesverfassungsschutzgesetzes)

Zu Nummer 1

Zu Buchstabe a

Die Änderungen sind überwiegend Folgeänderungen der neuen Begriffsdefinitionen in § 46 des BDSG (Artikel 1) zum Umgang mit personenbezogenen Daten.

Zu Buchstabe b

Es handelt sich um eine Folgeregelung zum neuen § 27 Nummer 2.

Zu Nummer 2

§ 8 Absatz 1 Satz 1 wird um einen Halbsatz ergänzt, der die Verarbeitung auch nach Einwilligung regelt. Damit wird einem fundamentalen Grundsatz des Datenschutzrechts Rechnung getragen, wie er bislang in § 4 Absatz 1

BDSG a. F. geregelt war und nunmehr in Artikel 6 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 niedergelegt ist. Die Einzelheiten der Einwilligung sind in § 51 BDSG geregelt, der über § 27 Nummer 2 entsprechende Anwendung findet (ohne § 51 Absatz 5 BDSG, der bereichsspezifisch nicht passt, weil der Umgang mit solchen Daten für das Bundesamt für Verfassungsschutz geradezu aufgabentypisch ist). Im Bereich öffentlicher Verwaltung steht nicht erst nötigender Druck der Freiwilligkeit entgegen (§ 51 Absatz 4 BDSG), vielmehr besteht auch ein Koppelungsverbot, wonach Vor- oder Nachteile nicht sachwidrig von einer Datenverarbeitungserlaubnis abhängen dürfen. Dies ist jedoch insbesondere dann nicht der Fall, wenn die Datenverarbeitung sachgemäß die Voraussetzungen der betreffenden Folge sicherstellen soll, beispielsweise ein Dateiabgleich zum Betroffenen für eine Risikoüberprüfung vor Zutrittsgewährung in einen besonders geschützten Bereich. Praktisch bedeutsam wird die Einwilligung vor allem in Akkreditierungsfällen.

Zu Nummer 3 bis 5

Die Änderungen sind Folgeänderungen der neuen Begriffsdefinitionen in § 46 des BDSG (Artikel 1) zum Umgang mit personenbezogenen Daten.

Zu Nummer 6

Die Ergänzung greift die Regelung des § 70 BDSG bereichsspezifisch im Bundesverfassungsschutzgesetz auf.

Zu Nummer 7

Zu Buchstabe a

Die Änderung ist eine Folgeänderung der neuen Begriffsdefinitionen in § 46 des BDSG (Artikel 1) zum Umgang mit personenbezogenen Daten.

Zu Buchstabe b

Es handelt sich um eine Folgeänderung zum neuen § 27 Nummer 2.

Zu Nummer 8

Es handelt sich um Folgeänderungen der neuen §§ 26a, 27 Nummer 2.

Zu Nummer 9

Die Änderung ist eine Folgeänderung der neuen Begriffsdefinitionen in § 46 Nummer 2 und 3 des BDSG (Artikel 1) zum Umgang mit personenbezogenen Daten.

Zu Nummer 10

Der neue § 26a BVerfSchG übernimmt die bisherigen Regelungen in § 21 und § 24 Absatz 1, Absatz 2 Satz 3 sowie Absatz 4 BDSG a. F., die sich auch in ihrer Ausprägung als bereichsspezifische Gestaltung der Datenschutzkontrolle im Bereich der nationalen Sicherheit (Artikel 4 Absatz 2 Satz 3 EUV) bewährt haben und daher im Aufgabenbereich des Bundesamtes für Verfassungsschutz beibehalten bleiben.

Absatz 2 Satz 2 enthält allerdings eine redaktionelle Klarstellung. Entgegen der bisherigen Gesetzesformulierung sind nicht personenbezogene Daten Kontrollgegenstand, sondern der Umgang der Verwaltung mit diesen Daten (am Maßstab der anzuwendenden Datenschutzvorschriften). Die Zuständigkeitsabgrenzung soll lediglich Doppelzuständigkeiten – mit dem Risiko konträrer Ergebnisse – ausschließen, anders als der bisherige § 24 Absatz 2 Satz 3 BDSG a. F. jedoch nicht vor Kenntnisnahme durch den oder die Bundesbeauftragte schützen, soweit solche Kenntnis für seine bzw. ihre – anderen – Kontrollaufgaben erforderlich ist. Mit der jetzt gewählten Formulierung werden somit Kontrolllücken klarer ausgeschlossen. Die G 10-Kommission ist die Fachbehörde zum Schutz des Artikels 10 GG, sie prüft folglich nicht die Einhaltung von Vorschriften, soweit sie nicht den Schutz des Post- oder Fernmeldegeheimnisses bezwecken. Am Beispiel der Regelungen einer Dateianordnung (§ 14 BVerfSchG) bedeutet dies, dass die oder der Bundesbeauftragte deren Einhaltung auch in Bezug auf die Speicherung von G 10-Aufkommen prüfen kann, soweit die Regelungen nicht spezielle Festlegungen zu Daten aus solchen Maßnahmen enthalten. Dies gilt beispielsweise für die allgemeinen Voraussetzungen zur Speicherung von Kontaktpersonen. Wenn die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit eine dies betreffende Querschnittsprüfung durchführt, kann sie oder er dabei an diesem Maßstab auch Datensätze einbeziehen, die unter Verwendung von G 10-Erkenntnissen angelegt worden sind.

Die Regelung ist nicht auf die Durchführung des Bundesverfassungsschutzgesetzes beschränkt, sondern bezieht beispielsweise auch Speicherungen des Bundesamtes für Verfassungsschutz in der Antiterrordatei ein. Zudem

wird mit Absatz 4 die gesamte Aufgabenwahrnehmung einbezogen, also beispielsweise auch die Personalverwaltung oder Beschaffungssachen. Ergänzend eingeschlossen sind Tätigkeiten Dritter für Aufgaben des Bundesamtes für Verfassungsschutz, zum Beispiel Übermittlungen nach § 18 BVerfSchG. Hierunter fällt auch die Fachaufsicht durch das Bundesministerium des Innern. Im Ergebnis beschränkt sich die Bereichsregelung also nicht auf die Behörde, sondern schließt deren Sachaufgabe und die wirksame Aufgabenwahrnehmung ein.

Die Neufassung des § 27 BVerfSchG ist eine Folgeregelung zur Neufassung des BDSG.

Die Differenzierung des Absatzes 1 in zwei Nummern folgt dem Regelungssystem des neu gefassten BDSG. Dessen Teile 1 und 4 gelten auch außerhalb des Anwendungsbereichs von Gemeinschaftsrecht. In § 27 Nummer 1 BVerfSchG werden zu diesen Teilen des BDSG folglich – wie bisher – Anwendungsausschlüsse bestimmt, soweit das Bundesverfassungsschutzgesetz bereichsspezifische Spezialregelungen trifft, die damit als abschließend im Sinne des § 1 Absatz 2 BDSG klargestellt werden. Dies betrifft § 4 und § 16 Absatz 4 BDSG, zu denen das Bundesverfassungsschutzgesetz mit § 8 Absatz 2 i. V. m. § 9 und § 26a Absatz 3 bereichsspezifische Regelungen trifft. Dies ist unionsrechtskonform möglich, da die Verordnung (EU) 2016/679 nur im Kompetenzrahmen der Europäischen Union gilt, die gemäß Artikel 4 Absatz 2 Satz 3 EUV keine Regelungskompetenz zum Bereich des Verfassungsschutzes besitzt. Die weiteren in Nummer 1 aufgeführten Vorschriften des BDSG sind bereits nach ihrem Regelungsinhalt auf den Anwendungsbereich der Verordnung (EU) 2016/679 bzw. der Richtlinie (EU) 2016/680 beschränkt, mithin hier nicht anwendbar. Zur Vermeidung von Missverständnissen, werden sie hier gleichwohl klarstellend mit aufgeführt. Ebenso klarstellend ist auch § 85 BDSG von der Anwendung ausgenommen, der Aufgaben regelt, die nicht in die Zuständigkeit des Bundesamtes für Verfassungsschutz fallen (zudem enthält das Bundesverfassungsschutzgesetz für die Regelungsgegenstände des § 85 BDSG eigene bereichsspezifische Regelungen).

Schließlich wird klarstellend § 1 Absatz 8 BDSG von der Anwendung ausgenommen, da das Bundesverfassungsschutzgesetz ein bereichsspezifisches Datenschutzvollsystem für die Aufgabenwahrnehmung nach § 3 BVerfSchG bildet, das keinen Raum für die Anwendung des Teils 2 des BDSG oder der Datenschutzgrundverordnung belässt. Der Anwendungsausschluss des § 1 Absatz 8 BDSG lässt die grundsätzliche Anwendbarkeit des Teils 1 BDSG unberührt (da sich diese bereits aus § 1 Absatz 1 BDSG ergibt; die Aufführung des Teils 1 in § 1 Absatz 8 BDSG ist insoweit rein deklaratorisch). Die nicht in § 27 Nummer 1 BVerfSchG aufgeführten Regelungen des Teils 1 sind also anwendbar.

Teil 3 des neu gefassten BDSG ist bereits im BDSG auf den Anwendungsbereich der Verordnung (EU) 2016/679 bzw. der Richtlinie (EU) 2016/680 beschränkt. Einige dort getroffene Regelungen sind aber auch im besonderen Aufgabenbereich des § 3 BVerfSchG angemessen. Diese Regelungen gelten daher nach § 27 Nummer 2 entsprechend. Der Einbezug von § 46 BDSG erfolgt vornehmlich im Hinblick auf dessen Nummern 2 und 3 die in der entsprechend angepassten Begrifflichkeit des Bundesverfassungsschutzgesetzes im Interesse einer einheitlichen Datenschutzterminologie aufgegriffen werden. Daneben hält das Bundesverfassungsschutzgesetz auch an im deutschen Recht etablierten Fachbegriffen – soweit sie nicht mit der neuen, EU-geprägten Terminologie kollidieren – weiter fest, so am Begriff der Datei.

Zu Artikel 3 (Änderung des MAD-Gesetzes)

Zu Nummer 1

Es handelt sich zum einen um eine Folgeänderung der neuen Begriffsdefinition in § 46 BDSG (Artikel 1) zum Umgang mit personenbezogenen Daten.

Zum anderen entspricht die hier vorgenommene Ergänzung des § 4 Absatz 1 Satz 1 MAD-Gesetz um die Zulässigkeit einer Verarbeitung auf der rechtlichen Grundlage einer Einwilligung der entsprechenden Änderung des neuen § 8 Absatz 1 Satz 1 BVerfSchG (Artikel 2 Nummer 2), indem dieser fundamentale Grundsatz des Datenschutzrechts mit Ausnahme der Aufgabenwahrnehmung nach § 1 Absatz 2 auch für den Militärischen Abschirmdienst übernommen wird.

Daneben geht mit der Neufassung des § 4 Absatz 1 MAD-Gesetz eine im Wesentlichen redaktionelle Änderung einher, die aus Anlass der Anpassungsgesetzgebung aufgegriffen und wie folgt gesondert begründet wird:

Durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl I S. 1938) wurde § 8 Absatz 2 BVerfSchG geändert. Auf Grund der Einfügung der neuen Sätze 2 und 3 wurden die bisherigen Sätze 2 und 3 der Vorschrift zu den Sätzen 4 und 5. Die auf § 8 Absatz 2 Sätze 2 und

3 BVerfSchG verweisende Vorschrift des § 4 Absatz 1 Satz 3 MAD-Gesetz blieb jedoch unverändert. Die Neufassung der Vorschrift im Rahmen der Anpassungsgesetzgebung trägt der vorerwähnten Änderung des Bundesverfassungsschutzgesetzes nunmehr durch Streichung der fehllaufenden Verweisung Rechnung.

Zu Nummer 2

Es handelt sich um eine Folgeänderung der neuen Begriffsdefinition in § 46 BDSG (Artikel 1) zum Umgang mit personenbezogenen Daten.

Zu Nummer 3

Durch das Erste Gesetz zur Änderung des MAD-Gesetzes vom 8. März 2004 (BGBl. I S. 334) wurde der Militärische Abschirmdienst ermächtigt, personenbezogene Daten auf der rechtlichen Grundlage von § 10 Absatz 2 Satz 2 MAD-Gesetz aus dem damaligen Personalführungs- und Informationssystem (PERFIS) der Bundeswehr abzurufen, um seine Zuständigkeit gemäß § 1 Absatz 1 MAD-Gesetz feststellen zu können. Im Zusammenhang mit der Einführung des Datenfelds „Personenkennziffer/ Personalnummer“ im Rahmen des Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl I S. 1938) ist das noch in der Erstfassung der Vorschrift enthaltene Datenfeld „Geburtsdatum“ entfallen. Mit der (Wieder-) Aufnahme des Datenfelds „Geburtsdatum“ in den Katalog des § 10 Absatz 2 Satz 2 MADG wird gelegentlich der Anpassungsgesetzgebung im Interesse der datenschutzrechtlichen Bestimmtheit der Norm klargestellt, dass das Geburtsdatum als (unvollständiger) Teil der Personenkennziffer auch weiterhin eigenständig abgefragt werden darf. Insoweit wird die Bedeutung des Datenfelds für eine zuverlässige Identifizierung im Rahmen der Zuständigkeitsfeststellung besonders unterstrichen; eine inhaltliche Änderung der Vorschrift ist damit nicht verbunden.

Zu Nummer 4

Durch den neuen § 12a MAD-Gesetz wird hinsichtlich der Ausgestaltung der Datenschutzkontrolle mit der Maßgabe, dass an die Stelle des Bundesministeriums des Innern das Bundesministerium der Verteidigung tritt, in vollem Umfang auf den entsprechend anwendbaren neuen § 26a BVerfSchG (Artikel 2 Nummer 10) verwiesen.

Wie im Aufgabenbereich des Bundesamtes für den Verfassungsschutz wird die bewährte Gestaltung der Datenschutzkontrolle damit auch im Aufgabenbereich des Militärischen Abschirmdienstes beibehalten.

Über die entsprechende Anwendbarkeit des neuen § 26a Absatz 4 BVerfSchG werden von der Regelung nicht nur die Aufgaben des Militärischen Abschirmdienstes nach § 1 Absatz 1 bis 3, § 2 und § 14 des MAD-Gesetzes umfasst, sondern sein gesamtes Aufgabenspektrum, wie beispielsweise auch Beschaffungssachen. Es wird ergänzend ferner sichergestellt, dass datenverarbeitende Tätigkeiten Dritter – die insoweit mithin selbst auf dem Gebiet der nationalen Sicherheit handeln – für Aufgaben des Militärischen Abschirmdienstes gleichfalls eingeschlossen sind.

Zu Nummer 5

Es handelt sich um eine Folgeregelung zur Neufassung des BDSG, die die entsprechenden Änderungen des neu gefassten § 27 BVerfSchG (Artikel 2 Nummer 10) aus den aus der dortigen Begründung ersichtlichen und auch hier geltenden Erwägungen auf den Militärischen Abschirmdienst überträgt.

Zu Artikel 4 (Änderung des BND-Gesetzes)

Zu Nummer 1

Die Änderungen sind überwiegend Folgeänderungen der neuen Begriffsdefinitionen in § 46 des BDSG zum Umgang mit personenbezogenen Daten.

Zu Nummer 2

Zu Buchstabe a

Die Änderung ist eine Folgeänderung der neuen Begriffsdefinition in § 46 des BDSG (Artikel 1) zum Umgang mit personenbezogenen Daten.

Zu Buchstabe b

§ 2 Absatz 1 wird um einen Satz ergänzt, der die Verarbeitung auch nach einer erfolgten Einwilligung regelt. Damit wird einem fundamentalen Grundsatz des Datenschutzrechts Rechnung getragen, wie er bislang in § 4 Absatz 1 BDSG a. F. geregelt war und nunmehr in Artikel 6 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679

niedergelegt ist. Die Einzelheiten der Einwilligung sind in § 51 BDSG geregelt, der über § 32a Nummer 2 entsprechende Anwendung findet (ohne § 51 Absatz 5 BDSG, der bereichsspezifisch nicht passt, weil der Umgang mit solchen Daten für den Bundesnachrichtendienst geradezu aufgabentypisch ist).

Zu Nummer 3 bis 9

Die Änderungen sind Folgeänderungen der neuen Begriffsdefinitionen in § 46 des BDSG (Artikel 1) zum Umgang mit personenbezogenen Daten.

Zu Nummer 10

Die Änderung ist eine Folgeänderung aus der Umstrukturierung des BDSG.

Zu Nummer 11

Für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz beim Bundesnachrichtendienst durch die Bundesbeauftragte oder den Bundesbeauftragten gilt § 26a Bundesverfassungsschutzgesetz mit der Maßgabe entsprechend, dass an die Stelle des Bundesministeriums des Innern das Bundeskanzleramt tritt. § 16 Absatz 5 BDSG ist dabei für die datenschutzrechtliche Kontrolle des Bundesnachrichtendienstes ohne Belang, da es keine Landesbehörden gibt, die vergleichbare Zuständigkeiten wie der Bundesnachrichtendienst haben.

Das in § 26a Absatz 3 Nummer 2 Bundesverfassungsschutzgesetz geregelte Zutrittsrecht zu allen Diensträumen bezieht sich nur auf die vom Bundesnachrichtendienst genutzten Räume. Räume, welche beispielsweise bei gemeinsam genutzten Dienststellen ausschließlich durch andere Einrichtungen genutzt werden, sind keine Diensträume des Bundesnachrichtendienstes. Insoweit besteht folglich auch kein Betretungsrecht nach dieser Vorschrift.

Zu Nummer 12

Es handelt sich um eine Folgeregelung zur Neufassung des BDSG. Dessen Teil 1 gilt ohne Beschränkung auf den Anwendungsbereich von Gemeinschaftsrecht. In § 32a Nummer 1a) BNDG werden folglich – wie bisher – Anwendungsausschlüsse bestimmt, soweit das Gesetz über den Bundesnachrichtendienst bereichsspezifische Spezialregelungen trifft, die damit als abschließend im Sinne des § 1 Absatz 2 BDSG klargestellt werden. Dies betrifft § 4 und § 16 Absatz 4 BDSG, zu denen das BNDG mit § 5 BNDG in Verbindung mit § 8 Absatz 2 und § 9 BVerfSchG bereichsspezifische Regelungen trifft. Dies ist unionsrechtskonform möglich, da die Verordnung (EU) 2016/679 nur im Kompetenzrahmen der Europäischen Union gilt, die gemäß Artikel 4 Absatz 2 Satz 3 EUV keine Regelungskompetenz zum Bereich der Nachrichtendienste besitzt. Die weiteren in Nummer 1a) aufgeführten Vorschriften des BDSG sind bereits nach ihrem Regelungsinhalt auf den Anwendungsbereich der Verordnung (EU) 2016/679 bzw. der Richtlinie (EU) 2016/680 beschränkt, mithin hier nicht anwendbar. Zur Vermeidung von Missverständnissen werden sie hier gleichwohl klarstellend mit aufgeführt. Ebenso wird klarstellend § 1 Absatz 8 BDSG von der Anwendung ausgenommen, da das BND-Gesetz ein bereichsspezifisches Datenschutzvollsystem für die Aufgabenwahrnehmung des Bundesnachrichtendienstes bildet, das keinen Raum für die Anwendung des Teil 2 des BDSG oder der Datenschutzgrundverordnung belässt.

Der § 14 Absatz 2 BDSG wird in Nummer 1b) mit der Maßgabe für anwendbar erklärt, dass sich die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nur an die für die Kontrolle des Bundesnachrichtendienstes zuständigen Gremien wenden darf (PKGr, G10-Kommission, Vertrauensgremium und Unabhängiges Gremium). Dies führt zu einem einheitlichen Kontrollansatz, denn damit ist sichergestellt, dass den Bundesnachrichtendienst betreffende Sachverhalte nach Abschluss der Stellungnahmefrist des § 16 Absatz 2 Satz 1 BDSG nur in den Gremien besprochen werden, die für die Kontrolle gesetzlich vorgesehen sind und auch entsprechend mit den zur Verfügung gestellten eingestuften Unterlagen umgehen. Weiterhin soll verhindert werden, dass zum Beispiel ein nicht abgeschlossener Kontrollvorgang durch die frühzeitige Befassung der Gremien kompromittiert wird.

Die Teile 2 und 3 des BDSG sind bereits im BDSG auf den Anwendungsbereich der Verordnung (EU) 2016/679 bzw. der Richtlinie (EU) 2016/680 beschränkt. Einige dort getroffene Regelungen sind aber auch im besonderen Aufgabenbereich des Bundesnachrichtendienstes angemessen. Diese Regelungen gelten daher nach § 32a Nummer 2 BNDG entsprechend. Entsprechende Anwendung bedeutet, dass nachrichtendienstliche Besonderheiten berücksichtigt werden. Das bedeutet z. B. dass die „entsprechende“ Anwendung der Vorschrift des § 64 BDSG dem gesetzlichen Auftrag des BND gemäß § 1 Absatz 2 BNDG Rechnung tragen muss. Danach ist es gerade Aufgabe des Bundesnachrichtendienstes (personenbezogene) Informationen zur Gewinnung von Erkenntnissen über das Ausland, die von außen- oder sicherheitspolitischer Bedeutung sind, zu sammeln und auszuwerten, weshalb

zwangsläufig auch die in § 64 Absatz 1 Satz 1 BDSG angesprochenen „besonderen Kategorien personenbezogener Daten“ i. S. d. § 48 Absatz 2 BDSG einbezogen sind und zulässigerweise verarbeitet werden dürfen. Spezielle Regelungen zur Thematik im BND-Gesetz (etwa § 20 BNDG) sind gemäß § 1 Absatz 2 BDSG vorrangig. § 85 BDSG in Teil 4 findet aufgrund vorrangiger Spezialregelungen auf den Bundesnachrichtendienst keine Anwendung.

Für die fachneutralen Verwaltungsaufgaben des Bundesnachrichtendienstes gilt gemäß § 1 Absatz 8 BDSG auch der Teil 2 des BDSG sowie die Datenschutzgrundverordnung. Für die unabhängige Datenschutzkontrolle gilt im Interesse eines einheitlichen Systems zum Bundesnachrichtendienst auch insoweit § 26a BVerfSchG (i. V. m. § 32 BNDG) entsprechend.

Zu Artikel 5 (Änderung des Sicherheitsüberprüfungsgesetzes)

Zu Nummer 1

Es handelt sich um Folgeänderungen zu den Nummern 5 und 6.

Zu Nummer 2

Die Änderungen sind überwiegend Folgeänderungen der neuen Begriffsdefinitionen in § 46 des BDSG zum Umgang mit personenbezogenen Daten.

Zu Nummer 3

Die Änderungen sind überwiegend Folgeänderungen der neuen Begriffsdefinitionen in § 46 des BDSG zum Umgang mit personenbezogenen Daten.

Zu Nummer 4

Die Änderungen sind überwiegend Folgeänderungen der neuen Begriffsdefinitionen in § 46 des BDSG zum Umgang mit personenbezogenen Daten.

Zu Nummer 5

Die Änderungen sind überwiegend Folgeänderungen der neuen Begriffsdefinitionen in § 46 des BDSG zum Umgang mit personenbezogenen Daten.

Zu Nummer 6

Es handelt sich um eine Folgeregelung zur Neufassung des BDSG a. F.

Dessen Teil 1 gilt ohne Beschränkung auf den Anwendungsbereich von Gemeinschaftsrecht. In § 36 Satz 1 Nummer 1 SÜG werden folglich Anwendungsausschlüsse bestimmt, soweit das SÜG bereichsspezifische Spezialregelungen trifft, die damit abschließend im Sinne von § 1 Absatz 2 BDSG sind. Dies betrifft § 16 Absätze 1 und 4 BDSG, zu denen das SÜG mit § 36a eine bereichsspezifische Regelung trifft. Dies ist gemeinschaftsrechtskonform möglich, da die Verordnung (EU) 2016/679 nur im Kompetenzrahmen der Europäische Union gilt, die gemäß Artikel 4 Absatz 2 Satz 3 EUV keine Regelungskompetenz im Bereich des Sicherheitsüberprüfungsgesetzes besitzt. Die weiteren in Nummer 1 aufgeführten Vorschriften des BDSG sind bereits nach ihrem Regelungsinhalt auf den Anwendungsbereich der Verordnung (EU) 2016/679 bzw. der Richtlinie (EU) 2016/680 beschränkt, mithin hier nicht anwendbar. Zur Vermeidung von Missverständnissen, werden sie hier gleichwohl klarstellend mit aufgeführt. Ebenso werden klarstellend die §§ 1 Absatz 8 und 85 BDSG von der Anwendung ausgenommen, da das SÜG ein bereichsspezifisches Datenschutzvollsystem für den Bereich der Sicherheitsüberprüfungen bildet, das keinen Raum für die Anwendung des Teil 2 des BDSG oder der Datenschutzgrundverordnung belässt.

Die Teile 2 und 3 des BDSG sind bereits nach dem BDSG auf den Anwendungsbereich der Verordnung (EU) 2016/679 bzw. der Richtlinie (EU) 2016/680 beschränkt. Einige dort getroffene Regelungen sind aber auch im Anwendungsbereich des SÜG angemessen. Diese Regelungen gelten daher nach § 36 Satz 1 Nummer 2 entsprechend. Entsprechende Anwendung bedeutet, dass die Besonderheiten im Bereich des SÜG berücksichtigt werden.

Der neue § 36a SÜG übernimmt die bisherigen Regelungen in § 21 und § 24 Absatz 1, Absatz 2 Satz 3 sowie Absatz 4 BDSG a. F., die sich auch in ihrer Ausprägung als bereichsspezifische Gestaltung der Datenschutzkontrolle im Bereich der nationalen Sicherheit (Artikel 4 Absatz 2 Satz 3 EUV) bewährt haben und daher im Anwendungsbereich des SÜG beibehalten bleiben.

Absatz 2 Satz 2 enthält allerdings eine redaktionelle Klarstellung. Entgegen der bisherigen Gesetzesformulierung sind nicht personenbezogene Daten Kontrollgegenstand, sondern der Umgang der Verwaltung mit diesen Daten (am Maßstab der anzuwendenden Datenschutzvorschriften). Die Zuständigkeitsabgrenzung soll lediglich Doppelzuständigkeiten – mit dem Risiko konträrer Ergebnisse – ausschließen, anders als der bisherige § 24 Absatz 2 Satz 4 BDSG a. F. jedoch nicht vor Kenntnisnahme durch den Bundesbeauftragten bzw. die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit schützen, soweit solche Kenntnis für seine bzw. ihre – anderen – Kontrollaufgaben erforderlich ist. Mit der jetzt gewählten Formulierung werden somit Kontrolllücken klarer ausgeschlossen. Die G 10-Kommission ist die Fachbehörde zum Schutz des Artikels 10 GG, sie prüft folglich nicht die Einhaltung von Vorschriften, soweit sie nicht den Schutz des Post- oder Fernmeldegeheimnisses bezwecken.

Zu Artikel 6 (Änderung des Artikel 10-Gesetzes)

Die Änderungen sind Folgeänderungen der neuen Begriffsdefinitionen in § 46 Nummer 2 und 3 des BDSG zum Umgang mit personenbezogenen Daten. Im Interesse einer einheitlichen Datenschutzterminologie werden die Begriffe über den Anwendungsbereich des Teils 3 BDSG hinaus auch im Artikel 10-Gesetz aufgegriffen. Nummer 1 Buchstabe b trifft zudem Klarstellungen zum Regelungsinhalt des § 4 Absatz 4 Artikel 10-Gesetz und seinem Verhältnis zu anderen Vorschriften.

§ 4 regelt in Absatz 2 Satz 3 die Verwendung der Daten, also in der bisherigen Terminologie das Verarbeiten und Nutzen (§ 3 Absatz 5 BDSG a. F.). Darüber hinaus enthält Absatz 4 spezielle Regelungen für die Übermittlung zu den dort genannten Zwecken. Gemeint ist damit die Weitergabe u. a. an Exekutivbehörden. Die weitere Verwendung zur nachrichtendienstlichen Aufklärung der gemäß § 1 Absatz 1 Nummer 1 drohenden Gefahren ist dagegen in Absatz 2 Satz 3 auch für den Fall der Übermittlung geregelt. Eine Landesbehörde für Verfassungsschutz darf die von ihr erhobenen Daten für die in § 1 Absatz 1 Nummer 1 genannten Zwecke verwenden. Erkennt sie ihre örtliche Unzuständigkeit, darf sie im gleichen Rahmen die Daten zuständigkeitshalber auf der Grundlage von Absatz 2 Satz 3 abgeben. Das Verhältnis der Absätze 2 und 4 zueinander wird mit der Einfügung in Absatz 4 klarer.

Im Übrigen ist § 4 Absatz 4 auch in Bezug auf Auslandsübermittlungen als unklar empfunden worden. Die Regelung trifft eine bereichsspezifische Zweckbindung. Sie ist insoweit Ergänzungsnorm der allgemeinen Übermittlungsvorschriften, für das Bundesamt für Verfassungsschutz in § 19 BVerfSchG und für den BND in § 24 Absatz 2 BNDG in Verbindung mit § 19 Absatz 2 bis 5 BVerfSchG. Die Befugnis des Bundesamtes für Verfassungsschutz zur Übermittlung an ausländische öffentliche Stellen folgt aus § 19 Absatz 3 BVerfSchG, ist bei G 10-Erkenntnissen jedoch speziell beschränkt durch § 4 Absatz 4 G 10. Eine Klarstellung erfolgt nunmehr durch Bezug auf § 19 Absatz 3 Sätze 2 und 4 BVerfSchG. Damit wird zugleich verdeutlicht, dass – selbstverständlich – auch bei der Übermittlung von G 10-Erkenntnissen überwiegende schutzwürdige Betroffeneninteressen zu beachten sind. Eine Verweisung auf § 19 Absatz 3 Satz 1 und 3 BVerfSchG erübrigt sich wegen der speziellen Regelungen in § 4 Absatz 4 und Absatz 5 Satz 3 G 10, insbesondere ist die Zweckbindung in § 4 Absatz 4 G 10 bereits enger als die in § 19 Absatz 3 Satz 1 BVerfSchG vorausgesetzten erheblichen Sicherheitsinteressen des Empfängers, da danach nur bestimmte erhebliche Sicherheitsinteressen übermittlungstragend sein können.

Zu Artikel 7 (Änderung des Bundesdatenschutzgesetzes)

Zu Nummer 1

Es handelt sich um eine Folgeänderung zu Nummer 3.

Zu Nummer 2

Der eingefügte Absatz 5a in § 22 BDSG stellt sicher, dass eine Rechtsgrundlage für die Übertragung von Aufgaben der Personalverwaltung und Personalwirtschaft von der oder dem Bundesbeauftragten auf andere Behörden und für die damit einhergehende Übermittlungsbefugnis für die Beschäftigtendaten schon unmittelbar nach Verkündung und nicht erst mit der Neufassung des BDSG durch Artikel 1 mit Wirkung vom 25. Mai 2018 zur Verfügung steht. Auf die Begründung zu Artikel 1 § 8 Absatz 3 wird verwiesen.

Zu Nummer 3

Mit der Einfügung des § 42b in das BDSG wird gewährleistet, dass das Klagerecht den Aufsichtsbehörden schon vor der Anwendbarkeit der Verordnung (EU) 2016/679, also vor dem 25. Mai 2018, zur Verfügung steht.

Zu Artikel 8 (Inkrafttreten, Außerkrafttreten)

Da die Verordnung (EU) 2016/679 nach Artikel 99 Absatz 2 der Verordnung ab dem 25. Mai 2018 unmittelbar geltendes Recht in Deutschland ist, treten mit Absatz 1 das neue, sie ergänzende Bundesdatenschutzgesetz (Artikel 1) und die weiteren Artikel (mit Ausnahme von Artikel 7) zu diesem Zeitpunkt in Kraft. Gleichzeitig tritt das geltende BDSG außer Kraft.

Mit Absatz 2 wird gewährleistet, dass das Klagerecht den Aufsichtsbehörden schon vor der Geltung der Verordnung (EU) 2016/679, also vor dem 25. Mai 2018, zur Verfügung steht.

Anlage 2

Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Abs. 1 NKRG

Datenschutz- Anpassungs- und Umsetzungsgesetz EU (BMI)

Der Nationale Normenkontrollrat hat den Entwurf des oben genannten Regelungsvorhabens geprüft.

I. Zusammenfassung

Bürgerinnen und Bürger	Kein Erfüllungsaufwand
Wirtschaft Jährlicher Aufwand: *davon aus Informationspflichten:* davon aus EU-VO resultierend: Einmaliger Aufwand: *davon aus Informationspflichten:* davon aus EU-VO resultierend:	 rund 17 Mio. Euro *rund 17 Mio. Euro* rund 17 Mio. Euro rund 59 Mio. Euro rund 59 Mio. Euro rund 59 Mio. Euro
Verwaltung Bund Jährlicher Erfüllungsaufwand: davon aus EU-VO resultierend: davon aus EU-RL resultierend: Einmaliger Erfüllungsaufwand: davon aus EU-VO resultierend: davon aus EU-RL resultierend: Länder Jährlicher Erfüllungsaufwand: Einmaliger Erfüllungsaufwand:	 rund 1,5 Mio. Euro rund 0,9 Mio. Euro rund 600.000 Euro rund 130.000 Euro rund 70.000 Euro rund 60.000 Euro rund 1,9 Mio. Euro kein einmaliger Erfüllungsaufwand
‚One in one out'-Regel	Die Belastungen resultieren aus der 1:1-Umsetzung des Datenschutzrechts an die Verordnung (EU) 2016/679. Daher sind diese im Rahmen der ‚One in one out'-Regel der Bundesregierung nicht zu kompensieren.
1:1-Umsetzung von EU-Recht	Es liegen dem NKR keine Anhaltspunkte dafür vor, dass über eine 1:1-Umsetzung der Vorgaben aus der DSGVO bzw. der Datenschutz-Richtlinie ((EU) 2016/680) für den Bereich Polizei und Justiz hinausgegangen wurde.

Evaluierung	Das Ressort hat nach Aufforderung des NKR eine Evaluierungsklausel aufgenommen. Es wird spätestens drei Jahre nach Inkrafttreten der Regelung evaluieren.

Das vorliegende Regelungsvorhaben ist in mehrfacher Hinsicht komplex. Zum einen betreffen Fragen des Datenschutzes – insbesondere die heute zentrale Frage der Weiterverarbeitung von Daten – unzählige Bereiche der Wirtschaft, der Verwaltung sowie der Bürger. Zum zweiten setzt der Entwurf die Datenschutzgrundverordnung der Europäischen Union um, die zwar ab Mai 2018 unmittelbar in allen Mitgliedstaaten der Europäischen Union gilt, jedoch zahlreiche Öffnungsklauseln und Regelungsaufträge beinhaltet, die mit dem vorliegenden Gesetzentwurf ausgestaltet werden. Zum dritten wird mit dem vorliegenden Entwurf die Datenschutz-Richtlinie ((EU) 2016/680) für den Bereich Polizei und Justiz in nationales Recht umgesetzt. Insgesamt löst der vorliegende Entwurf das bisherige Bundesdatenschutzgesetz komplett ab.

Nach gemeinsamem Verständnis der Bundesregierung ist Erfüllungsaufwand, der aus unmittelbar geltenden EU-Verordnungen resultiert, nicht auszuweisen. So hat das Ressort den Aufwand aus der Datenschutzgrundverordnung (EU) in der ab Mai 2018 geltenden Fassung nicht ermittelt. Aufgrund der zahlreichen Öffnungsklauseln, die die Datenschutzgrundverordnung (EU) ausdrücklich zulässt, wurde jedoch im vorliegenden Regelungsentwurf u.a. quantifiziert, welcher Erfüllungsaufwand aus der Nutzung dieser Öffnungsklauseln resultiert. Der Aufwand aus der Nutzung von Öffnungsklauseln ist hier als reine Belastung dargestellt. Bezogen auf den ursprünglichen Erfüllungsaufwand aus der Datenschutzgrundverordnung (EU), der wegen der fehlenden Ausweisung dieses Aufwands nicht quantifiziert vorliegt, ergibt sich jedoch für die Normadressaten im Ergebnis eine Entlastung. Denn der gesamte Erfüllungsaufwand aus der unmittelbar geltenden Datenschutzgrundverordnung (EU) wäre ohne die Nutzung von Öffnungsklauseln mittels des vorliegenden Umsetzungsgesetzes deutlich höher ausgefallen. Die Verringerung kann jedoch nur beschrieben und nicht ausgewiesen werden.

Der Nationale Normenkontrollrat erhebt im Rahmen seines gesetzlichen Auftrags keine Einwände gegen die Darstellung der Gesetzesfolgen in dem vorliegenden Regelungsentwurf.

II. Im Einzelnen

Der vorliegende Gesetzentwurf verfolgt drei wesentliche Zielsetzungen:

- Die Anpassung des nationalen Datenschutzrechts an die europäische Datenschutz-Grundverordnung (DS-GVO (EU) 2016/679), die im Mai 2018 in Kraft treten wird und unmittelbar EU-weit Gültigkeit erlangt.
- Die Umsetzung der Datenschutz-Richtlinie ((EU) 2016/680) für den Bereich Polizei und Justiz, soweit dies nicht im bereichsspezifischen Recht erfolgt.

Insoweit wird das derzeit geltende Bundesdatenschutzgesetz komplett abgelöst.

- Infolge der Ablösung des Bundesdatenschutzgesetzes sind Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes und des Sicherheitsüberprüfungsgesetzes erforderlich, die den Erfordernissen der außerhalb des Anwendungsbereichs des Unionsrechts fallenden Datenverarbeitungen im Bereich der nationalen Sicherheit Rechnung tragen.

Der vorliegende Gesetzentwurf sieht daher die folgenden wesentlichen Änderungen vor:

1. Neufassung des Bundesdatenschutzgesetzes, das für öffentliche Stellen des Bundes und der Länder (soweit nicht landesrechtliche Regelungen greifen) sowie für nichtöffentliche Stellen gilt, bestehend aus:
   a. Gemeinsamen Bestimmungen, u.a.:
      - Rechtsgrundlagen für die Datenverarbeitung durch öffentliche Stellen
      - Regelungen zu den Datenschutzbeauftragten öffentlicher Stellen
      - Festlegung der dt. Vertretung im europ. Datenschutzausschuss

b. Bestimmungen zur Durchführung der Verordnung (EU) 2016/679:, u.a.:

- Festlegung der Voraussetzungen unter denen eine Verarbeitung zu „anderen Zwecken“ zulässig ist
- Regelungen zu Betroffenenrechten
- Verhängung von Geldbußen bei Verstößen

c. Bestimmungen zur Umsetzung der Richtlinie EU 2016/680, u.a.:

- Aussagen zu Rechtsgrundlagen der Verarbeitung, Zweckbindung und -änderung
- Ausformung der Betroffenenrechte
- Festlegung von Verantwortlichenpflichten:
  - Umgang mit Datensicherheitsvorfällen
  - Instrumente zur Berücksichtigung des Datenschutzes (Datenschutzfolgenabschätzung, Anhörung der oder des Bundesbeauftragten, Verzeichnis von Verarbeitungstätigkeiten, Protokollierung)
  - Berichtigungs- und Löschungspflichten
- Datenübermittlungen an Stellen in Drittstaaten und an internationale Organisationen.

2. Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes und des Sicherheitsüberprüfungsgesetzes infolge der Ablösung des bisherigen Bundesdatenschutzgesetzes.
3. Änderung des geltenden Bundesdatenschutzgesetzes, die sicherstellt, dass das Klagerecht gegen Angemessenheitsbeschlüsse der Europäischen Kommission bereits vor Geltung der Verordnung (EU) 2016/679 zur Verfügung steht.

II.1 Erfüllungsaufwand

Bürger

- Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

Wirtschaft

- Das Gesetz verpflichtet die Wirtschaft bei der Verarbeitung personenbezogener Daten Maßnahmen zum Schutz der betroffenen Person in den Fällen zu ergreifen, in denen sie davon absehen wollen, die betroffene Person nach Artikel 13 und 14 der Verordnung (EU) 2016/679 zu informieren. Dazu gehört etwa das Nachholen der Informationspflicht durch Bereitstellen der Information auf einer allgemein zugänglichen Website. Darüber hinaus hat der Verantwortliche zu dokumentieren, aus welchen Gründen von einer Information abgesehen werden soll.
- Durch diese Maßnahmen entstehen für die Wirtschaft jährliche Bürokratiekosten aus Informationspflichten in Höhe von rund 17,2 Millionen Euro. Darüber hinaus fällt einmaliger Erfüllungsaufwand in Höhe von rund 58,9 Millionen Euro an.

Bürokratiekosten aus Informationspflichten für die Wirtschaft

Vorgabe	Paragraf/ Gesetz/Artikel	Art der Vorgabe	Fallzahl jährlich/einmalig	Zeitaufwand pro Fall in Min.	Lohnsatz in €/h	Summe jährl. Erfüllungsaufwand in €	Summe einm. Erfüllungsaufwand in €
Unterbleibt eine Information nach Art. 13 DS-GVO, sind geeignete Maßnahmen zum Schutz der Rechte, Freiheiten und Interessen der betroffenen Personen zu ergreifen	§ 31 Abs. 2 BDSG (Artikel 1)	IP	217.780/ 1.088.900	10	30,90	1.065.489	5.327.443
Dokumentation, wann von der Information nach Art. 13, 14 DS-GVO abgesehen werden kann	§§ 31 Abs. 2, 32 Abs. 2 BDSG (Artikel 1)	IP	255.000/ 2.700.000	75	47,30	15.076.875	48.285.909
Unterbleibt eine Information nach Art. 14 DS-GVO, sind geeignete Maßnahmen zum Schutz der Rechte, Freiheiten und Interessen der betroffenen Personen zu ergreifen	§ 32 Abs. 2 BDSG (Artikel 1)	IP	217.780/ 1.088.900	10	30,90	1.065.489	5.327.443
Summe						**17.207.853**	**58.940.795**

Verwaltung (Bund):

- Für die Verwaltung des Bundes entsteht insgesamt jährlicher Erfüllungsaufwand in Höhe von rund 1,5 Millionen Euro sowie einmalige Umsetzungskosten in Höhe von rund 130.000 Euro. Dieser Aufwand ergibt sich wie folgt:
- Der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit entstehen Mehrausgaben insbesondere durch die Wahrnehmung der Funktion des gemeinsamen Vertreters im Europäischen Datenschutzausschuss nach Artikel 68 der Verordnung (EU) 2016/679 (§ 17 BDSG) sowie durch die bei der Bundesbeauftragten für Datenschutz und Informationsfreiheit angesiedelte Einrichtung der zentralen Anlaufstelle und die damit verbundenen Aufgaben (aufgrund Artikel 51 Absatz 2 i. V. m. Erwägungsgrund 119 der Verordnung (EU) 2016/679 (§ 17 BDSG (10 Stellen). Hieraus resultieren jährlicher Erfüllungsaufwand in Höhe von rund 940.000 Euro sowie jährliche Umsetzungskosten in Höhe von 74.000 Euro.

Erfüllungsaufwand für die Verwaltung des Bundes (Bundesbeauftragte für Datenschutz und Informationsfreiheit)

Vorgabe	Paragraf/ Gesetz/Artikel	Vollzug	Fallzahl jährlich/einmalig	Zeitaufwand pro Fall in Min.	Lohnsatz in €/h	Summe jährl. Erfüllungsaufwand in €	Summe einm. Erfüllungsaufwand in €
Warnung des für die Verarbeitung Verantwortlichen durch den BfDI bei Verdacht auf Verstöße gegen das BDSG	§ 16 Abs. 2 BDSG (Artikel 1)	Bund	100/0	301	35,70	23.898	0
Tätigkeit als gemeinsamer Vertreter im Europäischen Datenschutz-ausschuss sowie zentrale Anlaufstelle	§ 17 Abs. 1 BDSG (Artikel 1)	Bund	1/0	960.000 (10 Stellen)	45,09	912.440	0
Dokumentation, wann von der Information nach Art. 13, 14 DS-GVO abgesehen werden kann	§§ 31 Abs. 2 , 32 Abs. 2 BDSG (Artikel 1)	Bund	308/0	75	57,80	0	26.849
Akkreditierung der Zertifizierungsstellen durch die Aufsichtsbehörden	§ 38 BDSG (Artikel 1)	Bund	1/17	2.400	57,80	2.790	47.422
Summe						**939.128**	**74.271**

- Die im neu gefassten Bundesdatenschutzgesetz zur Umsetzung der Richtlinie (EU) 2016/680 geschaffenen Regelungen schaffen gegenüber dem bestehenden Recht neue Pflichten für die Verwaltung. Es entstehen jährliche Mehrkosten von 563.000 Euro (rund 600.000 Euro).
- Der jährliche Erfüllungsaufwand wird ausgelöst durch die neu vorzunehmende Datenschutz-Folgenabschätzung nach § 63 BDSG-E (jährlich: 510.000 Euro). Darüber hinaus fällt jährlicher Erfüllungsaufwand durch die Einholung einer Genehmigung bei der Übermittlung personenbezogener Daten durch die zuständige Stelle in einen EU-Mitgliedstaat nach § 73 Abs. 3 BDSG-E (jährlich: 33.000 Euro) und durch den zusätzlichen Aufwand der BfDI, wenn diese Datenschutzbehörden in anderen EU-Staaten Amtshilfe nach § 79 BDSG-E leistet und hierzu maßgebliche Informationen übermittelt und Auskunftsersuchen nachkommt (jährlicher Erfüllungsaufwand: rd. 19.000 Euro).
- Zusätzlich entsteht einmaliger Erfüllungsaufwand für die Verwaltung in Höhe von rd. 60.000 Euro für die Anpassung der Software zur Protokollierung der Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen nach § 73 BDSG-E.

Verwaltung (Länder/Kommunen):

- Für die Länder entsteht jährlicher Erfüllungsaufwand in Höhe von insgesamt rund 1,9 Millionen Euro. Dieser Aufwand resultiert aus der Tätigkeit als Stellvertreter des gemeinsamen Vertreters im Europäischen Datenschutzausschuss (Artikel 1, § 17 BDSG), die mit Personalkosten in Höhe von schätzungsweise vier Stellen veranschlagt werden kann. Ferner resultiert der Aufwand aus dem Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder zur Findung eines gemeinsamen Standpunktes (§ 18 BDSG), für die schätzungsweise in der Summe mindestens Personalaufwand in Höhe von einer Stelle im höheren Dienst in jedem Land anzusetzen sein wird. .

Erfüllungsaufwand der Verwaltung für Länder und Kommunen

Vorgabe	Paragraf/ Gesetz	Vollzug	Fallzahl jährlich/einmalig	Zeitaufwand pro Fall in Min.	Lohnsatz in €/h	Summe jährl. Erfüllungsaufwand in €	Summe einm. Erfüllungsaufwand in €
Informationsaustausch und gegenseitige Stellungnahmen zwischen den BfDI und den Aufsichtsbehörden der Länder zur Findung eines gemeinsamen Standpunktes	§ 18 BDSG (Artikel 1)	Land	16/0	96.000 (jeweils 1 Stelle)	58,10	1.792.960	0
Tätigkeit als Stellvertreter des BfDI im Europäischen Datenschutz-ausschuss	§ 17 Abs. 1 BDSG (Artikel 1)	Bund	1/0	192.000 (4 Stellen)	46,75	187.800	0
						1.980.760	

Das Ressort hat die Auswirkungen auf den Erfüllungsaufwand transparent und nachvollziehbar dargestellt.

Der Nationale Normenkontrollrat erhebt im Rahmen seines gesetzlichen Auftrags keine Einwände gegen die Darstellung der Gesetzesfolgen in dem vorliegenden Regelungsentwurf.

Dr. Ludewig
Vorsitzender

Prof. Kuhlmann
Berichterstatterin

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333