Referentenentwurf des Bundesministeriums des Innern

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. EU Nr. L 119 vom 4. Mai 2016, S. 1 ff.) 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). Ihrem Charakter als Grundverordnung folgend enthält die Verordnung Öffnungsklauseln für den nationalen Gesetzgeber. 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 Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU Nr. L 119 vom 4. Mai 2016, S. 89 ff.), 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 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 durch ein neues Bundesdatenschutzgesetz abzulösen. Weiterer gesetzlicher Anpassungsbedarf ergibt sich hinsichtlich der bestehenden bereichsspezifischen Datenschutzregelungen des Bundes in Folge der Änderungen im allgemeinen Datenschutzrecht durch die Verordnung (EU) 2016/679 und das sie ergänzende neugefasste Bundesdatenschutzgesetz.

Im Interesse einer homogenen Entwicklung des allgemeinen Datenschutzrechts soll das neugefasste 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 Bundesdatenschutzgesetzes – BDSG-neu – (Artikel 1), das für öffentliche Stellen des Bundes und der Länder (soweit nicht landesrechtliche Regelungen greifen) sowie für nicht-öffentliche Stellen gilt, bestehend aus drei Teilen:

   a. Gemeinsame Bestimmungen mit folgenden Regelungsschwerpunkten:

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

   Die gemeinsamen Bestimmungen lassen unmittelbar geltendes Recht der Europäischen Union unberührt, insbesondere die Datenschutz-Grundverordnung (Verordnung (EU) Nr. 2016/679[1]). Sie finden außerdem Anwendung im Anwendungsbereich der Richtlinie (EU) 2016/680[2] 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-neu);
      - Festlegung der Zulässigkeitsvoraussetzungen für Verarbeitungen zu anderen Zwecken (§ 23 BDSG-neu);
      - Erhalt der Vorschriften zu Auskunfteien und Scoring sowie Regelung weiterer besonderer Verarbeitungssituationen (§§ 24 bis 29 BDSG-neu);
      - Regelungen zu den Betroffenenrechten (§§ 30 bis 35 BDSG-neu); sie berücksichtigen Artikel 23 der Verordnung (EU) 2016/679, orientieren sich sehr weitgehend an den bestehenden Regelungen des Bundesdatenschutzgesetzes (BDSG-alt) und sorgen für einen angemessenen Interessenausgleich;
      - Verhängung von Geldbußen bei Verstößen gegen die Verordnung (EU) 2016/679 (§§ 39, 40 BDSG-neu).

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

---

[1] 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. EU Nr. L 119 vom 4. Mai 2016, S. 1 ff.)

[2] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU Nr. L 119 vom 4. Mai 2016, S. 89 ff.)

- Aussagen zu Rechtsgrundlagen der Verarbeitung, Zweckbindung und -änderung (§§ 44 bis 46 BDSG-neu)
- Ausformung der Betroffenenrechte (§§ 51 bis 53 BDSG-neu)
- Festlegung unterschiedlich akzentuierter Verantwortlichenpflichten
    - Anforderungen an Auftragsverarbeitungsverhältnisse (§ 57 BDSG-neu)
    - Datensicherheit und Umgang mit Datensicherheitsvorfällen (§§ 58 bis 60 BDSG-neu)
    - Instrumente zur Berücksichtigung des Datenschutzes (Datenschutzfolgenabschätzung, Anhörung der oder des Bundesbeauftragten, Verzeichnis von Verarbeitungstätigkeiten, Protokollierung §§ 61 bis 63 und 71 BDSG-neu)
    - Berichtigungs- und Löschungspflichten (§ 70 BDSG-neu)
- Datenübermittlungen an Stellen in Drittstaaten und an internationale Organisationen (§§ 73 bis 76 BDSG-neu).

2. Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes und des Sicherheitsüberprüfungsgesetzes (Artikel 2 bis 6) in Folge 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 Angemessenheitsbeschlüsse 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 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 Erfüllungsaufwand, der aber durch die Verordnung (EU) 2016/679 und nicht durch dieses Gesetz verursacht wird.

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein neuer Erfüllungsaufwand durch dieses Gesetz.

E.2 Erfüllungsaufwand für die Wirtschaft

Der vorliegende Gesetzentwurf enthält keine Regelungen, die zusätzlichen Erfüllungsaufwand bei der Wirtschaft auslösen. Soweit der Gesetzentwurf Betroffenenrechte einschränkt, führen sie bei den Unternehmen zu einer Reduzierung von Pflichten, die ohne den Gesetzentwurf unmittelbar durch die Verordnung (EU) 2016/679 ausgelöst worden wären.

[siehe Hinweis für NKR im Anschreiben des BMI]

E.3 Erfüllungsaufwand der Verwaltung

Im Einzelplan 21 der Bundesbeauftragten für Datenschutz und Informationsfreiheit entstehen Mehrausgaben durch:

- die Wahrnehmung der Funktion des gemeinsamen Vertreters im Europäischen Datenschutzausschuss nach Artikel 68 der Verordnung (EU) 2016/679 (§ 17 BDSG-neu),
- die bei der Bundesbeauftragten für Datenschutz und Informationsfreiheit angesiedelte Einrichtung der zentralen Anlaufstelle aufgrund des Erwägungsgrundes 119 der Verordnung (EU) 2016/679 (§ 17 BDSG-neu).

Im Regierungsentwurf zum Bundeshaushalt 2017 sind für den Bereich der Umsetzung Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 32 neue Planstellen mit entsprechenden Haushaltsmitteln etatisiert. Der Gesetzentwurf zur Übernahme der Funktionen des gemeinsamen Vertreters und der zentralen Anlaufstelle lag bei Verabschiedung des Regierungsentwurfs noch nicht vor und konnte in seinen Auswirkungen deswegen noch nicht berücksichtigt werden. Sollte die zentrale Anlaufstelle im Ausland (d. h. in Brüssel) verortet werden, ist mit weiterem Mehrbedarf zu rechnen.

[Erfüllungsaufwand zu Teil 3 ist noch zu ermitteln]

Für die Länder entstehen Mehrausgaben durch die Wahl und Bestellung des Stellvertreters des gemeinsamen Vertreters im Europäischen Datenschutzausschuss (§ 17 BDSG-neu). Die Höhe dieser Mehrausgaben kann derzeit nicht quantifiziert werden.

[*im Rahmen der Länderbeteiligung wird eine Schätzung der Mehrausgaben abgefragt werden*].

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

F. Weitere Kosten

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

Referentenentwurf des Bundesministeriums des Innern

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

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

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

Abschnitt 2
Besondere Verarbeitungssituationen

Kapitel 2
Rechte der betroffenen Person

Teil 1
Gemeinsame Bestimmungen
Kapitel 1
Anwendungsbereich und Begriffsbestimmungen

§ 1
Anwendungsbereich des Gesetzes

[ex. § 1 BDSG-alt mod.] (1) Dieses Gesetz gilt für

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,

3. nicht-öffentliche Stellen.

(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.

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

(4) Die Vorschriften dieses Gesetzes finden nur Anwendung, soweit der Verantwortliche oder Auftragsverarbeiter personenbezogene Daten im Rahmen der Tätigkeiten einer inländischen Niederlassung verarbeitet. Hat der Verantwortliche oder Auftragsverarbeiter keine inländische Niederlassung, finden nur §§ 17 bis 19 und § 38 Anwendung.

(5) Die Vorschriften dieses Gesetzes finden Anwendung vorbehaltlich des Rechts der Europäischen Union, im besonderen der Verordnung (EU) 2016/679.

§ 2
Begriffsbestimmungen

[ex. § 2 BDSG-alt] (1) Es bezeichnet der Ausdruck:

1. „öffentliche Stellen des Bundes“ die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen des Bundes gelten Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, ungeachtet der Beteiligung nicht-öffentlicher Stellen, wenn

a. sie über den Bereich eines Landes hinaus tätig werden oder

b. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht. Andernfalls gelten sie als öffentliche Stellen der Länder;

2. „öffentliche Stellen der Länder“ 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. „nicht-öffentliche Stellen“ natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Nummern 1 und 2 fallen; nimmt eine nicht-öffentliche Stelle hoh eitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

[Art. 4 DS-GVO; Art. 3 DSRL] (2) Es bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

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 oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder 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, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen 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 personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

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 möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

10. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise 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 natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen 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, wie 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. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 51 der Verordnung (EU) 2016/679 oder gemäß Artikel 41 der Richtlinie (EU) 2016/680 eingerichtete unabhängige staatliche Stelle;

15. „internationale Organisation" eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

Kapitel 2

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 3

Verarbeitung personenbezogener Daten durch öffentliche Stellen

[ex §§ 13 Abs. 1, 14 Abs. 1 BDSG-alt mod.; Art. 6 Abs. 1 lit. e i.V.m. Abs. 3 Satz 1 DS-GVO] Unbeschadet anderer Rechtsgrundlagen ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen 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.

§ 4

[*ex. § 6b BDSG-alt*] Videoüberwachung

(1) Für die Videoüberwachung öffentlich zugänglicher Räume gilt:

1. öffentliche Stellen dürfen personenbezogene Daten aus optisch-elektronischen Einrichtungen verarbeiten (Videoüberwachung), wenn es für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgaben des Verantwortlichen erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen.

2. nicht-öffentliche Stellen dürfen personenbezogene Daten aus optisch-elektronischen Einrichtungen verarbeiten (Videoüberwachung), wenn es zum Schutz von Leben, Gesundheit oder Freiheit von Personen erforderlich ist, die sich in öffentlich zugänglichen großflächigen Anlagen, insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder Einrichtungen und Fahrzeu-

gen des öffentlichen Personenverkehrs aufhalten, und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen. Bei der Abwägungsentscheidung nach Satz 1 ist der Schutz von Leben, Gesundheit oder Freiheit von Personen, die sich in Anlagen nach Satz 1 aufhalten, in besonderem Maße zu berücksichtigen.

(2) Der Umstand der Videoüberwachung nach Absatz 1 und der Verantwortliche sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Für einen anderen Zweck als zu demjenigen, zu dem die Daten gemäß Absatz 1 erhoben wurden, dürfen sie nur verarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

Kapitel 3
Datenschutzbeauftragte öffentlicher Stellen

§ 5
Benennung

[Art. 37 Abs. 1 lit. a) DS-GVO; Art. 32 Abs. 1 DS-RL] (1) Öffentliche Stellen benennen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln.

(2) ***[Art. 37 Abs. 3 DS-GVO; Art. 32 Abs. 3 DS-RL]*** Für mehrere öffentliche Stellen kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe eine gemeinsame Datenschutzbeauftragte oder ein gemeinsamer Datenschutzbeauftragter benannt werden.

(3) ***[Art. 37 Abs. 5 Ds-GVO; Art. 32 Abs. 2 DS-RL]*** 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) ***[Art. 37 Abs. 6 DS-GVO]*** Die oder der Datenschutzbeauftragte kann Beschäftigte oder Beschäftigter der öffentlichen Stelle sein oder ihre oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(5) ***[Art. 37 Abs. 7 DS-GVO; Art. 32 Abs. 4 DS-RL]*** 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) ***[ex § 4f Abs. 3 Satz 5 und 6 BDSG-alt]*** Die Kündigung des Arbeitsverhältnisses der oder des Datenschutzbeauftragten ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach der Abberufung als Datenschutzbeauftragte oder als Datenschutzbeauftragter ist die Kündigung innerhalb eines Jahres nach der Beendigung der Benennung unzulässig, es sei denn, dass die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

§ 6
Stellung

(1) ***[Art. 38 Abs. 1 DS-GVO; Art. 33 Abs. 1 DS-RL]*** 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) ***[Art. 38 Abs. 2 DS-GVO; Art. 33 Abs. 2 DS-RL]*** 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) ***[Art. 38 Abs. 3 DS-GVO]*** 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 darf von der öffentlichen Stelle wegen der Erfüllung ihrer oder seiner Aufgaben nicht abberufen oder benachteiligt werden. Die oder der Datenschutzbeauftragte berichtet unmittelbar der höchsten Leitungsebene der öffentlichen Stelle.

(4) ***[Art. 38 Abs. 4 DS-GVO]*** 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, dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen. [***Art. 38 Abs. 5 DS-GVO, ex § 4f Abs. 4 BDSG-alt]*** 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.

(5) [***Art. 38 Abs. 5 DS-GVO, ex § 4f Abs. 4a BDSG-alt]*** Wenn die oder der Datenschutzbeauftragte bei der 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) **[Art. 39 Abs. 1 DS-GVO, Art. 34 Abs. 1 DS-RL]** Der oder dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

a) Unterrichtung und Beratung der öffentlichen Stelle und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der Verordnung (EU) 2016/679, diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften;

b) Überwachung der Einhaltung der Verordnung (EU) 2016/679, 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 Schulung der an den Verarbeitungsvorgängen beteiligten Beschäftigten und der diesbezüglichen Überprüfungen;

c) Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgeabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35 der Verordnung (EU) 2016/679 sowie § 62 dieses Gesetzes;

d) Zusammenarbeit mit der Aufsichtsbehörde;

e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36

der Verordnung (EU) 2016/679 und § 64 dieses Gesetzes, und gegebenenfalls Beratung zu allen sonstigen Fragen.

(2) **[Art. 38 Abs. 6 DS-GVO]** 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) **[Art. 39 Abs. 2 DS-GVO]** 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) ***[ex § 22 Abs. 5 BDSG-alt]*** 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. Diesen Stellen dürfen personenbezogene Daten der Beschäftigten übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

§ 9

Zuständigkeit

(1) ***[ex § 24 Abs. 1 BDSG-alt mod.]*** Die oder der Bundesbeauftragte ist zuständig für die Aufsicht über die öffentlichen Stellen des Bundes. ***[ex. § 11 Abs. 4 Nr. 1b mod.]*** 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) ***[ex § 24 Abs. 3 BDSG-alt mod.]*** 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) ***[ex § 22 Abs. 4 S. 2 BDS***G***-alt mod./Art 42 Abse. 1 und 2 DS-RL]*** 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) ***[neu Art. 52 Abs. 6 DS-GVO/ Art. 42 Abs. 6 DS-RL]*** Die oder der Bundesbeauftragte unterliegt der Rechnungsprüfung durch den Bundesrechnungshof, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

§ 11

Ernennung und Amtszeit

(1) ***[ex § 22 Abs. 1 BDSG-alt mod.]*** 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 nachgewiesene Kenntnisse des deutschen und europäischen Datenschutzrechts verfügen und die Befähigung zum Richteramt oder höheren Dienst haben.

(2) ***[ex § 22 Abs. 2 BDSG-alt]*** 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) ***[ex § 22 Abs. 3 BDSG-alt]*** Die Amtszeit der oder des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.

§ 12

Amtsverhältnis

(1) ***[ex § 22 Abs. 4 S. 1 BDSG-alt]*** Die oder der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis.

(2) ***[ex § 23 Abs. 1 BDSG-alt mod.]*** 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 Falle 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) ***[ex § 22 Abs. 6 BDSG-alt]*** 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) ***[ex § 23 Abs. 7 BDSG-alt]*** Die oder der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Ka-

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

lendermonats, in dem das Amtsverhältnis endet, im Falle 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) ***[ex § 23 Abs. 2 BSDG-alt mod.]*** 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) ***[ex § 23 Abs. 3 BSDG]*** 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) ***[ex § 23 Abs. 4 BDSG-alt]*** 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) ***[ex § 23 Abs. 5 BDSG-alt]*** 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 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, 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) ***[ex § 23 Abs. 6 BDSG-alt]*** Die oder der Bundesbeauftragte darf als Zeugin oder Zeuge aussagen, es sei denn, die Aussage würde

1. dem Wohle des Bundes oder eines deutschen 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) ***[ex § 23 Abs. 8 BDSG-alt]*** Absatz 3 und Absatz 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) ***[Art. 46 DS-RL]*** Die oder der Bundesbeauftragte hat unbeschadet der Aufgaben nach der Verordnung (EU) 2016/679 die Aufgabe,

1. die Anwendung der Verordnung (EU) 2016/679, 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 zu sensibilisieren und sie darüber aufzuklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder,

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 zu beraten,

4. die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus der Verordnung (EU) 2016/679, 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 der Verordnung (EU) 2016/679, 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 zusammen zu arbeiten,

6. sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 80 der Verordnung (EU) 2016/679 oder 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 zusammen zu arbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe zu leisten, um die einheitliche Anwendung und Durchsetzung der Verordnung (EU) 2016/679, 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 der Verordnung (EU) 2016/679, 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 Artikel 36 Absatz 2 der Verordnung (EU) 2016/679 und die in Artikel 28 der Richtlinie (EU) 2016/680 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 § 54 wahr.

(2) ***[§ 26 Abs. 2 BDSG-alt mod.]*** Zur Erfüllung der in Absatz 1 Satz 1 Nummer 3 genannten Aufgabe kann sich 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 Anforderung des Deutschen Bundestages oder der Bundesregierung hat die oder der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. 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

[ex § 26 Abs. 1 BDSG-alt mod.] 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 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. ***[ex § 25 Abs. 1 BDSG-alt mod.; Art. 58 Abs. 4 DS-GVO]*** 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 Gelegenheit zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden 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 entgegen steht. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der oder des Bundesbeauftragten getroffen worden sind.

(2) ***[Art. 47 Abs. 2 DS-RL; § 25 BDSG-alt mod.]*** 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 Rechts- oder Fachaufsichtsbehörde und fordert zur Stellungnahme innerhalb einer von ihm oder ihr 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. Der oder die 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) ***[ex § 24 Abs. 2 BDSG-alt]*** 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) [***ex § 24 Abs. 4 BDSG-alt mod.]*** 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,

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

(5) ***[ex § 26 Abs. 4 S. 1 BDSG-alt]*** 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 § 38 hin. § 38 Absatz 2 Satz 1 Halbsatz 2 gilt entsprechend.

Kapitel 5

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

§ 17

[Art. 51 Abs. 3, EG 119 DS-GVO] 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 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.

§ 18

[Art. 68 Abs. 3, 4, EG 119 DS-GVO] 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 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 Artikel 85 und 91 der Verordnung

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

(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 der gemeinsame Vertreter einen Vorschlag fest. In Angelegenheiten, die die Wahrnehmung von Aufgaben betreffen, für welche die Länder alleine das Recht der Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, legt sein Stellvertreter den Vorschlag für einen gemeinsamen 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 und die Angelegenheit die Wahrnehmung von Aufgaben betreffen, für welche die Länder alleine das Recht zur Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betrifft, entscheidet 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 Artikel 4 Nummer 16 der Verordnung (EU) 2016/679 oder seine einzige Niederlassung in der Europäischen Union im Sinne des Artikel 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. Für die Festlegung der federführenden Aufsichtsbehörde findet § 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 der Artikel 60 Absatz 7 bis 9 und 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 der Länder über Rechte gemäß Artikel 78 Ab-

satz 1 und 2 der Verordnung (EU) 2016/679 und § 56 ist der Verwaltungsrechtsweg gegeben. Satz 1 gilt nicht für Straf- und 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.

(8) Die Absätze 1 bis 7 gelten entsprechend für Datenverarbeitung, die zu Zwecken erfolgt, die weder dem Anwendungsbereich der Verordnung (EU) 2016/679 noch demjenigen der Richtlinie (EU) 2016/680 unterfallen.

§ 21
[*Art. 58 Abs. 5 DS-GVO, Art. 47 Abs. 5 DS-RL*] Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Europarechtswidrigkeit eines Angemessenheitsbeschlusses der Kommission

(1) Hält eine Aufsichtsbehörde einen Angemessenheitsbeschluss der Kommission, auf dessen Gültigkeit es bei der Entscheidung über die Beschwerde einer betroffenen Person ankommt, für europarechtswidrig, 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 Kommission Gelegenheit zur Äußerung binnen einer zu bestimmenden Frist geben.

(5) Ist ein Verfahren zur Überprüfung der Gültigkeit des Angemessenheitsbeschlusses der Kommission 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 Angemessenheitsbeschluss der Kommission gültig ist, so stellt es dies in seiner Entscheidung fest. Andernfalls legt es die Frage nach der Gültigkeit des Angemessenheitsbeschlusses der Kommission 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

[ex. § 13 Abs. 2 BDSG-alt mod.; Art. 6 Abs. 1 i.V.m. 9 Abs. 2 DS-GVO] (1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 und unbeschadet anderer Rechtsgrundlagen ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig

1. durch öffentliche und nicht-öffentliche Stellen, wenn

[Art. 9 Abs. 2 lit. b DS-GVO]

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

[ex. § 13 Abs. 2 Nr. 7, § 28 Abs. 7 BDSG-alt, Art. 9 Abs. 2 lit. h, Abs. 3 DS-GVO]

b. sie zum Zweck der Gesundheitsvorsorge oder der Arbeitsmedizin, 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 mit einem Angehörigen eines Gesundheitsberufs, der dem Berufsgeheimnis unterliegt oder durch andere Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, erforderlich ist; [**ex. *§ 28 Abs. 7 Satz 2 BDSG-alt***] die Verarbeitung von Daten zu diesen Zwecken richtet sich nach den für die genannten Personen geltenden Geheimhaltungspflichten,

[Art. 9 Abs. 2 lit. i DS-GVO]

c. sie aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist oder

[Art. 9 II lit. j DS-GVO]

d. sie für im öffentlichen Interesse liegende Archivzwecke oder für statistische Zwecke erforderlich ist;

2. durch öffentliche Stellen, wenn

[ex. § 13 Abs. 2 Nr. 1, 5, 6 und 9 BDSG-alt, Art. 9 Abs. 2 lit. g DS-GVO]

a. sie aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist

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

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

d. sie 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.

(2) Mit Ausnahme des Absatzes 1 Nummer 1 Buchstabe b sind in den Fällen des Absatzes 1 angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen 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 kann dazu unbeschadet der in den Artikeln 25, 32 und 36 der Verordnung (EU) 2016/679 genannten Maßnahmen insbesondere gehören:

1. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,

2. an Verarbeitungsvorgängen Beteiligte zu sensibilisieren und zu schulen.

§ 23
Verarbeitung zu anderen Zwecken

[ex. §§ 13 Abs. 2, 14 Abs. 2 u. 3, 28 Abs. 2, 6 und 8 BDSG-alt mod.; Art. 6 Abs. 4 DS-GVO]

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen ist über Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 hinaus zulässig, wenn

[ex: § 14 Abs. 2 Nr. 3 BDSG-alt]

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,

[ex: § 14 Abs. 2 Nr. 4 BDSG-alt]

2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

[ex: § 14 Abs. 2 Nr. 5 BDSG-alt]

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 Zweckänderung offensichtlich überwiegt,

[ex: § 14 Abs. 2 Nr. 6 BDSG-alt; Art. 23 Abs. 1 lit. a u. b. DS-GVO]

4. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Landesverteidigung oder die nationale Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,

[ex: § 14 Abs. 2 Nr. 7 BDSG-alt]

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 Bußgeldentscheidungen erforderlich ist,

[ex: § 14 Abs. 2 Nr. 8 BDSG-alt]

6. sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder

[ex: § 14 Abs. 3 BDSG-alt]

7. sie für die 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 personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nicht-öffentliche Stellen ist über Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 hinaus nur zulässig, wenn

[ex: § 28 Abs. 3 Nr. 2b BDSG-alt]

1. sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist,

[Art. 23 Abs. 2 lit. j DS-GVO]

2. sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist,

[ex: 28 Abs. 2 Nr. 1 BDSG i.V.m. § 28 Abs. 1 Satz 1 Nr. 2 BDSG]

3. sie zur Wahrung berechtigter Interessen des Verantwortlichen erforderlich ist,

[ex: 28 Abs. 2 Nr. 1 BDSG-alt i.V.m. § 28 Abs. 1 Satz 1 Nr. 3 BDSG-alt]

4. 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 Verarbeitung gegenüber dem berechtigten Interesse des Verantwortlichen offensichtlich überwiegt und kein Grund zu der Annahme besteht, dass die betroffene Person ein schutzwürdiges Interesse an dem Ausschluss der Weiterverarbeitung hat.

(3) 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, durch öffentliche Stellen ist über Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 hinaus zulässig, wenn

[ex: § 14 Abs. 5 Nr. 1 i.V.m. § 13 Abs. 2 Nr. 1 BDSG-alt, Art. 9 Abs. 2 lit g DS-GVO]

1. sie aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist,

[ex: § 14 Abs. 5 Nr. 1 i.V.m. § 13 Abs. 2 Nr. 3 BDSG]

2. sie zum Schutz lebenswichtiger Interessen der betroffenen Person erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben oder

[ex: § 14 Abs. 5 Nr. 1 i.V.m. § 13 Abs. 2 Nr. 4 BDSG-alt]

3. es sich um Daten handelt, die die betroffene Person offenkundig öffentlich gemacht hat.

[ex: § 14 Abs. 5 Nr. 1 i.V.m. § 13 Abs. 2 Nr. 5 BDSG]

4. sie zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit, erforderlich ist,

[ex: § 14 Abs. 5 Nr. 1 i.V.m. § 13 Abs. 2 Nr. 6 BDSG]

5. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,

[ex: § 14 Abs. 6i.V.m. § 13 Abs. 2 Nr. 7 BDSG]

6. sie zum Zweck der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs, der dem Berufsgeheimnis unterliegt oder durch andere Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, erforderlich ist,

[ex: § 14 Abs. 5 Nr. 1 i.V.m. § 13 Abs. 2 Nr. 9 BDSG]

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

[ex: § 16 Abs. 1 Nr. 2 Satz 2 BDSG]

8. sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

(4) 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, durch nicht-öffentliche Stellen ist über Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 hinaus zulässig, wenn

[ex: § 28 Abs. 8 Satz 2 BDSG]

1. sie zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,

[ex: § 28 Abs. 8 Satz 2 BDSG]

2. sie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist,

[ex: § 28 Abs. 8 Satz 1 i.V.m. Abs. 7 Satz 1 BDSG]

3. sie zum Zweck der Gesundheitsvorsorge oder der Arbeitsmedizin, 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 mit einem Angehörigen eines Gesundheitsberufs, der dem Berufsgeheimnis unterliegt oder durch andere Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, erforderlich ist,

[ex: § 28 Abs. 8 Satz 1 i.V.m. Abs. 6 Nr. 1 BDSG]

4. sie zum Schutz lebenswichtiger Interessen der betroffenen Person erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,

[ex: § 28 Abs. 8 Satz 1 i.V.m. Abs. 6 Nr. 2 BDSG]

5. es sich um Daten handelt, die die betroffene Person offenkundig öffentlich gemacht hat oder

[ex: § 28 Abs. 8 Satz 1 i.V.m. Abs. 6 Nr. 3 BDSG]

6. sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Abschnitt 2
Besondere Verarbeitungssituationen

§ 24

[ex. §§ 32, 3 Abs. 11 BDSG-alt, Art. 88 DS-GVO] Datenverarbeitung im Beschäftigungskontext

(1) Vorbehaltlich hiervon abweichender Kollektivvereinbarungen dürfen personenbezogene Daten einer oder eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für dessen Begründung, Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten

einer oder eines 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 verhältnismäßig sind.

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

(3) Beschäftigte sind:

1. Arbeitnehmerinnen und Arbeitnehmer,

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

8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

§ 25

Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken

[Art. 9 Abs. 2 lit. j DS-GVO; ex. § 13 II Nr. 8; § 14 II Nr. 9, V 1 Nr. 2; 28 II Nr. 3, VI Nr. 4 BDSG-alt] (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 für wissenschaftliche oder historische Forschungszwecke zulässig, wenn die Verarbeitung zur Durchführung wissenschaftlicher oder historischer Forschung erforderlich ist. § 22 Absatz 2 gilt entsprechend.

[Art. 23 DS-*GVO*; ex. § 33 II 1 Nr. 5 BDSG-alt] (2) Werden personenbezogene Daten zu eigenen wissenschaftlichen oder historischen Forschungszwecken verarbeitet, bestehen gegenüber nicht-öffentlichen Stellen die Rechte auf Auskunft und Erhalt einer Kopie gemäß Artikel 15 der Verordnung (EU) 2016/679 nicht, wenn die Auskunfts- oder Kopieerteilung einen unverhältnismäßigen Aufwand erfordern würde.

[Art. 9 Abs. 4 DS-*GVO*; ex. § 40 BDSG-alt] (3) Für zu wissenschaftlichen oder historischen Forschungszwecken verarbeitete genetische oder Gesundheitsdaten gilt Folgendes:

1. die Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. 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 Forschungszweck dies erfordert;

2. die wissenschaftliche oder historische Forschung betreibenden Stellen dürfen genetische oder Gesundheitsdaten nur veröffentlichen, wenn die betroffene Person ein-

gewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 26

Verarbeitung von einer Geheimhaltungspflicht unterliegenden Daten

(1) Für Daten, die nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, einer Geheimhaltungspflicht unterliegen, gilt Folgendes:

1. ***[ex. § 19a Abs. 3 i.V.m. § 19 Abs. 4 Nr. 3 BDSG-alt; § 33 Abs. 2 Satz 1 Nr. 3 BDSG-alt; Art. 23 Abs. 1 lit. i) DS-GVO]*** Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, wenn die Daten geheim gehalten werden müssen und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.

2. ***[ex. § 19 Abs. 4 Nr. 3, § 34 Abs. 7 BDSG-alt]*** Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, wenn die betroffene Person nach Nummer 1 nicht zu informieren ist.

[Art. 90 DS-GVO] (2) Wenn Daten im Sinne des Absatzes 1 einer Geheimhaltungspflicht unterliegen, sind die Befugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 auf die Untersuchung beschränkt, ob der Verantwortliche die Anforderungen des Artikels 25 der Verordnung (EU) 2016/679 erfüllt. Erlangt eine Aufsichtsbehörde im Rahmen einer solchen Untersuchung Kenntnis von Daten im Sinne des Absatzes 1, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde und dürfen die Erkenntnisse in einem Strafverfahren nicht verwertet werden.

§ 27

***[ex. §§ 28a, 35 Absatz 2 Satz 3 BDSG-alt]* Datenübermittlung an Auskunfteien**

(1) Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und

1. die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,

2. die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,

3. die betroffene Person die Forderung ausdrücklich anerkannt hat,

4. a) die betroffene Person nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,

   b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,

   c) der Verantwortliche die betroffene Person rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und

   d) die betroffene Person die Forderung nicht bestritten hat oder

5. das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und der Verantwortliche die betroffenen Person über die bevorstehende Übermittlung unterrichtet hat.

Satz 1 gilt entsprechend, wenn der Verantwortliche selbst die Daten geschäftsmäßig zum Zweck der Übermittlung verarbeitet, weil dies seiner Tätigkeit als Auskunftei dient.

(2) Zur zukünftigen Übermittlung für eine Datenverarbeitung von Auskunfteien gemäß § 28 dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Absatz 1 Satz 2 Nummer 2, 8 oder Nummer 9 des Kreditwesengesetzes an Auskunfteien übermitteln, es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. Die betroffene Person ist vor Abschluss des Vertrages hierüber zu unterrichten. Satz 1 gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben. Zur zukünftigen Übermittlung für eine Datenverarbeitung von Auskunfteien gemäß § 28 ist die Übermittlung von Daten über Verhaltensweisen der betroffenen Person, die im Rahmen eines vorvertraglichen Vertrauensverhältnisses der Herstellung von Markttransparenz dienen, an Auskunfteien auch mit Einwilligung der betroffenen Person unzulässig.

(3) Nachträgliche Änderungen der einer Übermittlung nach Absatz 1 oder Absatz 2 zugrunde liegenden Tatsachen hat der Verantwortliche der Auskunftei innerhalb von einem Monat nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Auskunftei hat die übermittelnde Stelle über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

(4) Personenbezogene Daten, die auf der Grundlage des Absatzes 2 Satz 1 gespeichert werden, sind nach Beendigung des Vertrages auch zu löschen, wenn die betroffene Person dies verlangt.

§ 28

[ex. § 28 b BDSG-alt] Scoring

Zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit der betroffenen Person darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten der betroffenen Person erhoben oder verwendet werden, wenn

1. 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,
2. hinsichtlich der für die Berechnung des Wahrscheinlichkeitswerts genutzten Daten die Voraussetzungen für eine Übermittlung vorliegen und die Verarbeitung durch den Verantwortlichen zulässig ist,
3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,
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.

§ 29

[ex. § 29 Abs. 6 und 7 BDSG-alt; Verbraucherkredit-RL 2008/48/EG] 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 oder anderen Vertragsstaaten des Ab-

kommens über den Europäischen Wirtschaftsraum 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. § 35 bleibt unberührt.

Kapitel 2
Rechte der betroffenen Person

§ 30
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 nicht, wenn die Erteilung der Information

[23 Absatz 1 lit. i); Rechtsgedanke Art. 14 Abs. 5 lit. b); 23 Abs. 2 lit. h) DS-GVO]

1. sich als unmöglich erweist,
2. einen unverhältnismäßigen Aufwand erfordern würde, oder
3. voraussichtlich die Verwirklichung der Ziele der Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen würde und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie 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. Der Verantwortliche legt schriftlich fest, unter welchen Voraussetzungen von einer Information abgesehen wird.

(3) Wenn sich die Pflicht zur Information der betroffenen Person in den Fällen des Artikel 13 Absatz 1 und 2 zum Zeitpunkt der Erhebung der Daten bei der betroffenen Person oder in den Fällen des Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 zum Zeitpunkt der Weiterverarbeitung als unmöglich erweist, 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. Unbeschadet dessen ist bei der Videoüberwachung öffentlich zugänglicher Räume der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

§ 31
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 und 2 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, wenn

1. im Falle einer öffentlichen Stelle

[ex. § 19a Abs. 3 i.V.m. § 19 Abs. 4 Nr. 1 BDSG-alt; Art. 23 Abs. 1 lit. c), d) und e) DS-GVO]

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

a) die Information die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben gefährden würde oder

[ex. § 19a Abs. 3 i.V.m. § 19 Abs. 4 Nr. 2 BDSG-alt; Art. 23 Abs. 1 lit. a), c) u. d) i.V.m. Abs. 2 lit. c) DS-GVO]

b) die Information die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde

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

2. im Falle einer nicht-öffentlichen Stelle

[ex. § 33 Abs. 2 Satz 1 Nr. 7 Buchstabe b BDSG-alt; Art. 23 Abs. 1 lit. i) i.V.m. Abs. 2 lit. c DS-GVO]

a) die Information die Geschäftszwecke des Verantwortlichen erheblich gefährden würde, es sei denn, dass das Interesse der betroffenen Person an der Information überwiegt, oder

[ex. § 33 Abs. 2 Satz 1 Nr. 6 BDSG-alt; Art. 23 Abs. 1 lit. a) bis e)) i.V.m. Abs. 2 lit. c DS-GVO]

b) die zuständige öffentliche Stelle gegenüber dem Verantwortlichen festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

[Art. 14 Abs. 5 lit. b Satz 1 DS-GVO]

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Aritkel 14 Absatz 1 und 2 der Verordnung (EU) 2916/679 genannten Informationen für die Öffentlichkeit. Der Verantwortliche legt schriftlich fest, unter welchen Voraussetzungen von einer Information abgesehen wird.

(3) ***[§ 19a Abs. 3 i.V.m. § 19 Abs. 3 BDSG-alt; Art. 23 Abs. 1 lit. a, b i.V.m. Abs. 2 lit. c und e DS-GVO]*** 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.

§ 32

Auskunftsrecht der betroffenen Person

(1) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, wenn

1. ***[ex § 19 Abs. 2 bis 4; § 33 Abs. 7 BDSG- alt]*** die betroffene Person nach § 31 Absatz 1 und 3 nicht zu informieren ist,

2. ***[ex. § 19a Abs. 3 i.V.m. § 19 Abs. 2 BDSG- alt; § 33 Abs. 2 Satz 1 Nr. 2, Art. 23 Abs. 1 lit. h) i.V.m. Abs. 2 lit. c DS-GVO]*** die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger 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, oder

3. [**ex § 19 Abs. 1 Satz 3]** 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.

(2) [***ex § 34 Abs. 1 Satz 4 BDSG-alt***] Unbeschadet des Absatzes 1 kann eine nichtöffentliche Stelle die Auskunft über die in Artikel 15 Absatz 1 Buchstabe c und g sowie Absatz 2 der Verordnung (EU) 2016/679 genannten Informationen verweigern, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse der betroffenen Person überwiegt.

(3) ***[ex. § 19 Abs. 5 BDSG-alt mod.]*** 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. **[ex § 34 Absatz 5 BDS-alt mod.]** 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.

(4) ***[ex. § 19 Abs. 6 BDSG-alt]*** 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 betroffenene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Auskunft zustimmt.

§ 33

Recht auf Löschung

[ex § 20 Abs. 3, § 35 Abs. 3 BDSG-alt, Art. 23 Abs. 1 lit. i i.V.m. Abs. 2 lit. c DS-GVO]

(1) 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 und die Pflicht des Verantwortlichen zur Gewährleistung der Speicherbegrenzung gemäß Artikel 5 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 bestehen ergänzend zu den in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, wenn eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679.

(2) Ergänzend zu Artikel 18 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 gilt Absatz 1 entsprechend im Fall des Artikel 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 Artikel 17 Absatz 1 Buchstabe a der Verordnung 2016/679, wenn einer Löschung satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

§ 34

Widerspruchsrecht

[ex § 20 Absatz 5 Satz 2 BDSG-alt, Art. 23 Abs. 1 i.V.m. Abs. 2 lit. c DS-GVO]
Das Recht auf Widerspruch gemäß Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 besteht nicht, wenn die Verarbeitung zu einem der in § 22 Absatz 1 genannten Zwecke erforderlich ist und der Widerspruch die Verwirklichung des Zwecks der Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen würde. Die Daten dürfen nur für die Zwecke des § 22 Absatz 1 verarbeitet werden; die Verarbeitung für andere Zwecke ist nur unter den Voraussetzungen des Artikels 21 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 zulässig.

§ 35

Automatisierte Einzelentscheidungen im Einzelfall einschließlich Profiling

[ex. § 6a Abs. 2 BDSG; Art. 22 Abs. 2 lit. b DS-GVO] Das Recht gemäß Artikel 22 Absatz 1 der Verordnung (EU) 2016/679, keiner ausschließlich auf einer automatisierten Verarbeitung berufenden Entscheidung unterworfen zu werden, besteht ergänzend zu den Ausnahmen des Artikel 22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 nicht, wenn die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrags- oder sonstigen Rechtsverhältnisses ergeht und dem Begehren der betroffenen Person stattgegeben wurde. Wird dem Begehren der betroffenen Person nicht stattgegeben, gelten Artikel 13 Absatz 2 Buchstabe f, Artikel 14 Absatz 2 Buchstabe g und Artikel 22 Absatz 3 der Verordnung (EU) 2016/679 entsprechend.

Kapitel 3
Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 36

Datenschutzbeauftragte nicht-öffentlicher 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 Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegt 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 bestellen.

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

§ 37

Akkreditierung

Die Akkreditierung der Zertifizierungsstellen gemäß Artikel 43 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 erfolgt durch die Aufsichtsbehörden des Bundes und der Länder im Rahmen ihrer jeweiligen Zuständigkeit oder durch die Deutsche Akkreditierungsstelle. Die Aufsichtsbehörden und die Deutsche Akkreditierungsstelle unterrichten sich gegenseitig über die Erteilung, Versagung oder den Widerruf einer Akkreditierung.

Kapitel 4
Aufsichtsbehörde für die Datenverarbeitung durch nicht-öffentliche Stellen

§ 38
Aufsichtsbehörden der Länder

(1) ***[ex § 38 Abs. 1 S. 1 mod.]*** Die nach Landesrecht zuständigen Behörden (Aufsichtsbehörden der Länder) überwachen im Anwendungsbereich der Verordnung (EU) 2016/679 bei den nicht-öffentlichen Stellen die Anwendung der Vorschriften über den Datenschutz.

(2) ***[ex § 38 Abs. 1 S. 3 und 6]*** Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten; insbesondere darf die Aufsichtsbehörde zum Zweck der Aufsicht 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 Bußgeldentscheidungen 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. ***[ex § 38 Abs. 1 S. 8 BDSG-alt mod.]*** § 13 Absatz 4 Satz 4 bis 7 gelten entsprechend.

(3) ***[ex § 38 Abs. 3]*** Die der Aufsicht unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der 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) ***[ex § 38 Abs. 4 S. 1 mod.]*** Die von der Aufsichtsbehörde mit der Überwachung der Einhaltung der Vorschriften über den Datenschutz beauftragten Personen sind befugt, zur Erfüllung ihrer Aufgaben während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und Zugang zu allen Datenverarbeitungsanlagen und -geräten zu erhalten.

(5) ***[ex § 38 Abs. 1 Satz 2 mod.]*** Die Aufsichtsbehörde berät und unterstützt die Datenschutzbeauftragten mit Rücksicht auf deren typische Bedürfnisse. ***[ex § 38 Abs. 5 S. 3 BDSG-alt]*** Sie kann 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) ***[ex § 38 Abs. 7]*** Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnittes unterliegenden Gewerbebetriebe bleibt unberührt.

Kapitel 5
Sanktionen

§ 39

[Art. 83 Abs. 8 DS-GVO] 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 §§ 9, 17, 30, 35, 36 und 130 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung.

(2) Für Verfahren wegen eines Verstoßes nach Artikel 83 Absatz 4 bis 6 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, 100 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung. § 68 des Gesetzes über Ordnungswidrigkeiten findet mit der Maßgabe Anwendung, dass das Landgericht entscheidet, wenn der Betrag einer Geldbuße die Summe von fünftausend Euro übersteigt. § 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.

§ 40

[ex. § 43 Abs. 1 Nr. 7a und b BDSG-alt; Art. 83 Abs. 7 DS-GVO] Weitere Vorschriften für die Verhängung von Geldbußen

(1) Ordnungswidrig handelt, wer in Ausübung seiner Tätigkeit für den Verantwortlichen oder Auftragsverarbeiter vorsätzlich oder fahrlässig einen der in Artikel 83 Absatz 4, 5 oder 6 der Verordnung (EU) 2016/679 genannten Verstöße begeht. Die Ordnungswidrigkeit kann im Fall des Satzes 1 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 29 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder entgegen § 29 Absatz 2 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Nummer 1 werden keine Geldbußen verhängt. Satz 1 gilt nicht für öffentliche Stellen, soweit die Verarbeitung im Rahmen einer Tätigkeit erfolgt, hinsichtlich derer die öffentliche Stelle mit anderen Verarbeitern im Wettbewerb steht.

[ex. § 42a Satz 6 BDSG-alt] (4) Eine Meldung, die die oder der Meldepflichtige nach Artikel 33 der Verordnung (EU) 2016/679 erteilt hat, darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen sie oder ihn oder in § 52 Absatz 1 der Strafprozessordnung bezeichnete Angehörige nur mit Zustimmung der oder des Meldepflichtigen verwendet werden.

§ 41

Strafbare Handlungen

[ex. § 44 Abs. 1 BDSG-alt] Wer eine in Artikel 83 Absatz 5 der Verordnung (EU) 2016/679 bezeichnete Handlung vorsätzlich gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 42

Strafantrag und Verwendung von Meldungen

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

[ex. § 44 Abs. 2 BDSG-alt] (1) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

[ex. § 42a Satz 6 BDSG-alt] (2) Eine Meldung, die die oder der Meldepflichtige nach Artikel 33 der Verordnung (EU) 2016/679 erteilt hat, darf in einem Strafverfahren gegen sie oder ihn oder in § 52 Absatz 1 der Strafprozessordnung bezeichnete Angehörige der oder des Meldepflichtigen nur mit Zustimmung der oder des Meldepflichtigen verwendet werden.

Teil 3

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

Kapitel 1

Anwendungsbereich und Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 43

Anwendungsbereich

[Art. 1 Abs. 1; Art. 2 Abs. 1 DS-RL] Die Vorschriften dieses Teils gelten unbeschadet spezieller Regelungen in den entsprechenden Fachgesetzen für die Verarbeitung personenbezogener Daten durch 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 zuständigen öffentlichen Stellen des Bundes, soweit diese personenbezogene Daten zu diesen Zwecken verarbeiten.

§ 44

Verarbeitung personenbezogener Daten

(1) **[Art. 8 Abs. 1 DS-RL]** Die Verarbeitung personenbezogener Daten ist zulässig, wenn diese Verarbeitung für die Aufgabenerfüllung zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit erforderlich ist und keine spezielleren Regelungen in anderen Gesetzen vorgehen.

[Art. 8 Abs. 2 DS-RL] In Rechtsvorschriften, die eine Verarbeitung regeln, müssen zumindest die Ziele und Zwecke der Verarbeitung sowie die personenbezogenen Daten, die verarbeitet werden sollen, angegeben werden.

(2) **[Art. 4 Abs. 3 DS-RL]** Die Verarbeitung kann zu im öffentlichen Interesse liegenden archivarischen, wissenschaftlichen oder statistischen Zwecken erfolgen, wenn sie von den in § 43 genannten Zwecken umfasst ist und wenn geeignete Garantien für die Rechtsgüter der betroffenen Personen vorhanden sind.

(3) **[Art. 9 Abs. 3 DS-RL]** Bei Datenübermittlungen weist die übermittelnde Stelle den Empfänger gegebenenfalls darauf hin, dass für die Verarbeitung der übermittelten Daten besondere Bedingungen gelten und diese einzuhalten sind.

(4) **[§ 4 Abs. 1 am Ende BDSG-alt, ErwG 35 DS-RL]** Unbeschadet Absatz 1 ist eine Verarbeitung aufgrund einer Einwilligung der betroffenen Person zulässig, wenn die Voraussetzungen des § 47 gegeben sind.

§ 45

Verarbeitung besonderer personenbezogener Daten

(1) **[Art. 10 DS-RL]** Die Verarbeitung besonderer personenbezogener Daten im Sinne des Absatzes 2 ist unbeschadet § 44 Absatz 1 Satz 1 nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist und wenn

1. dies in einer sonstigen Rechtsvorschrift vorgesehen ist,

2. dies zur Wahrung lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich ist,

3. es sich um Daten handelt, die die betroffene Person offenkundig öffentlich gemacht hat oder

4. **[§ 13 Abs. 2 Nr. 2 BDSG-alt]** die betroffene Person eingewilligt hat.

Die Verarbeitung muss vorbehaltlich geeigneter Garantien für die Rechtsgüter der betroffenen Person erfolgen. Geeignete Garantien können unter anderem in spezifischen Anforderungen der Datensicherheit, der Festlegung von besonderen Aussonderungsprüffristen oder der Datenschutzkontrolle bestehen.

(2) Besondere personenbezogene Daten sind

1. solche, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,

2. genetische Daten,

3. biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,

4. Gesundheitsdaten,

5. Daten zum Sexualleben oder der sexuellen Orientierung.

§ 46
Zweckbindung und -änderung

(1) **[Art. 4 Abs. 2 DS-RL]** Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn

1. es sich bei diesem anderen Zweck um einen der in § 43 genannten Zwecke handelt und sie für diesen anderen Zweck erforderlich und verhältnismäßig ist oder

2. **[§ 14 Absatz 3 BDSG-alt; § 23 Absatz 1 Nummer 7 BDSG-neu]** sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für den Verantwortlichen dient. Das gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(2) **[Art. 9 Abs. 1 DS-RL]** Auf eine Verarbeitung von personenbezogenen Daten, die für einen der in § 43 genannten Zwecke erhoben wurden, zu nicht von den in § 43 genannten umfassten Zwecken findet § 23 Anwendung.

§ 47
Einwilligung

(1) **[Art. 7 Abs. 1 DS-GVO]** Erfolgt die Verarbeitung personenbezogener Daten aufgrund einer Einwilligung, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können.

(2) **[Art. 7 Abs. 2 DS-GVO]** 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) **[Art. 7 Abs. 3 DS-GVO]** 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 wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt.

(4) **[Art. 7 Abs. 4 DS-GVO]** Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. **[§ 4a Abs. 1 BDSG-alt]** 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 sowie, wenn nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

(5) **[§ 4a Abs. 3 BDSG-alt]** Soweit besondere personenbezogene Daten gemäß § 45 Absatz 2 verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

§ 48
Verarbeitung unter Weisung des Verantwortlichen oder des Auftragsverarbeiters

[Art. 23 DS-RL] Jede dem 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 dem Unionsrecht oder einer sonstigen Rechtsvorschrift zur Verarbeitung verpflichtet ist.

§ 49
Datengeheimnis

[§ 5 BDSG-alt] Den mit der Verarbeitung befassten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 50
Automatisierte Einzelentscheidung

(1) **[Art. 11 DS-RL; § 6a Abs. 1 am Ende BDSG-alt]** Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, etwa auf der Grundlage von Profiling, die eine nachteilige Rechtsfolge für die betroffene Person hat oder sie erheblich beeinträchtigt, ist nur zulässig, wenn dies im Unionsrecht oder einer sonstigen Rechtsvorschrift vorgesehen ist und dort sichergestellt ist, dass die berechtigten Interessen und Rechtsgüter der betroffenen Person durch geeignete Maßnahmen und Garantien gewahrt werden, zumindest aber, dass eine inhaltliche Bewertung und darauf gestützte Entscheidung durch den Verantwortlichen erwirkt werden kann.

(2) Entscheidungen nach Absatz 1 dürfen nicht auf besonderen personenbezogener Daten nach § 45 Absatz 2 beruhen, wenn nicht geeignete Maßnahmen zum Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Personen getroffen wurden.

Kapitel 3
Rechte der betroffenen Person

§ 51
Auskunftsrecht

(1) **[Art. 14 DS-RL]** Der betroffenen Person ist auf Antrag Auskunft zu erteilen, ob sie betreffende personenbezogene Daten verarbeitet werden. Sie hat darüber hinaus das Recht, Informationen zu erhalten über

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind sowie alle verfügbaren Informationen über die Herkunft der Daten,

2. die Zwecke der Verarbeitung und deren Rechtsgrundlage,

3. die Kategorien personenbezogener Daten, die verarbeitet werden,

4. die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind, insbesondere bei Empfängern in Drittstaaten oder bei internationalen Organisationen,

5. falls möglich die Speicher- oder Aussonderungsprüffrist oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Frist,

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

7. das Bestehen des Rechts, die Datenschutzaufsicht anzurufen sowie Angaben zu deren Erreichbarkeit.

(2) **[§ 19 Abs 2 BDSG-alt; § 32 Abs. 1 Nr. 2 BDSG-neu]** Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(3) **[§ 19 Abs 1 S. 3 BDSG-alt; § 32 Abs. 1 Nr. 3 BDSG-neu]** Die Auskunftserteilung unterbleibt, 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) **[Art. 15 Abs. 1 DS-RL]** Der Verantwortliche kann von der Auskunft nach Absatz 1 Satz 1 absehen und die Auskunftserteilung nach Absatz 1 Satz 2 teilweise oder vollständig einschränken, wenn andernfalls

1. behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren gefährdet werden,

2. die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung gefährdet werden,

3. die öffentliche Sicherheit oder Ordnung durch Erteilung der Auskunft gefährdet wird oder

4. die Rechtsgüter Dritter gefährdet werden.

[§ 19 Abs. 3 BDSG-alt] 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.

(5) **[Art. 15 Abs. 3 S. 1 und 2 DS-RL]** Der Verantwortliche unterrichtet die betroffene Person unverzüglich schriftlich über die Verweigerung oder die Einschränkung der Auskunft und die Gründe hierfür. Dies gilt nicht, soweit die Erteilung dieser Informationen einem der in Absatz 4 genannten Zwecke zuwiderliefe. **[§ 19 Abs. 5 S. 1 BDSG-alt]** Einer Begründung bedarf es insbesondere nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

(6) **[Art. 17 Abs. 1 DS-RL]** Wird die betroffene Person nach Absatz 5 über die Verweigerung oder die Einschränkung der Auskunft unterrichtet, kann die betroffene Person ihr Auskunftsrecht auch über die Bundesbeauftragte oder den Bundesbeauftragten aus-

üben. **[Art. 17 Abs. 2 DS-DL]** Der Verantwortliche unterrichtet die betroffene Person über diese und über die Möglichkeit, gemäß § 55 die Bundesbeauftragte oder den Bundesbeauftragten anzurufen oder gerichtlichen Rechtsschutz zu suchen. **[§ 19 Abs. 6 S. 1 BDSG-alt]** 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. **[Art. 17 Abs. 3 S. 1 DS-RL]** Die oder der Bundesbeauftragte unterrichtet die betroffene Person zumindest darüber, dass alle erforderlichen Prüfungen oder eine Überprüfung erfolgt sind. Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. **[§ 19 Abs. 6 S. 1 BDSG-alt]** Die Mitteilung der oder des Bundesbeauftragten an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, wenn er nicht einer weitergehenden Auskunft zustimmt. **[Art. 17 Abs. 3 S. 2 DS-RL]** Die oder der Bundesbeauftragte hat zudem die betroffene Person über ihr Recht auf einen gerichtlichen Rechtsbehelf zu unterrichten.

(7) **[Art. 15 Abs. 4 DS-RL]** Der Verantwortliche dokumentiert die sachlichen oder rechtlichen Gründe für die Entscheidung.

§ 52
Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) **[Art. 16 Abs. 1 und 3 DS-RL]** Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung die Einschränkung der Verarbeitung; in diesem Fall unterrichtet der Verantwortliche die betroffene Person, bevor er die Beschränkung aufhebt. Unter Berücksichtigung der Verarbeitungszwecke hat die betroffene Person weiterhin das Recht, auch mittels einer ergänzenden Erklärung die Vervollständigung unvollständiger personenbezogener Daten zu verlangen. **[Art. 16 Abs. 5 DS-RL]** Der Verantwortliche teilt der Stelle, die die personenbezogenen Daten zuvor an den Verantwortlichen übermittelt hat, die Berichtigung mit.

(2) **[Art. 16 Abs. 2 DS-RL]** Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender personenbezogener Daten zu verlangen, wenn ihre Verarbeitung unzulässig oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist.

(3) **[Art. 16 Abs. 3 DS-RL; § 20 Abs. 3 BDSG-alt]** Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigt würden,

2. die personenbezogenen Daten für Zwecke eines gerichtlichen Verfahrens weiter aufbewahrt werden müssen oder

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

[§ 32 Abs. 2 S. 3 BKAG] In ihrer Verarbeitung eingeschränkte Daten dürfen nur für den Zweck verarbeitet werden, für den die Löschung unterblieben ist; sie dürfen auch verarbeitet werden, wenn dies zur Behebung einer bestehenden Beweisnot unerlässlich ist oder die betroffene Person einwilligt.

(4) **[Art. 16 Abs. 6 DS-RL; Art. 7 Abs. 3 DS-RL]** In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1, 2 und 3 gilt § 70 Absatz 4 entsprechend.

(5) **[Art. 16 Abs. 4 DS-RL]** Der Verantwortliche unterrichtet die betroffene Person schriftlich über eine Verweigerung der Berichtigung oder Löschung personenbezogener

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung und über die Gründe hierfür. Dies gilt nicht, wenn die Erteilung dieser Informationen einem der in § 51 Absatz 4 genannten Zwecke zuwiderliefe. Einer Begründung bedarf es insbesondere nicht, wenn durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Unterrichtungsverweigerung verfolgte Zweck gefährdet würde.

(6) § 51 Absätze 6 und 7 finden entsprechende Anwendung.

§ 53

Zweckbindung für Daten über die Ausübung von Rechten der betroffenen Person

[§ 6 Abs. 3 BDSG-alt] Personenbezogene Daten über die Ausübung eines Rechts der betroffenen Person, das sich aus diesem Gesetz oder aus einer anderen Rechtsvorschrift über den Datenschutz ergibt, dürfen nur zur Erfüllung der sich aus der Ausübung des Rechts ergebenden Pflichten des Verantwortlichen verwendet werden.

§ 54

Verfahren für die Ausübung der Rechte der betroffenen Person

(1) **[Art. 12 Abs. 3 DS-RL]** Unbeschadet des § 51 Absatz 5 und § 52 Absatz 5 setzt der Verantwortliche die betroffene Person unverzüglich schriftlich darüber in Kenntnis, wie mit ihrem Antrag verfahren wurde.

(2) **[Art. 12 Abs. 4 DS-RL]** Benachrichtigungen nach den §§ 66 und 67, Mitteilungen nach § 60 und die Bearbeitung von Anträgen nach den §§ 51 und 52 erfolgen für die betroffene Person unentgeltlich. Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen der betroffenen Person nach den §§ 51 und 52 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 trägt der Verantwortliche die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter des Antrags.

(3) **[Art. 12 Abs. 5 DS-RL]** Hat der Verantwortliche begründete Zweifel an der Identität der betroffenen Person, die den Antrag nach § 51 oder § 52 stellt, so kann er bei der betroffenen Person zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

§ 55
Anrufung der oder des Bundesbeauftragten

(1) **[Art. 52 Abs. 1 DS-RL; § 21 BDSG-alt]** Jede betroffene Person kann sich unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs mit einer Beschwerde an die Bundesbeauftragte oder den Bundesbeauftragten wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen des Bundes zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit in ihren Rechten verletzt worden zu sein. Für die Verarbeitung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden. Die oder der Bundesbeauftragte unterrichtet die betroffene Person über den Stand und das Ergebnis der Beschwerde und weist sie hierbei auf die Möglichkeit gerichtlichen Rechtsschutzes nach § 56 hin.

(2) **[Art. 52 Abs. 2 DS-RL]** Die oder der Bundesbeauftragte leitet 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 weiter. Die betroffene Person wird über die Weiter-

leitung unterrichtet. Die oder der Bundesbeauftragte leistet der betroffenen Person auf deren Ersuchen weitere Unterstützung.

§ 56
Rechtsschutz gegen Anordnungen der oder des Bundesbeauftragten oder bei deren oder dessen Untätigkeit

(1) **[Art. 53 Abs. 1 DS-RL]** Jede natürliche oder juristische Person kann unbeschadet anderer Rechtsbehelfe gerichtlich gegen eine verbindliche Anordnung der oder des Bundesbeauftragten vorgehen. § 20 findet Anwendung.

(2) **[Art. 53 Abs. 2 DS-RL]** Absatz 1 gilt entsprechend zugunsten betroffener Personen, wenn sich die oder der Bundesbeauftragte nicht mit einer Beschwerde nach § 55 befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.

Kapitel 3
Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 57
Auftragsverarbeitung

(1) **[§ 11 Abs. 1 BDSG-alt]** Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die Rechte der betroffenen Person auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind ihm gegenüber geltend zu machen.

(2) **[Art. 22 Abs. 1 DS-RL]** Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(3) **[Art. 22 Abs. 2 DS-RL]** Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung unterrichtet der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(4) **[Art. 28 Abs. 4 DS-GVO]** Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 6 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den gesetzlichen Anforderungen erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) **[Art. 28 Abs. 5 DS-GVO]** Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 der Verordnung 2016/679 oder eines genehmigten Zertifizierungsverfahrens

gemäß Artikel 42 der Verordnung 2016/679 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 2 und 4 nachzuweisen.

(6) **[Art. 22 Abs. 3 DS-RL; Art. 28 Abs. 3 DS-GVO; § 11 Abs. 2 und 3 BDSG-alt]** Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und der den Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

1. **[Art. 28 Abs. 3 Buchst. a DS-GVO; § 11 Abs. 3 S. 2 BDSG-alt]** nur auf dokumentierte Weisung des Verantwortlichen handelt; falls der Auftragsverarbeiter der Auffassung ist, dass eine Weisung gegen dieses Gesetz oder gegen andere anwendbare Datenschutzbestimmungen verstößt, informiert er den Verantwortlichen unverzüglich;

2. gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer 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 bzw. löscht und bestehende Kopien vernichtet, wenn nicht nach dem Unionsrecht oder sonstigen Rechtsvorschriften eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

5. **[Art. 28 Abs. 3 Buchst. h DS-GVO]** dem Verantwortlichen alle erforderlichen Informationen, insbesondere die gemäß § 71 generierten Protokolle, zum Nachweis der Einhaltung der hier niedergelegten Pflichten zur Verfügung stellt und Überprüfungen, die von dem Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt;

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

7. **[Art. 28 Abs. 3 Buchst. c DS-GVO]** alle gemäß § 58 erforderlichen Maßnahmen ergreift;

8. **[Art. 28 Abs. 3 Buchst. f DS-GVO]** unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in §§ 58 bis 60 und §§ 62 und 63 genannten Pflichten unterstützt.

(7) **[Art. 22 Abs. 4 DS-RL]** Der Vertrag oder das andere Rechtsinstrument im Sinne des Absatzes 6 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. **[§ 11 Abs. 2 S. 3 BDSG-alt]** Der Auftrag kann auch durch die zuständige Fachaufsichtsbehörde erteilt werden.

(8) **[Art. 22 Abs. 5 DS-RL]** Ein Auftragsverarbeiter, der unter Verstoß gegen diese Vorschrift die Zwecke und Mittel der Verarbeitung bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

(9) **[§ 11 Abs. 2 S. 4 und 5 BDSG-alt]** Der Verantwortliche hat sich vor Beginn der Verarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(10) **[§ 11 Abs. 5 BDSG-alt]** Die Absätze 1 bis 9 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen

durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 58

Anforderungen an die Sicherheit der Datenverarbeitung

(1) **[Art. 29 DS-RL]** Der Verantwortliche und der Auftragsverarbeiter treffen 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 Gefährdung für die Rechtsgüter der betroffenen Person erforderliche technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des § 45 Absatz 2. Der Verantwortliche berücksichtigt hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik. **[§ 9 S. 2 BDSG-alt]** Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(2) **[Art. 32 Abs. 1 Buchst. a-c DS-GVO]** Die in Absatz 1 genannten Maßnahmen schließen unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten ein, wenn dies angesichts der Verarbeitungszwecke möglich ist. Sie verfolgen darüber hinaus das Ziel,

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, und

2. die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

(3) **[§ 9 BDSG-alt inkl. Anhang]** Bei der automatisierten Verarbeitung ergreift der Verantwortliche oder der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen, 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 ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugangskontrolle),

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 wird (Transportkontrolle),

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

10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),

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

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

13. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Ein Zweck nach Satz 1 Nummer 1 bis 6 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

§ 59

Meldung von Datensicherheitsvorfällen an die oder den Bundesbeauftragten

[Art. 30 DS-RL] (1) Der Verantwortliche meldet Datensicherheitsvorfälle unverzüglich und möglichst binnen 72 Stunden, nachdem ihm diese bekannt wurden, dem oder der Bundesbeauftragten, es sei denn, dass der Datensicherheitsvorfall voraussichtlich nicht zu einer Gefahr für die Rechtsgüter natürlicher Personen führt. Erfolgt die Meldung an die Bundesbeauftragte oder den Bundesbeauftragten nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter ein Datensicherheitsvorfall bekannt wird, meldet er diesen dem Verantwortlichen unverzüglich.

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

1. eine Beschreibung der Art des Datensicherheitsvorfalls, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien personenbezogener Daten und der ungefähren Zahl der betroffenen personenbezogenen Datensätze,

2. Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,

3. eine Beschreibung der wahrscheinlichen Folgen des Datensicherheitsvorfalls und

4. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung des Datensicherheitsvorfalls und gegebenenfalls der Maßnahmen zur Abmilderung seiner möglichen nachteiligen Auswirkungen.

(4) Wenn die Informationen nicht zur gleichen Zeit bereitgestellt werden können, darf der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Der Verantwortliche dokumentiert Datensicherheitsvorfälle nach Absatz 1 einschließlich aller im Zusammenhang mit ihnen stehenden Tatsachen, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen.

(6) Soweit von dem Datensicherheitsvorfall personenbezogene Daten betroffen sind, die von dem oder an den Verantwortlichen in einem anderen Mitgliedstaat übermit-

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

telt wurden, werden die in Absatz 3 genannten Informationen dem Verantwortlichen in jenem Mitgliedstaat unverzüglich übermittelt.

(7) **[§ 42a S. 6 BDSG-alt mod.]** Der Inhalt einer Meldung nach Absatz 1 darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen eine im Verantwortungsbereich des Verantwortlichen beschäftigte Person nur mit Zustimmung des Verantwortlichen verwendet werden.

(8) Weitere Pflichten des Verantwortlichen zur Benachrichtigung überDatensicherheitsvorfälle bleiben unberührt.

§ 60

Benachrichtigung der betroffenen Person bei Datensicherheitsvorfällen

[Art. 31 DS-RL] (1) Wenn ein Datensicherheitsvorfall voraussichtlich eine hohe Gefährdung für die Rechtsgüter natürlicher Personen zur Folge hat, benachrichtigt der Verantwortliche die betroffene Person unverzüglich über die Verletzung.

(2) Die in Absatz 1 dieses Artikels genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art des Datensicherheitsvorfalls und enthält zumindest die in § 59 Absatz 3 Nummern 2 bis 4 genannten Informationen und Maßnahmen.

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn

1. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen auf die von dem Vorfall betroffenen personenbezogenen Daten angewandt hat, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung,

2. der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass die erhebliche Gefahr für die Rechtsgüter der betroffenen Person gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht 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 betroffene Person nicht bereits über den Datensicherheitsvorfall benachrichtigt hat, kann die oder der Bundesbeauftragte unter Berücksichtigung der Wahrscheinlichkeit, mit der der Datensicherheitsvorfall zu einer erheblichen Gefahr führt, von dem Verantwortlichen verlangen, dies nachzuholen oder sie oder er kann förmlich feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

(5) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 kann unter den in § 51 Absatz 4 genannten Voraussetzungen und aus den dort genannten Gründen aufgeschoben, eingeschränkt oder unterlassen werden.

§ 61

Durchführung einer Datenschutzfolgenabschätzung

[Art. 27 DS-RL] (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 hohe Gefährdung 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) **[Art. 35 Abs. 1 Nr. 2 DS-GVO]** Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohem Gefährdungspotential kann eine einzige Abschätzung vorgenommen werden.

(3) **[Art. 35 Abs. 2 DS-GVO]** Der Verantwortliche beteiligt die Datenschutzbeauftragte oder den Datenschutzbeauftragten an der Durchführung einer Datenschutzfolgenabschätzung.

(4) **[Art. 27 Abs. 2 DS-RL; Art. 35 Abs. 7 DS-GVO]** Die Folgenabschätzung gemäß Absatz 1 trägt den Rechten der von der Verarbeitung betroffenen Personen und sonstiger betroffener Personen Rechnung und enthält zumindest Folgendes:

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 Gefährdung für die Rechtsgüter der betroffenen Person und

4. die zur Bewältigung der Gefahr geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die gesetzlichen Vorgaben eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger betroffener Personen Rechnung getragen wird.

(5) **[Art. 35 Abs. 11 DS-GVO]** Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung den Maßgaben folgt, die sich aus der Folgenabschätzung ergeben haben; dies gilt zumindest, wenn hinsichtlich der mit den Verarbeitungsvorgängen verbundenen Gefährdung Änderungen eingetreten sind.

§ 62
Anhörung der oder des Bundesbeauftragten

[Art. 28 DS-RL] (1) Der Verantwortliche oder der Auftragsverarbeiter hört vor der Inbetriebnahme neuartiger maßgeblicher Systeme und Verfahren zur Verarbeitung personenbezogener Daten die Bundesbeauftragte oder den Bundesbeauftragten an, wenn

1. aus einer Datenschutz-Folgenabschätzung gemäß § 61 hervorgeht, dass die Verarbeitung eine hohe Gefährdung zur Folge hätte, wenn der Verantwortliche keine Maßnahmen zur Eindämmung der Gefährdung trifft, oder

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

(2) **[Art. 28 Abs. 4 DS-RL; Art. 36 Abs. 3 DS-GVO]** Der oder dem Bundesbeauftragten sind

1. die gemäß § 61 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 die Mitteln der beabsichtigten Verarbeitung,

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

5. die Kontaktdaten der oder des Datenschutzbeauftragten

vorzulegen und auf Anfrage alle sonstigen Informationen zu übermitteln, die sie oder er benötigt, um die Ordnungsgemäßheit der Verarbeitung sowie insbesondere die in Be-

zug auf den Schutz der personenbezogenen Daten der betroffenen Person 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 nicht ausreichend eingedämmt hat, kann diese oder dieser dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu sechs Wochen nach Einleitung der Anhörung entsprechende schriftliche Empfehlungen unterbreiten. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um einen weiteren Monat verlängert werden. Die oder der Bundesbeauftragte unterrichtet den Verantwortlichen oder gegebenenfalls den Auftragsverarbeiter über eine solche Fristverlängerung innerhalb eines Monats nach Einleitung der Anhörung die Verzögerung.

(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 gebührend zu berücksichtigen und die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.

§ 63
Verzeichnis von Verarbeitungstätigkeiten

[Art. 24 DS-RL] (1) Der Verantwortliche führt ein Verzeichnis aller Kategorien von Verarbeitungen, die seiner Zuständigkeit unterliegen. Dieses Verzeichnis enthält die folgenden Angaben:

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

2. die Zwecke der Verarbeitung,

3. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfängern in Drittländern oder internationalen Organisationen,

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 § 58.

(2) Auftragsverarbeiter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Verarbeitungen, das Folgendes enthält:

1. Name und Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie des Datenschutzbeauftragten,

2. die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden,

3. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, wenn von dem Verantwortlichen entsprechend angewiesen, einschließlich der Identifizierung des Drittlandes oder der internationalen Organisation und

4. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 58.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche und der Auftragsverarbeiter stellen der oder dem Bundesbeauftragten das Verzeichnis auf Anfrage zur Verfügung.

§ 64

Gemeinsam Verantwortliche

[Art. 21 DS-RL] Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung fest, insbesondere, wenn Daten der betroffenen Person automatisiert in einer Weise gespeichert sind, dass mehrere Stellen speicherungsberechtigt sind, gelten sie als gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten fest, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten nachkommt, soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch das Unionsrecht oder sonstige Rechtsvorschriften festgelegt sind. In der Vereinbarung wird angegeben, an welche Stelle sich betroffene Personen zur Wahrnehmung ihrer Rechte wenden können.

§ 65

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

[Art. 20 DS-RL] (1) Der Verantwortliche trifft 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 Gefährdung für die Rechtsgüter der betroffenen Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung angemessene Vorkehrungen — wie z. B. Pseudonymisierung —, die dafür ausgelegt sind, Datenschutzgrundsätze wie etwa Datensparsamkeit wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den gesetzlichen Anforderungen zu genügen und die Rechte der betroffenen Personen zu schützen. **[§ 3a BDSG-alt]** Insbesondere ist 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 zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

§ 66

Allgemeine Informationen zu Datenverarbeitungen

[Art. 13 Abs. 1 DS-RL] Der Verantwortliche stellt in allgemeiner Form und für jedermann zugänglich die folgenden Informationen zur Verfügung:

1. die Zwecke der Verarbeitung,

2. das Bestehen der Rechte der betroffenen Person auf Auskunft, Berichtigung und Löschung personenbezogener Daten sowie auf Einschränkung der Verarbeitung,

3. Informationen über das Bestehen des Rechts, die oder den Bundesbeauftragten anzurufen sowie deren oder dessen Erreichbarkeit und

4. die Erreichbarkeit des Verantwortlichen und der oder des Datenschutzbeauftragten zur Erlangung weitergehender Informationen.

§ 67
Benachrichtigung betroffener Personen

[Art. 13 Abs. 2 DS-RL] (1) Ist die Benachrichtigung betroffener Personen über Datenverarbeitungen in speziellen Rechtsvorschriften vorgesehen oder angeordnet, enthält diese Benachrichtigung zumindest die folgenden Angaben:

1. die in § 66 Absatz 1 Satz 1 Nummern 1 bis 4 genannten Angaben,

2. die Rechtsgrundlage der Verarbeitung,

3. die Dauer, für die die personenbezogenen Daten gespeichert werden bzw. die Aussonderungsprüffrist oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Fristen und

4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten, auch der Empfänger in Drittstaaten oder in internationalen Organisationen.

(2) In Fällen des Absatzes 1 kann der Verantwortliche die Benachrichtigung aufschieben, einschränken oder unterlassen, soweit andernfalls

1. behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren gefährdet werden,

2. die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung gefährdet werden,

3. die öffentliche Sicherheit oder Ordnung gefährdet wird oder

4. die Rechtsgüter Dritter gefährdet werden.

[§ 19 Abs. 3 BDSG-alt] 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.

§ 68
Unterscheidung verschiedener Kategorien betroffener Personen; Unterscheidung zwischen Tatsachen und Bewertungen

(1) **[Art. 6 DS-RL]** Der Verantwortliche unterscheidet bei der Verarbeitung so weit wie möglich zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen darunter:

1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden,

2. verurteilte Straftäter,

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

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

4. anderen Personen im Zusammenhang mit einer Straftat, wie Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeugen in Betracht kommen, Personen, die Hinweise zur Straftat geben können oder Personen, die mit den unter den Nummern 1 und 2 genannten Personen in Kontakt oder in Verbindung stehen.

(2) **[Art. 7 Abs. 1 DS-RL]** Der Verantwortliche unterscheidet bei der Verarbeitung so weit wie möglich zwischen auf Tatsachen und auf persönlichen Einschätzungen beruhenden Daten. Hierzu werden Bewertungen oder sonstige auf persönlichen Einschätzungen beruhende Beurteilungen als solche kenntlich gemacht. Es muss außerdem feststellbar sein, bei welcher Stelle die Unterlagen geführt werden, die der Bewertung oder der sonstigen auf persönlicher Einschätzung beruhenden Beurteilung zugrunde liegen.

§ 69

Qualitätssicherung personenbezogener Daten vor deren Übermittlung

[Art. 7 Abs. 2 DS-RL] Der Verantwortliche ergreift angemessene Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht übermittelt oder sonst bereitgestellt werden. Zu diesem Zweck überprüft der Verantwortliche, soweit durchführbar, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung. Bei jeder Übermittlung personenbezogener Daten werden nach Möglichkeit Informationen beigefügt, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der personenbezogenen Daten sowie deren Aktualitätsgrad zu beurteilen.

§ 70

Berichtigung und Löschung personenbezogener Daten sowie die Einschränkung der Verarbeitung

[Art. 16 DS-RL] (1) Der Verantwortliche hat personenbezogene Daten zu berichtigen, wenn sie unrichtig sind **[Art. 16 Abs. 5 DS-RL]** und teilt der Stelle, die die personenbezogenen Daten zuvor an ihn übermittelt hat, die Berichtigung mit.

(2) **[Art. 16 Abs. 2 DS-RL]** 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. An die Stelle einer Löschung tritt die Einschränkung der Verarbeitung, wenn

1. Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigt würden,

2. die personenbezogenen Daten für Zwecke eines gerichtlichen Verfahrens 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 eingeschränkte Daten dürfen nur für den Zweck verarbeitet werden, für den die Löschung unterblieben ist; sie dürfen auch verarbeitet werden, wenn dies zur Behebung einer bestehenden Beweisnot unerlässlich ist oder die betroffene Person einwilligt.

(3) **[Art. 5 DS-RL]** Unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschfristen prüft der Verantwortliche regelmäßig nach festgesetzten Fristen, ob die Speicherung personenbezogener Daten für die Aufgabenerfüllung noch erforderlich ist oder die Daten zu löschen sind (Aussonderungsprüffrist).

(4) **[Art. 16 Abs. 6 DS-RL; Art. 7 Abs. 3 DS-RL]** Stellt der Verantwortliche fest, dass unrichtige, zu löschende oder in ihrer Verarbeitung einzuschränkende Daten über-

mittelt worden sind, ist dem Empfänger die Berichtigung, Löschung oder Verarbeitungseinschränkung mitzuteilen.

§ 71
Protokollierung

[Art. 25 DS-RL] (1) In automatisierten Verarbeitungssystemen protokollieren Verantwortliche und Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge: Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung. Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identifizierung der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers solcher personenbezogenen Daten festzustellen.

(2) Die Protokolle stehen für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten sowie die Bundesbeauftragte oder den Bundesbeauftragten zur Verfügung. Darüber hinaus werden die Protokolle für die Eigenüberwachung, für die Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten sowie für die Verhütung oder Verfolgung von Straftaten verwendet.

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

§ 72
Vertrauliche Meldung von Verstößen

[Art. 48 DS-RL] Der Verantwortliche trägt dafür Sorge, dass ihm vertrauliche Meldungen über Verstöße gegen anwendbare Datenschutzvorschriften im Zusammenhang mit unter seiner Verantwortung durchgeführte Verarbeitungen zur Kenntnis gebracht werden können.

Kapitel 4
Datenübermittlung an Verantwortliche in Drittstaaten und an internationale Organisationen

§ 73
Allgemeine Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten und internationalen Organisationen

[Art. 35 DS-RL] (1) **[Art. 35 Abs. 1 Buchst. a, b, d DS-RL]** Die Übermittlung personenbezogener Daten an Stellen in Drittstaaten oder an internationale Organisationen ist unbeschadet speziellerer Regelungen in Fachgesetzen zulässig, wenn

1. dies für die in § 43 genannten Zwecke erforderlich ist,

2. die personenbezogenen Daten an einen Verantwortlichen in einem Drittstaat oder eine internationale Organisation, die eine für Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit zuständige Behörde ist, übermittelt werden und

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

(2) **[Art. 35 Abs. 1 Buchst. c, Abs. 2 DS-RL]** In Fällen, in denen personenbezogene Daten aus einem anderen Mitgliedstaat der Europäischen Union übermittelt oder zur Verfügung gestellt werden, muss die zuständige Stelle in diesem Mitgliedstaat die

Übermittlung zuvor genehmigen. Übermittlungen ohne vorherige Genehmigung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittstaats oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Die Behörde, die für die Erteilung der vorherigen Genehmigung zuständig ist, wird unverzüglich über die Übermittlung unterrichtet.

(3) **[Art. 35 Abs.1 Buchst. e DS-RL]** Der Verantwortliche, der die Übermittlung durchführt, stellt mittels geeigneter Maßnahmen sicher, dass der Empfänger die übermittelten Daten an Stellen in anderen Drittstaaten oder an eine internationale Organisation nur mit seiner vorab erteilten Genehmigung weiterübermittelt. Bei der Entscheidung über die Erteilung der Genehmigung berücksichtigt der Verantwortliche gebührend sämtliche maßgebliche Faktoren, einschließlich der Schwere der Straftat, des Zwecks der ursprünglichen Übermittlung und des Schutzniveaus für personenbezogene Daten in dem Drittland oder der internationalen Organisation, an das bzw. die die zuvor übermittelten Daten weiterübermittelt werden sollen. Die Zuständigkeit für die Erteilung der Genehmigung kann auch abweichend geregelt werden.

(4) **[Art. 9 Abs. 3 DS-RL]** § 44 Absatz 3 gilt entsprechend.

§ 74

Datenübermittlung ohne Angemessenheitsbeschluss und mit geeigneten Garantien

[Art. 37 DS-RL] (1) Liegt entgegen § 73 Absatz 1 Nummer 3 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor, ist eine Übermittlung an Stellen gemäß § 73 Absatz 1 Nummer 2 in einem Drittstaat oder an eine internationale Organisation 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 zum Schutz personenbezogener Daten bestehen.

(2) Der Verantwortliche unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten jährlich über Übermittlungen, die aufgrund der Beurteilung durch den Verantwortlichen gemäß Absatz 1 Nummer 2 erfolgt sind. In der Unterrichtung können die Empfänger und die Übermittlungszwecke angemessen kategorisiert werden.

(3) Übermittlungen gemäß Absatz 1 Nummer 2 werden dokumentiert. Der Verantwortliche stellt die Dokumentation einschließlich Datum und Zeitpunkt der Übermittlung, Informationen über den Empfänger, Begründung der Übermittlung und übermittelte personenbezogenen Daten, der oder dem Bundesbeauftragten auf Anforderung zur Verfügung.

§ 75

Datenübermittlung ohne Angemessenheitsbeschluss und ohne geeignete Garantien

[Art. 38 DS-RL] (1) Liegt entgegen § 73 Absatz 1 Nummer 3 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor und liegen auch keine geeigneten Garantien gemäß § 74 Absatz 1 Nummern 1 oder 2 vor, ist eine Übermittlung an Stellen gemäß § 73 Absatz 1 Nummer 2 in einem Drittland oder an eine internationale Organisation zulässig, wenn diese im Einzelfall für Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit erforderlich ist

1. zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person,

2. zur Wahrung berechtigter Interessen der betroffenen Person,

3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Mitgliedstaats der Europäischen Union oder eines Drittstaats oder

4. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 43 genannten Zwecken.

(2) Eine Übermittlung unterbleibt, wenn der übermittelnde Verantwortliche feststellt, dass die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

(3) Übermittlungen gemäß Absatz 1 werden dokumentiert. Der Verantwortliche stellt die Dokumentation einschließlich Datum und Zeitpunkt der Übermittlung, Informationen über den Empfänger, Begründung der Übermittlung und übermittelte personenbezogene Daten, der oder dem Bundesbeauftragten auf Anforderung zur Verfügung.

§ 76

Übermittlung an nicht für die Verarbeitung zu Zwecken nach § 43 zuständige und nicht-öffentliche Stellen in Drittstaaten

[Art. 39 DS-RL] (1) Verantwortliche können abweichend von § 73 Absatz 1 Nummer 2 und unbeschadet von Abkommen im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit im besonderen Einzelfall personenbezogene Daten direkt an andere als in § 73 Absatz 1 Nummer 2 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Aufgabenerfüllung unbedingt erforderlich ist und

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

2. die Übermittlung an einen von § 73 Absatz 1 Nummer 2 umfassten Empfänger wirkungslos oder ungeeignet ist, insbesondere weil die Übermittlung nicht rechtzeitig durchgeführt werden kann und

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

Der Verantwortliche unterrichtet die von § 73 Absatz 1 Nummer 2 umfasste Stelle, an die abweichend von § 73 Absatz 1 Nummer 2 nicht übermittelt wurde, unverzüglich über die Übermittlung, es sei denn, dies ist wirkungslos oder ungeeignet.

(2) Der Verantwortliche dokumentiert Übermittlungen gemäß Absatz 1 und unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten über diese Übermittlungen.

Kapitel 5
Zusammenarbeit der Aufsichtsbehörden

§ 77

Gegenseitige Amtshilfe

[Art. 50 DS-RL] (1) Die oder der Bundesbeauftragte übermittelt Datenschutzaufsichtsbehörden in anderen Mitgliedstaaten der Europäischen Union maßgebliche Informationen und gewährt ihnen Amtshilfe, um die Richtlinie (EU) 2016/680 umsetzende Rechtsvorschriften einheitlich durchzuführen und anzuwenden. Sie oder er trifft Vorkehrungen für eine wirksame Zusammenarbeit. Die Amtshilfe bezieht sich insbesondere auf Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

(2) Die oder der Bundesbeauftragte ergreift alle geeigneten Maßnahmen, um dem Ersuchen einer anderen Aufsichtsbehörde unverzüglich und spätestens innerhalb eines Monats nach Eingang des Ersuchens nachzukommen. Dazu kann insbesondere auch die Übermittlung maßgeblicher Informationen über die Durchführung einer Untersuchung gehören.

(3) Amtshilfeersuchen enthalten alle erforderlichen Informationen, einschließlich Zweck und Begründung des Ersuchens. Die übermittelten Informationen werden ausschließlich für den Zweck verwendet, für den sie angefordert wurden.

(4) Die oder der Bundesbeauftragte lehnt das Ersuchen nur ab, 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 Unionsrecht oder sonstige Rechtsvorschriften verstoßen würde.

(5) Die oder der Bundesbeauftragte informiert die ersuchende Aufsichtsbehörde über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen, die getroffen wurden, um dem Ersuchen nachzukommen. Sie oder er erläutert gegebenenfalls die Gründe für die Ablehnung des Ersuchens gemäß Absatz 4.

(6) Die oder der Bundesbeauftragte übermittelt die Informationen, um die sie oder er von einer anderen Aufsichtsbehörde ersucht wurde, in der Regel auf elektronischem Wege unter Verwendung eines standardisierten Formats.

(7) Die oder der Bundesbeauftragte verlangt für Maßnahmen, die sie oder er aufgrund eines Amtshilfeersuchens getroffen haben, keine Gebühren. Die Aufsichtsbehörden können untereinander Regeln vereinbaren, um einander in Ausnahmefällen besondere aufgrund der Amtshilfe entstandene Ausgaben zu erstatten.

Kapitel 6
Haftung und Sanktionen

§ 78
Schadensersatz

[Art. 56 DS-RL; §§ 7, 8 BDSG-alt] (1) Fügt ein Verantwortlicher einer betroffenen Person durch eine nach diesem Gesetz oder anderen auf die beim Verantwortlichen durchgeführten Verarbeitungen anwendbaren Vorschriften rechtswidrige Verarbeitung personenbezogener Daten einen Schaden zu, ist er der betroffenen Person zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt bei nicht-automatisierten Verarbeitungen, soweit der Schaden nicht durch ein Verschulden des Verantwortlichen verursacht 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 speicherungsberechtigten Stellen den Schaden verursacht hat, so haftet jede dieser Stellen.

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

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

§ 79
Bußgeld- und Strafvorschriften

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

[Art. 57 DS-RL; §§ 43, 44 BDSG-alt] (1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. **[§ 43 Abs. 1 Nr. 2 BDSG-alt]** entgegen § 5 eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten nicht oder nicht in der vorgeschriebenen Weise benennt.

2. **[§ 43 Abs. 1 Nr. 2b BDSG-alt]** entgegen § 57 Absätze 5 und 6 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 57 Absatz 8 sich nicht vor Beginn der Verarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt.

3. **[§ 43 Abs. 2 Nr. 1 BDSG-alt]** unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, verarbeitet,

4. **[§ 43 Abs. 2 Nr. 2 BDSG-alt]** unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

5. **[§ 43 Abs. 2 Nr. 3 BDSG-alt]** unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

6. **[§ 43 Abs. 2 Nr. 4 BDSG-alt]** die Übermittlung personenbezogener Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht oder

7. **[§ 43 Abs. 2 Nr. 5 BDSG-alt]** als nicht-öffentliche Stelle von öffentlichen Stellen übermittelte Daten für andere Zwecke nutzt als für die, für die sie übermittelt wurden.

(2) **[§ 43 Abs. 3 BDSG-alt]** Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummern 1 und 2 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 1 Nummern 3 bis 7 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

(3) Die sachliche Zuständigkeit für die Ahndung und Verfolgung der in Absatz 1 Nummern 1 bis 6 genannten Ordnungswidrigkeiten liegt bei der Behörde, bei welcher der ordnungswidrig Handelnde beschäftigt ist.

(4) **[§ 44 Abs. 1 und 2 BDSG-alt]** Wer eine in Absatz 1 Nummern 3 bis 7 dieses Gesetzes bezeichnete Handlung vorsätzlich gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

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 § 58“ 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 zu beschränken, 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 Sätze 5 und 6 werden wie folgt gefasst:

      „In diesem Fall ist die Verarbeitung der in der Akte gespeicherten personenbezogenen Daten zu beschränken 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 werden die Wörter „Sperrung“ durch das Wort „Verarbeitungsbeschränkung“ ersetzt.

   b) In Absatz 6 Satz 1 Nummer 9 wird die Angabe „nach § 8“ durch die Angabe „entsprechend § 78“ ersetzt.

8. § 22b Absatz 7 Sätze 1 und 2 werden wie folgt gefasst:

   „Das Bundesamt für Verfassungsschutz trifft für die Dateien die technischen und organisatorischen Maßnahmen entsprechend § 58 des Bundesdatenschutzgesetzes. § 6 Ab-

satz 3 Satz 2 bis 5 und § 26a gelten nur für die vom Bundesamt für Verfassungsschutz eingegebenen Daten sowie dessen Abrufe.“

9. In § 25 Satz 3 wird der letzte Halbsatz wie folgt gefasst:

„in diesem Fall ist die Verarbeitung der Daten zu beschränken.“

10. Im Dritten Abschnitt wird folgender § 26a eingefügt:

„§ 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 Kommission nach § 15 des Artikel 10-Gesetzes unterliegt, unterliegt sie nicht der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten, es sei denn, die Kommission ersucht die Bundesbeauftragte oder den Bundesbeauftragten, 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 und ihre oder seine schriftlich besonders Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen 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 Absätze 1 und 4 des Bundesdatenschutzgesetzes finden keine Anwendung.“

11. § 27 wird wie folgt gefasst:

„§ 27
Anwendung des Bundesdatenschutzgesetzes

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

1. von Teil 1 finden §§ 4, 16 Absätze 1 und 4 und §§ 17 bis 21 keine Anwendung,

2. von Teil 2 und 3 sind § 47 Absätze 1 bis 4 und §§ 48 bis 50, 57, 58, 78, 79 entsprechend anzuwenden.

(2) Bei der Erfüllung allgemeiner Verwaltungsaufgaben durch das Bundesamt für Verfassungsschutz findet die Verordnung (EU) 2016/679 Anwendung. § 26a Absatz 4 Satz 3 bleibt unberührt.“

Artikel 3

Änderung des MAD-Gesetzes

BMVg wird gebeten, ev. Änderungsbedarf zu prüfen und zu ergänzen.

[…]

Artikel 4

Änderung des BND-Gesetzes

BK-Amt wird gebeten, ev. Änderungsbedarf zu prüfen und zu ergänzen.

[…]

Artikel 5

Änderung des Sicherheitsüberprüfungsgesetzes

[…]

Artikel 6

Änderung des Artikel-10-Gesetzes

1. § 4 wird wie folgt geändert:
   a) Absatz 1 Satz 7, 1. Halbsatz wird wie folgt gefasst:
   „In diesem Fall ist die Verarbeitung der Daten zu beschränken“
   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) Dem Absatz wird folgender Satz angefügt:
      „Bei der Übermittlung an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen ist § 19 Absatz 3 Sätze 2 und 4 des Bundesverfassungsschutzgesetzes anzuwenden.“
2. § 6 Absatz 1 Satz 7, 1. Halbsatz wird wie folgt gefasst:
   „In diesem Fall ist die Verarbeitung der Daten zu beschränken“
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 zu § 42b eingefügt:

„§ 42b Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Europarechtswidrigkeit eines Angemessenheitsbeschlusses der Kommission“.

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

„§ 42b
Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Europarechtswidrigkeit eines Angemessenheitsbeschlusses der Kommission

(1) Hält eine Aufsichtsbehörde einen Angemessenheitsbeschluss der Kommission, auf dessen Gültigkeit es bei der Entscheidung über die Beschwerde einer betroffenen Person ankommt, für europarechtswidrig, 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 Kommission Gelegenheit zur Äußerung binnen einer zu bestimmenden Frist geben.

(5) Ist ein Verfahren zur Überprüfung der Gültigkeit des Angemessenheitsbeschlusses der Kommission 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 Angemessenheitsbeschluss der Kommission gültig ist, so stellt es dies in seiner Entscheidung fest. Andernfalls legt es die Frage nach der Gültigkeit des Angemessenheitsbeschlusses der Kommission gemäß Artikel 267 des Vertrags über die Arbeitsweise der Europäischen Union dem Gerichtshof der Europäischen Union zur Entscheidung vor.“

Artikel 8

Änderung des Bundesstatistikgesetzes

Nach § 17 des Bundesstatistikgesetzes in der Fassung der Bekanntmachung vom 20. Oktober 2016 (BGBl. I S. 2394), das zuletzt durch Artikel 1 des Gesetzes vom 21. Juli 2016 (BGBI. I S. 1768) geändert worden ist, wird folgender § 17a eingefügt:

„§ 17a
Rechte auf Auskunft und Berichtigung

Das Recht auf Auskunft gemäß Artikel 15 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. EU Nr. L 119 vom 4. Mai 2016, S. 1 ff.) und das Recht auf Berichtigung gemäß Artikel 16 der Verordnung (EU) 2016/679 bestehen bis zur Löschung der Hilfsmerkmale im Sinne des § 12, es sei denn, das Interesse der betroffenen Person an der Auskunft oder Berichtigung muss zurücktreten, weil die Verwirklichung des jeweiligen Rechts die ordnungsgemäße

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben gefährden würde.“

Artikel 9

Weitere Folgeänderungen

[…]

Artikel 10

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: Datum der Verkündung 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. EU Nr. L 119 vom 4. Mai 2016, S. 1 ff.) 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). Ihrem Charakter als Grundverordnung folgend enthält die Verordnung Öffnungsklauseln für den nationalen Gesetzgeber. 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 Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU Nr. L 119 vom 4. Mai 2016, S. 89 ff.), 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-alt) durch ein neues Bundesdatenschutzgesetz (BSDG-neu) abzulösen. Weiterer gesetzlicher Anpassungsbedarf ergibt sich hinsichtlich der bestehenden bereichsspezifischen Datenschutzregelungen des

Bundes in Folge der Änderungen im allgemeinen Datenschutzrecht durch die Verordnung (EU) 2016/679 und das sie ergänzende neugefasste BDSG-alt.

Im Interesse einer homogenen Entwicklung des allgemeinen Datenschutzrechts findet das BDSG-neu, 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.

Vor dem Hintergrund des Vorstehenden ergibt sich folgende Dreiteilung des neugefassten BSDG:

- 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.

II. Wesentlicher Inhalt des Entwurfs

Der Gesetzentwurf sieht folgende Gesetzesänderungen vor:

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

   a. Gemeinsame Bestimmungen mit folgenden Regelungsschwerpunkten:

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

   Die gemeinsamen Bestimmungen lassen unmittelbar geltendes Recht der Europäischen Union unberührt, insbesondere die Datenschutz-Grundverordnung (Verordnung (EU) Nr. 2016/679[3]). Sie finden außerdem Anwendung im Anwendungsbereich

[3] 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 Datenver-

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-neu);
- Festlegung der Zulässigkeitsvoraussetzungen für Verarbeitungen zu anderen Zwecken (§ 23 BDSG-neu);
- Erhalt der Vorschriften zu Auskunfteien und Scoring sowie Regelung weiterer besonderer Verarbeitungssituationen (§§ 24 bis 29 BDSG-neu);
- Regelungen zu den Betroffenenrechten (§§ 30 bis 35 BDSG-neu); sie berücksichtigen Artikel 23 der Verordnung (EU) 2016/679, orientieren sich sehr weitgehend an den bestehenden Regelungen des Bundesdatenschutzgesetzes (BDSG-alt) und sorgen für einen angemessenen Interessenausgleich;
- Verhängung von Geldbußen bei Verstößen gegen die Verordnung (EU) 2016/679 (§§ 39, 40 BDSG-neu).

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

- Aussagen zu Rechtsgrundlagen der Verarbeitung, Zweckbindung und -änderung (§§ 44 bis 46 BDSG-neu)
- Regelungen zu den Betroffenenrechten (§§ 51 bis 53 BDSG-neu)
- Festlegung unterschiedlich akzentuierter Verantwortlichenpflichten
  - Anforderungen an Auftragsverarbeitungsverhältnisse (§ 57 BDSG-neu)
  - Datensicherheit und Umgang mit Datensicherheitsvorfällen (§§ 58 bis 60 BDSG-neu)
  - Instrumente zur Berücksichtigung des Datenschutzes (Datenschutzfolgenabschätzung, Anhörung der oder des Bundesbeauftragten, Verzeichnis von Verarbeitungstätigkeiten, Protokollierung §§ 61 bis 63 und 71 BDSG-neu)
  - Berichtigungs- und Löschungspflichten (§ 70 BDSG-neu)
- Datenübermittlungen an Stellen in Drittstaaten und an internationale Organisationen (§§ 73 bis 76 BDSG-neu).

2. Die mit dem Gesetzentwurf vorgenommenen Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes und des Sicherheitsüberprüfungsgesetzes (Artikel 2 bis 6) erfolgen vor dem Hintergrund der Neufassung des BDSG. Die Änderungen sind erforderlich, um den speziellen Erfordernissen der außerhalb des Anwendungsbereichs des Unionsrechts fallenden Datenverarbeitungen im Bereich der nationalen Sicherheit Rechnung zu tragen.

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

III. Alternativen

Keine.

---

kehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 vom 4. Mai 2016, S. 1 ff.)

IV. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt für Regelungen des Datenschutzes als Annex aus den jeweiligen Sachkompetenzen der Artikel 73 bis 74 Grundgesetz (GG). Im Bereich der öffentlichen Verwaltung bedarf es bundesrechtlicher Datenschutzbestimmungen, soweit dem Bund die Verwaltungskompetenz zusteht. Für nicht-öffentliche 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 Kapitel 6 (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 Europäischen 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.

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

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 Mitgliedstaates 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 die innerstaatliche Willensbildung durch die von der Angelegenheit betroffenen Aufsichtsbehörden im Rahmen des durch Kapitel 5 geregelten nationalen Begleitverfahrens sowie die Beteiligung eines Ländervertreters im Ausschuss. Durch diese Vorkehrungen wird die innerstaatliche Wahrnehmungskompetenz der Länder in den Ausschuss hinein verlängert.

Die Gesetzgebungskompetenz des Bundes für die Vorschriften über Rechtsbehelfe gegen Angemessenheitsbeschlüsse der Kommission (Artikel 1 § 19) und zum gerichtlichen Rechtsschutz (Artikel 1 § 23) 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).

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

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und völkerrechlichen 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 Unions (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 Rechtsgrund-

lagen 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 Art. 4 der Verordnung (EU) 2016/679 bzw. Art. 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, verfassungsmäßigen 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 Arti-

kel 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 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 Erfüllungsaufwand, der aber durch die Verordnung (EU) 2016/679 und nicht durch dieses Gesetz verursacht wird.

Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein neuer Erfüllungsaufwand durch dieses Gesetz.

Wirtschaft

Der vorliegende Gesetzentwurf enthält keine Regelungen, die zusätzlichen Erfüllungsaufwand bei der Wirtschaft auslösen. Soweit der Gesetzentwurf Betroffenenrechte einschränkt, führen sie bei den Unternehmen zu einer Reduzierung von Pflichten, die ohne den Gesetzentwurf unmittelbar durch die Verordnung (EU) 2016/679 ausgelöst worden wären.

[siehe Hinweis für NKR im Anschreiben des BMI]

Verwaltung

Im Einzelplan 21 der Bundesbeauftragten für Datenschutz und Informationsfreiheit entstehen Mehrausgaben durch:

- die Wahrnehmung der Funktion des gemeinsamen Vertreters im Europäischen Datenschutzausschuss nach Artikel 68 der Verordnung (EU) 2016/679 (§ 17 BDSG-neu),
- die bei der Bundesbeauftragten für Datenschutz und Informationsfreiheit angesiedelte Einrichtung der zentralen Anlaufstelle aufgrund des Erwägungsgrundes 119 der Verordnung (EU) 2016/679 (§ 17 BDSG-neu).

Im Regierungsentwurf zum Bundeshaushalt 2017 sind für den Bereich der Umsetzung der Datenschutzgrundverordnung und der JI-Richtlinie 32 neue Planstellen mit entsprechenden Haushaltsmitteln etatisiert. Der Gesetzentwurf zur Übernahme der Funktionen des gemeinsamen Vertreters und der zentralen Anlaufstelle lag bei Verabschiedung des Regierungsentwurfs noch nicht vor und konnte in seinen Auswirkungen deswegen noch nicht berücksichtigt werden. Sollte die zentrale Anlaufstelle im Ausland (d. h. in Brüssel) verortet werden, ist mit weiterem Mehrbedarf zu rechnen.

[Erfüllungsaufwand zu Teil 3 ist noch zu ermitteln]

Für die Länder entstehen Mehrausgaben durch die Wahl und Bestellung des Stellvertreters des gemeinsamen Vertreters im Europäischen Datenschutzausschuss (§ 17 BDSG-neu). Die Höhe dieser Mehrausgaben kann derzeit nicht quantifiziert werden.

[*im Rahmen der Länderbeteiligung wird eine Schätzung der Mehrausgaben abgefragt werden*].

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

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 oder Evaluierung des Gesetzes ist nicht vorgesehen.

B. Besonderer Teil

Zu Artikel 1 (Bundesdatenschutzgesetz)

Zu § 1 (Anwendungsbereich)

Die Vorschrift bestimmt den Anwendungsbereich des Gesetzes.

Nach Absatz 1 gilt das Gesetz, wie bisher auch das Bundesdatenschutzgesetz in der bisher geltenden Fassung (BDSG-alt), für alle öffentlichen Stellen des Bundes sowie für öffentliche Stellen der Länder und nicht-öffentlichen Stellen. Die Begriffsbestimmungen zu öffentlichen Stellen des Bundes, der Länder und nicht-öffentlichen Stellen finden sich in § 2 Absatz 1 Nummern 1 bis 3 BDSG-neu.

Soweit die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten öffentlicher Stellen des Bundes erfolgt, die weder vom Anwendungsbereich der Verordnung (EU) 679/2016 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 neugefasste Bundesdatenschutzgesetz (BDSG-neu) 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 § 2 Absatz 2 den Vorschriften des BDSG-neu vor.

Absatz 2 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-neu 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-neu

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

weitergehende oder engere gesetzliche Regelung getroffen ist. Liegt allerdings keine bereichsspezifische Datenschutzregelung für einen vergleichbaren Sachverhalt vor, so übernimmt das BDSG-neu seine lückenfüllende Auffangfunktion. Auch eine nicht abschließende (teilweise) Regelung oder das Schweigen eines bereichsspezifischen Gesetzes führt dazu, dass subsidiär auf die Vorschriften des BDSG-neu zurückgegriffen werden kann. Bedeutsam ist dies insbesondere mit Blick auf die in Kapitel 3 des BDSG-neu vorgenommenen Einschränkungen der Betroffenenrechte. Auf diese Regelungen kann als Auffangregelung zurückgegriffen werden, sofern im bereichsspezifischen Recht keine tatbestandskongruente Regelung vorgehalten ist.

Absatz 3 entspricht der bisherigen Regelung des § 1 Absatz 4 BDSG-alt.

Absatz 4 bestimmt, dass die Vorschriften des BDSG-neu 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 5 berücksichtigt, dass der Verordnung (EU) 2016/679 im Rahmen ihres Anwendungsbereichs unmittelbare Geltung im Sinne des Art. 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 sind 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.

Zu § 2 (Begriffsbestimmungen)

Die Nummern 1 bis 3 in Absatz 1 entsprechen § 2 BDSG-alt. Sie bestimmen, welche öffentlichen Stellen und nicht-öffentlichen Stellen unter den Anwendungsbereich nach § 1 Absatz 1 BDSG-neu fallen.

Die Begriffsbestimmungen in den Nummern 1 bis 15 des Absatzes 2 sind zum Zwecke der Umsetzung der Richtlinie (EU) 2016/680 aufgenommen worden. Dies indes nur insoweit, als sie sich gleichlautend sowohl in Artikel 4 der Verordnung (EU) 2016/679 und Artikel 3 der Richtlinie (EU) 2016/680 finden. Als gemeinsame Schnittmenge der Verordnung und der Richtlinie handelt es sich um „Gemeinsame Bestimmungen“ im Sinne des Teils 1 dieses Gesetzes.

Zu § 3 (Verarbeitung personenbezogener Daten)

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 bereichsspezifi-

scher Regelungen auf die Regelung unabhängig davon zurückgreifen, ob die Datenverarbeitung zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679, zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 oder zu nicht von diesen beiden EU-Rechtsakten erfassten Zwecken im Rahmen (z. B. Datenverarbeitung durch Nachrichtendienste) erfolgt.

Wer zu dem Kreis der öffentlichen Stellen gehört, wird in § 2 Absatz 1 Nummer 1 bis 3 BDSG-neu bestimmt. Soweit nicht-öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen (sog. Beliehene), gelten sie nach § 2 Absatz 1 Nummer 3 Satz 2 BDSG-neu als öffentliche Stellen und können ihre Datenverarbeitung daher ebenfalls auf die Befugnis in § 3 BDSG-neu 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. Durch den Zusatz „unbeschadet anderer Rechtsvorschriften“ wird klargestellt, dass die Verarbeitung personenbezogener Daten 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.

Die Regelung nimmt den bisher in §§ 13 Absatz 1 und 14 Absatz 1 BDSG-alt enthaltenen Regelungsgehalt auf, unterscheidet im 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. Diese umfasst nach der Definition in § 2 Absatz 2 Nummer 2 BDSG-neu alle Verarbeitungsphasen.

Zu § 4 (Videoüberwachung)

Die Vorschrift enthält Regelungen zur Videoüberwachung in öffentlich zugänglichen Räumen. Von Absatz 1 umfasst wird sowohl die Erhebung von personenbezogenen Daten aus optisch-elektronischen Einrichtungen wie auch alle weiteren Verarbeitungen.

Absatz 1 Nummer 1 regelt die Videoüberwachung in öffentlich zugänglichen Räumen durch öffentliche Stellen. Sie ist gestützt auf Artikel 6 Absatz 1 Satz 1 Buchstabe e („Wahrnehmung einer Aufgabe …, die im öffentlichen Interesse liegt“) i. V. m. Artikel 6 Absatz 3 Satz 1 der Verordnung (EU) 2016/679.

Absatz 1 Nummer 2 begründet eine spezifische Befugnis zur Videoüberwachung durch nichtöffentliche Stellen, die als Betreiber großflächiger, öffentlich zugänglicher Anlagen, wie Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder Einrichtungen und Fahrzeugen des öffentlichen Personenverkehrs, einen über die zivilrechtliche Verpflichtung (z. B. Verkehrssicherungspflicht) hinausgehende Beitrag leisten, der auch im öffentlichen Interesse liegt. Soweit Videoüberwachung in anderen Gesetzen spezieller geregelt ist (z. B. § 27 Bundespolizeigesetz), bleiben diese Regelungen unberührt. Die Regelung ist gedeckt durch Artikel 6 Absatz 1 Satz 1 Buchstabe e („Wahrnehmung einer Auf-

gabe …, die im öffentlichen Interesse liegt“) i. V. m. Artikel 6 Absatz 3 Satz 1 der Verordnung (EU) 2016/679 und gestützt durch den Erwägungsgrund 45. Dort heißt es in Satz 5: „*Desgleichen sollte im Unionsrecht oder im Recht der Mitgliedstaaten geregelt werden, ob es sich bei dem Verantwortlichen, der eine Aufgabe wahrnimmt, die im öffentlichen Interesse liegt, oder in Ausübung öffentlicher Gewalt erfolgt, um eine Behörde oder um eine andere unter das öffentlichen Recht fallende natürliche oder juristische Person oder, sofern dies durch das öffentliche Interesse …. gerechtfertigt ist, eine natürliche oder juristische Person des Privatrecht … handeln sollte.*“

Öffentlich zugängliche großflächige Anlagen sind dabei bauliche Anlagen, die nach dem erkennbaren Willen des Betreibers von jedermann betreten oder genutzt werden können und von ihrer Größe her geeignet sind, eine größere Anzahl von Menschen aufzunehmen. Insbesondere kommen hierbei Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren und Parkräume in Betracht, die einen entsprechenden Publikumsverkehr aufweisen. Hierzu gehören auch Flächen, die eine gleichzeitige Anwesenheit vieler Menschen bei Veranstaltungen ermöglichen, und ganz oder teilweise aus baulichen Anlagen bestehen und daher auch besonderen baurechtlichen Bestimmungen der Länder unterliegen.

Der Personenverkehr bezeichnet die Ortsveränderung von Personen und umfasst die technischen, technologischen, organisatorischen und ökonomischen Bedingungen der Personenbeförderung und die zu befördernden Personen selbst. Die Beurteilung der Zulässigkeit einer Videoüberwachung unterliegt bei öffentlichen Verkehrsmitteln nur dann dem § 6b BDSG-alt, wenn der Verkehrsbetrieb nicht öffentlich-rechtlich betrieben wird.

Neben dieser auf Artikel 6 Abs. 1 Buchstabe e der Verordnung (EU) 2016/679 gestützten Überwachungsbefugnis verbleibt für andere Fallgestaltungen Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 als allgemeine Rechtsgrundlage der Videoüberwachung durch Private.

Die Regelung in Absatz 1 Nummer 2 Satz 2 enthält eine gesetzliche Vorgabe für die nach Absatz 1 Nummer 2 Satz 1 zu treffende Abwägungsentscheidung für den Einsatz von optisch-elektronischen Einrichtungen in von nicht-öffentlichen Stellen betriebenen öffentlich zugänglichen großflächigen Anlagen. Bei solchen Anlagen ist in der Abwägungsentscheidung verstärkt zu beachten, dass die Betreiber neben ihren zivilrechtlichen Verpflichtungen (z. B. Verkehrssicherungspflicht) auch sicherheitsrelevante Belange berücksichtigen sollen. Die aus dem grundgesetzlich abgesicherten Recht auf informationelle Selbstbestimmung herrührende Interessenabwägung nach Absatz 1 Nummer 2 Satz 2 bleibt weiterhin notwendig. Die Abwägung hinsichtlich der Zulässigkeit von Videoüberwachungsanlagen ist nicht pauschal, sondern für jede Teilanlage in diesen öffentlich zugänglichen großflächigen Anlagen oder Einrichtungen und Fahrzeugen des öffentlichen Personenverkehrs, gesondert vorzunehmen.

Absatz 2 legt fest, dass der Umstand der Videoüberwachung und des Verantwortlichen durch geeignete Maßnahmen erkennbar zu machen ist. Die Regelung entspricht § 6b Absatz 2 BDSG-alt.

Absatz 3 schafft eine § 6b Absatz 3 Satz 2 BDSG-alt entsprechende Regelung für die Zulässigkeit der Weiterverarbeitung.

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 diesem

Zweck werden in Umsetzung der Artikel 32 bis 34 der Richtlinie (EU) 2016/680 die für öffentliche Stellen unmittelbar geltenden Teile der Artikel 37 bis 39 der Verordnung (EU) 2016/679 in den §§ 5 bis 7 aufgegriffen.

Zu § 5 (Benennung)

In Umsetzung des Artikels 32 Absatz 1 der Richtlinie (EU) 2016/680 erfolgt in Absatz 1 eine wörtliche 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 Richlinie (EU) 2016/680 durch wortgleiche Wiederholung des Artikels 37 Absatz 3, 5 und 7 der Verordnung (EU) 2016/679 um.

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 Richlinie (EU) 2016/680 hinaus.

Absatz 6 entspricht der bisherigen Regelung des § 4f Absatz 3 Sätze 5 und 6 BDSG-alt. Bei dem besonderen 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.

Zu § 6 (Stellung)

Die Absätze 1 und 2 setzen Artikel 33 der Richtlinie (EU) 2016/680 durch inhaltsgleiche Wiederholung des Artikels 38 Absatz 1 und 2 der Verordnung (EU) 2016/679 um.

Die Absätze 3 und 4 Satz 1 übertragen die Vorgaben des Artikels 38 Absatz 3 und 4 der Verordnung (EU) 2016/679 wortgleich auf alle öffentlichen Stellen des Bundes, unabhängig davon, zu welchem Zweck die Datenverarbeitung erfolgt. Dies geht über die Vorgaben der Richlinie (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 eröffent ist (z. B. Nachrichtendienste) wird die Rechtsstellung der oder des behördlichen Datenschutzbeauftragten in öffentlichen Stellen des Bundes einheitlich ausgestaltet.

Die Regelung zur Verschwiegenheitspflicht in Absatz 4 Satz 2 entspricht § 4f Absatz 4 BDSG-alt. Die Verletzung von Privatgeheimnissen durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten ist gemäß § 203 Absatz 2a des Strafgesetzbuches zudem strafbewehrt. Das Zeugnisverweigerungsrecht in Absatz 5 sichert die Verschwiegenheitspflicht ab und entspricht § 4f Absatz 4a BDSG-alt. Die Regelungskomeptenz 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 Richlinie (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 setzt Artikel 34 der Richtlinie (EU) 2016/680 um. Um die Aufgaben der oder des Datenschutzbeauftragten öffentlicher Stellen für alle Verarbeitungszwecke einheitlich auszugestalten, wird Artikel 39 der Verordnung (EU) 2016/679 redaktionell angepasst und wiederholt.

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 Aritkel 34 der Richtlinie (EU) 2016/680, wird aber für den nationalen Bereich als Anwendungsbereich der Verordnung (EU) 2016/679 als allgemeiner Grundsatz festgeschrieben und allgemeine Regelungen für die Bereiche außerhalb des Rechts der Europäischen Union festgelegt.

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

Kapitel 4 passt die Regelungen des BDSG-alt 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-alt 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 sowie das Recht zur Anrufung 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-alt 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 (Satz 1) steht im engen Zusammenhang mit dem Erfordernis der völligen Unabhängigkeit der oder des Bundesbeauftragten (§ 19 BDSG-alt). 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 (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 Charak-

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

ters 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 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 Mitgliedstaates 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 Unionsrecht fällt oder nicht. Hierzu wird der bisherige § 24 Absatz 1 BDSG-alt ohne inhaltliche Änderungen sprachlich an die Verordnung (EU) 2016/679 angepasst. Zu den öffentlichen Stellen des Bundes zählen auch öffentliche Stellen des Bundes im Sinne des § 2 Absatz 1, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen (vormals § 27 Absatz 1 Nr. 2 a BDSG-alt). Spezialgesetzliche Zuweisungen der Datenschutzaufsicht über nicht-öffentliche 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 1b BDSG-alt (nicht-öffentliche Auftragnehmer in öffentlicher Hand) fort.

Die justizielle Tätigkeit der Bundesgerichte unterliegt – wie bisher nach § 24 Absatz 3 BDSG-alt – 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 der Richtlinie (EU) 2016/680 umgesetzt; Artikel 55 Absatz 3 der Verordnung (EU) 2016/679 gilt hingegen unmittelbar.

Zu § 10 (Unabhängigkeit)

Absatz 1 Satz 1 und 2 setzen 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-alt 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 fin-

det 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 Satz 1 und 3, Absatz 2 und 3 BDSG-alt unverändert übernommen. Im Anschluss an die bisherige Regelung zum Mindestalter (§ 22 Absatz 1 Satz 2 BDSG-alt) wird die Vorschrift in Absatz 1 Satz 4 und 5 um weitere Anforderungen an die Qualifikation und sonstigen 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-alt.

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-alt. 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, ausgezeichnete Kenntnisse des deutschen und europäischen Datenschutzrechts verfügen und die Befähigung zum Richteramt oder höheren Dienst haben muss.

In Absatz 2 wird die bisherige Regelung des § 22 Absatz 2 BDSG-alt 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-alt übernommene Regelung zur Länge der Amtszeit und zur einmaligen Wiederwahl entsprechen den Vorgaben des Artikels 54 Ab-

satz 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-alt 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 Abs. 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-alt 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-alt.

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-alt 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-alt 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-alt 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 die in § 23 Absatz 1 Satz 4 und 5 BDSG-alt angelehnt sind.

Satz 6 regelt die bislang in § 23 Absatz 1 Satz 6 BDSG-alt 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 § 26 Absatz 6 BDSG-alt 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-alt 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 Buchstaben a und c der Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstaben 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-alt 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-alt 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 sind eine wortgleiche Übernahme des bisherigen § 23 Absatz 3 bis 6 und 8 BDSG-alt.

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 Regelungsspielräumen zu den Pflichten und Handlungsverboten. Der bisherige § 23 Absatz 3 BDSG-alt wird unverändert übernommen.

Absatz 3 regelt das Zeugnisverweigerungsrecht der oder des Bundesbeauftragten und ihrer oder seiner Mitarbeiterinnen und 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-alt 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-alt wortgleich übernommen.

In Absatz 5 (Zeugenaussage und dessen Einschränkungen) wird der bisherige § 23 Absatz 6 BDSG-alt 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 enthält eine wortgleiche Übernahme des § 12 Absatz 3 und des § 23 Absatz 8 BDSG-alt 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 Zwecke 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 des 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-alt – auch für Datenverarbeitungen, die nicht in den Anwendungsbereich des Unionsrechts fallen.

Absatz 2 konkretisiert die Beratungsbefugnisse der oder des Bundesbeauftragten für den gesamten Anwendungsbereich des BDSG. Hiedurch 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 und 3 greift die bislang in § 26 Absatz 2 Satz 1 und 2 BDSG-alt geregelten Tätigkeiten der oder des Bundesbeauftragten auf Ersuchen (Erstellung von Gutachten, Erstattung von Berichten, Nachgehen von Hinsiwesen auf Angelegenheiten des Datenschutzes) auf. Diese stellen zusätzliche Befugnisse der oder des Bundesbeauftragten im Einklang mit Artikel 58 Absatz 6 der Verordnung (EU) 2016/679 dar.

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.

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

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–alt) 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 (Jahresberichts). 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 (Jahresberichts). Auch der Bundesrat ist nach unionsrechtlichem Verständnis nationales Parlament im Sinne des Artikel 12 des Vertrags über die Europäische Union (EUV) und der Protokolle Nr. 1 und 2 des Lissabon-Vertrags.Nach Satz 3 ist 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-neu die Befugnisse der oder des Bundesbeauftragten. Absatz 1 regelt die Befugnisse und deren Ausübung im Anwendungsbereich 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 sowie Datenerarbeitungen im Geltungsbereich der Richtlinie (EU) 2016/680. Absatz 3 bis 7 gelten sowohl im Anwendungsbereich der Verordnung (EU) 2016/679 und der Richtlinie 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-alt wird 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 erhalten. 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 Nr. 1 und Absatz 3 VwVfG angelehnten Ausnahmen für Eilfälle und entgegenstehende zwingende öffentlicher 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 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 Rechtsauffasung 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 keine Durchgriffsbefugnisse gegenüber Verantwortlichen beigegeben, 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 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 andererseits, die im Bereich der Richtlinie eine größere Flexibilität erlauben. 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-alt bekannten Instrument der Beanstandung 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.

In Absatz 3 wird für den gesamten Anwendungsbereich des BDSG-alt der bisherige § 24 Absatz 2 Satz 1 und 2 BDSG-alt weitgehend übernommen. Für Berufsgeheimnisträger findet sich im Anwendungsbereich der Verordnung (EU) 2016/679 eine Spezialregelung in § 27 BDSG-alt.

Absatz 4 greift die bislang in § 24 Absatz 4 Satz 2 BDSG-alt 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). Für die Zugangs- und Betretensrechte von Wohnungen gilt Absatz 1 Satz 2 unter den einschränkenden Maßgaben des Artikels 13 GG. Demnach muss entweder das Einverständnis des Verantwortlichen oder Auftragsverarbeiters vorliegen oder eine richterliche Anordnung bestehen und das Betreten der Grundstücke und Diensträume zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen, zur Verhütung der durch Datenschutzverstöße begründeten dringenden Gefahren für die öffentliche Sicherheit erforderlich sein.

Das umfassende Informationsrecht der oder des Bundesbeauftragten in Nummer 2 erfolgt in Umsetzung des Artikels 47 Absatz 1 der Richtlinie (EU) 2016/680 sowie aus Gründen der Verständlichkeit und Kohärenz unter Wiederholung des Artikels 58 Absatz 1 Buchstabe a der Verordnung 2016/679.

Absatz 5 enthält die bislang in § 26 Absatz 4 BDSG-alt vorgesehene Hinwirkungsfunktion der oder des Bundesbeauftragten auf die Zusammenarbeit mit den Aufsichtsbehörden der Länder im öffentlichen und nicht-öffentlichen 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 (EUZ-BLG) 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 Euro-

päischen 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. Bei persönlicher Verhinderung der oder des Bundesbeauftragten oder der Leiterin oder des Leiters der stellvertretenden Aufsichtsbehörde sind Abwesenheitsvertretungen durch die Vertreter im Amt möglich.

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 es einer inhaltlichen Vorabstimmung bedarf, 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 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 Datenschutzgrundverordnung 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-alt angelehnt.

Absatz 1 Satz 4 verpflichtet die Aufsichtsbehörden des Bundes und der Länder dazu, die nach Artikel 85 und 91 der Verordnung 2016/679 eingerichteten spezifischen Aufsichtsbe-

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

hörden 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 einer 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 Aufsichtsbeöhrden können im Rahmen möglicher Schwerpunktssetzungen von ihrem Recht auf Stimmenthaltung (Absatz 2 Satz 6) Gebrauch machen.

Die in 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 Abs. 2 und § 6 Abs. 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.

Zu § 19 (Zuständigkeiten)

§ 19 trifft ergänzend zu den Verfahrensregelungen des § 10 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 Über-

tragung 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 Mechanismus der Mehrheitsentscheidung aller Aufsichtsbehörden. Einen ähnlichen Mechanismus innerhalb des Europäischen Datenschutzausschusses sieht Artikel 65 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 vor.

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 Datenschutzgrundverordnung 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. Zu den Personen gehören damit auch Behörden.

Soweit durch bereichsspezifische Rechtsvorschriften des Bundes der Rechtsweg vor anderen Gerichten als den Verwaltungsgerichten eröffnet ist (siehe z.B. § 51 Sozialgerichtsgesetz für die Gerichte der Sozialgerichtsbarkeit), findet § 20 keine Anwendung.

Absatz 1 Satz 1 bestimmt, dass von § 20 das Straf- und Bußgeldverfahren ausgenommen ist, da in dessen Anwendungsbereich nicht der Verwaltungsrechtsweg, sondern der Weg zu den Gerichten der ordentlichen Gerichtsbarkeit eröffnet ist.

Durch Absatz 3 wird die Zuständigkeit 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 besteht keine Befugnis, durch Verwaltungsentscheidung die aufschiebende Wirkung der Anfechtungsklage einer anderen Behörde auszuschließen. Unbeschadet der Anordnungskompetenz der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit stehen sich die beteiligten Verwaltungsträger nicht in einem Subordinationsverhältnis gegenüber. Im Falle einer Verwaltungsstreitsache kann eine verbindliche Entscheidung allein durch das Verwaltungsgericht getroffen werden.

Zu § 21 (Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Europarechtswidrigkeit eines Angemessenheitsbeschlusses der Kommission)

§ 21 enthält erstmals eine Regelung zu Rechtsbehelfen der Aufsichtsbehörden des Bundes und der Länder gegen Angemessenheitsbeschlüsse der Europäischen Union nach Artikel 45 der Verordnung (EU) 2016/679 und Artikel 36 der Richtlinie (EU) 2016/680.
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 be-

treiben oder sich sonst daran zu beteiligen, um die Bestimmungen der Verordnung oder Richtlinie durchzusetzen. Im Rahmen der Durchführung dieser Vorschriften dient § 22 auch der Umsetzung des EuGH-Urteils vom 6. Oktober 2015 (Rechtssache C-362/14, Maximillian Schrems ./. Data Protection Commissioner), in dem der Europäische Gerichtshof die Angemessenheitsentscheidung der Kommission [Entscheidung der 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 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 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)

§ 22 Absatz 1 regelt Sachverhalte, bei deren Vorliegen abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 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. Durch den Zusatz „unbeschadet anderer Rechtsvorschriften“ wird zusätzlich klargestellt, dass die Verarbeitung besonderer Kategorien personenbezogener Daten zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679 nicht nur auf dieser Rechtsgrundlage zulässig ist, sondern etwa auch auf der Grundlage der weiteren in Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 aufgeführten Erlaubnistatbestände einschließlich der auf der Grundlage der Verordnung (EU) 2016/679 erlassenen bereichsspezifischen Regelungen.

Absatz 1 Nummer 1 erfasst die Tatbestände, die für öffentliche und nicht-öffentliche Stellen gleichermaßen gelten, während Absatz 1 Nummer 2 nur Tatbestände für öffentliche Stellen enthält. Im Einzelnen wird mit der Vorschrift von der Öffnungsklausel 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 g der Verordnung (EU) 2016/679 (in Bezug auf Absatz 1 Nummer 2 Buchstabe a bis d, 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 und des Artikels 9 Absatz 2 Buchstabe i der Verordnung (EU) 2016/679 (in Bezug auf Absatz 1 Nummer 1 Buchstabe c Gebrauch gemacht.

Absatz 1 Nummer 1 Buchstabe b entsprechen im wesentlichen § 13 Absatz 2 Nummer 7 und § 28 Absatz 7 BDSG-alt und Absatz 1 Nummer 2 Buchstabe a bis d dem § 13 Absatz 1 Nummern 1, 5, 6 und 9 BDSG-alt. 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 Indentifikation Betroffener verarbeitet werden.

Absatz 1 Nummer 1 Buchstabe d stützt sich auf Artikel 9 Absatz 2 Buchstabe j der Verordnung (EU) 679/2016. Von der in Absatz 1 Nummer 1 Buchstabe d geregelten Verarbeitung ist zugleich die Weiterverarbeitung umfasst, da nach Artikel 5 Absatz 1 Buchstabe b a. E. der der Verordnung (EU) 679/2016 eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke oder für statistische Zwecke nicht als unvereinbar mit den ursprünglichen Zwecken gilt und Erwägungsgrund 50 Satz 2 vorsieht, dass im Falle der Vereinbarkeit der Zwecke für die Weiterverarbeitung „keine andere gesonderte Rechtsgrundlage erforderlich ist als diejenige für die Erhebung der personenbezogenen Daten“.

Absatz 2 Satz 1 setzt das Erfordernis aus Artikel 9 Absatz 2 Buchstabe b, g und i der Verordnung (EU) 2016/679 um, „geeignete Garantien“ bzw. „angemessene und spezifische Maßnahmen“ vorzusehen. Die in Artikel 9 Absatz 2 Buchstabe h der Verordnung (EU) 2016/679 unter Bezugnahme auf den dortigen Absatz 3 geforderten besonderen Garantien sind unmittelbar durch Absatz 1 Nummer 1 Buchstabe b umgesetzt und daher in von Absatz 2 Satz 1 ausgenommen. Die in Absatz 2 Satz 2 aufgeführten Maßnahmen nach den Artikeln 25, 32 und 35 der Verordnung (EU) 2016/679 treffen jeden Verantwortlichen und damit auch jeden, der besondere Kategorien personenbezogener Daten verarbeitet. Die zusätzlich in Nummer 2 genannte besondere Maßnahme der Sensibilisierung und Schulung greift Artikel 39 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 auf. Die in Nummer 1 genannte besondere Maßnahme ist Nummer 5 der Anlage zu § 9 Satz 1 BDSG-alt entlehnt.

Durch Absatz 3 wird von der Möglichkeit des Artikels 9 Absatz 4 der Verordnung (EU) 2016/679 Gebrauch gemacht.

Zu § 23 (Verarbeitung zu anderen Zwecken)

Die Vorschrift schafft ausschließlich für den Anwendungsbereich der Verordnung (EU) 2016/679 eine nationale Rechtsgrundlage für die Weiterverarbeitung personenbezogener Daten zu anderen Zwecken durch öffentliche und nicht-öffentliche Stellen. Weiterverarbeitungen personenbezogener Daten zu anderen Zwecken als zu demjenigen, zu dem sie ursprünglich erhoben wurden, können damit über die nach Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 eröffnete Möglichkeit der Weiterverarbeitung personenbezogner Daten zu vereinbaren Zwecken auf diese Vorschrift gestützt werden, soweit einer der tatbestandlichen Voraussetzungen erfüllt ist.

Die Vorschrift unterscheidet, ob Weiterverarbeitungen personenbezogener Daten durch öffentliche Stellen oder nicht-öffentliche Stellen vorgenommen werden und welche Kategorien von Daten weiterverarbeitet werden sollen. Die Absatz 1 und 2 regeln danach unterteilt nach öffentlichen Stellen (Absatz 1) und nicht-öffentlichen Stellen (Absatz 2) die Weiterverarbeitungen personenbezogener Daten, die Absätze 3 und 4 wiederum unterteilt nach öffentlichen Stellen (Absatz 3) und nicht-öffentlichen Stellen (Absatz 4) die Weiterverarbeitungen besonderer Kategorien personenbezogener Daten.

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 Regelung orientiert sich an den Regelungen der §§ 14 Absatz 2, 3, 5 und 4, 13 Absatz 2 und § 16 Absatz 1 Nummer 2 Satz 2 BDSG-alt, soweit es um die zweckändernde Weiterverarbeitung durch öffentliche Stellen geht und an den §§ 28 Absatz 2 i. V. m.Absatz 1 Nummer 2 und 3 sowie § 28 Absatz 8 Satz 1 i. V. m. Absatz 6 Nummern 1 bis 3 und Absatz 7 Satz 2 und Absatz 8 Satz 2 BDSG-alt, soweit die zweckändernde Weiterverarbeitung durch nicht-

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

öffentliche Stellen betroffen ist. Indem die Vorschrift allgemein an den Begriff der Verarbeitung anknüpft, sind auch Datenübermittlungen umfasst.

Zu § 24 (Verarbeitung im Beschäftigungskontext)

Absätze 1 bis 2 entsprechen § 32 BDSG-alt. Der Wortlaut ist an die Terminologie der Verordnung (EU) 2016/679 angepasst. Die Öffnungsklausel des Artikels 88 der Verordnung (EU) 2016/679 lässt nationale Regelungen zur Datenverarbeitung im Beschäftigungskontext zu.

Artikel 88 Absatz 1 der Verordnung bestimmt ausdrücklich, dass Mitgliedstaaten Vorschriften zur Verarbeitung personenbezogener Beschäftigtendaten auch in Form von Kollektivvereinbarungen vorsehen können. Auch Erwägungsgrund 41 bestätigt, dass sich Rechtsgrundlagen einer Datenverarbeitung nicht immer zwingend allein nur aus gesetzlichen Vorgaben ergeben können. Dem trägt § 24 Absatz 1 Satz 1 Rechnung: Wenn es dort heißt, dass personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden dürfen, ist davon auch die Datenverarbeitung aufgrund von Kollektivvereinbarungen umfasst, indem die Möglichkeit einer Regelung durch Kollektivvereinbarung zur Klarstellung ausdrücklich genannt wird.
Absatz 3 übernimmt weitgehend die bisher in § 3 Absatz 11 BDSG-alt vorgesehenen Begriffsbestimmungen. In Nummer 5 wurden die Ausführungen zum Jugendfreiwilligendienstegesetz redaktionell überarbeitet und um das Bundesfreiwilligendienstgesetz ergänzt.

Zu § 25 (Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken)

Mit § 25 Absatz 1 wird von der Ermächtigung aus Artikel 9 Absatz 2 Buchstabe j der Verordnung (EU) Nr. 679/2016 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 regelt Ausnahmen von diesem Verbot: So ist die Verarbeitung besonderer Kategorien personenbezogener Daten z.B. zulässig, wenn die betroffene Person eingewilligt hat (Buchstabe a) oder für wissenschaftliche oder historische Forschungszwecke eine nationale Regelung geschaffen wurde (Buchstabe j).

Bereits das bisherige BDSG-alt enthielt sogenannte „Forschungsklauseln“, die eine Verarbeitung sensibler Daten auch ohne Einwilligung der betroffenen Person nach Abwägung der Interessen der Forschung mit jenen der betroffenen Person zuließen (§ 13 Absatz Nr. 8; § 14 Absatz Nr. 9, Absatz 5 Satz 1 Nr. 2; § 28 Absatz 2 Nr. 3, Absatz 6 Nr. 4 BDSG-alt). § 25 Absatz 1 sieht eine vergleichbare Regelung vor, die für die öffentliche und private Forschung gilt.

Artikel 9 Absatz 2 Buchstabe j der Verordnung (EU) Nr. 679/2016 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 Rechnung.

§ 25 Absatz 1 gilt nicht für die Weiterverarbeitung nicht-sensibler Daten. Diese richtet sich entweder unmittelbar nach der Verordnung (EU) 679/2016 (insbesondere Artikel 6 Absatz 1) oder nach den Rechtsgrundlagen der Verarbeitung, die dieses Gesetz (insbesondere § 3 BDSG-neu) an anderer Stelle vorsieht (sofern nicht ohnehin bereichsspezifisches Recht greift).

Von der in § 25 geregelten Verarbeitung ist zugleich die Weiterverarbeitung umfasst, da nach Artikel 5 Absatz 1 Buchstabe b a. E. der Verordnung (EU) 679/2016 eine Weiterverarbeitung für wissenschaftliche oder historische Forschungszwecke nicht als unvereinbar mit den ursprünglichen Zwecken gilt und Erwägungsgrund 50 Satz 2 vorsieht, dass im Falle der

Vereinbarkeit der Zwecke für die Weiterverarbeitung „keine andere gesonderte Rechtsgrundlage erforderlich ist als diejenige für die Erhebung der personenbezogenen Daten“.

§ 25 Absatz 2 schränkt unter Ausnutzung der Öffnungsklausel des Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 679/2016 das Auskunftsrecht nach Artikel 15 der Verordnung (EU) 679/2016 ein. Wie schon bisher (§ 33 Absatz 2 Satz 1 Nr. 5 BDSG-alt) gilt diese Beschränkung nur gegenüber nicht-öffentlichen Stellen. Beschränkungen der Betroffenenrechte sind darüber hinaus nicht nur nach Artikel 89 Absatz 2 der Verordnung (EU) 679/2016, sondern auch nach Artikel 23 der Verordnung (EU) 679/2016 möglich, da die Verarbeitung zu Forschungszwecken anderenfalls gegenüber sonstigen Verarbeitungen schlechter gestellt wäre, obwohl der Verordnungsgeber Forschung ausweislich der Sonderreglung in Kapitel IX der Verordnung (EU) 679/2016 privilegieren wollte. Es finden mithin auch bei der Verarbeitung zu Forschungszwecken die Vorschriften der §§ 30 ff. BDSG-neu Anwendung; daraus ergibt sich z. B. auch gegenüber öffentlichen Stellen eine Beschränkung des Auskunftsrechts aus Gründen eines unverhältnismäßigen Aufwandes (§ 32 Absatz 1 Nr. 3 BDSG-neu) sowie eine Beschränkung wegen Gefährdung ordnungsgemäßer Aufgabenerfüllung bzw. erheblicher Gefährdung des Geschäftszweckes (§ 32 Absatz 1 Nr. 1 i. V. m. § 31 Absatz 2 Nr. 1 bzw. Absatz 3 Nr. 1 BDSG-neu).

Absatz 3 ist § 40 BDSG-alt entlehnt und macht von der Möglichkeit des Artikel 9 Absatz 4 der Verordnung (EU) 679/2016 Gebrauch, dass die Mitgliedstaaten im Hinblick auf die Verarbeitung von genetischen oder Gesundheitsdaten zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten können.

Soweit spezialgesetzliche Regelungen zur Datenverarbeitung aus dem bereichsspezifischen Recht anzuwenden sind, gehen sie § 25 vor (§ 1 Absatz 2 BDSG-neu). Solche spezialgesetzlichen Regelungen finden sich derzeit etwa in den Sozialgesetzbüchern oder in medizinrechtlichen Gesetzen (z. B. Arzneimittelgesetz, Gendiagnostikgesetz, Transplantationsgesetz).

Zu § 26 (Verarbeitung von einer Geheimhaltungspflicht unterliegenden Daten)

Auf der Grundlage der Öffnungsklausel des Artikel 23 Abs. 1 Buchstabe i der Verordnung (EU) 2016/679 beschränkt Absatz 1 wie bisher nach dem BDSG-alt 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-alt) und Auskunft § 19 Abs. 4 Nr. 3; § 34 Abs. 7 BDSG-alt. Absatz 1 ergänzt die unmittelbar nach Artikel 14 Absatz 5 Buchstabe c und d geltenden Ausnahmen von der Informationspflicht aus Gründen des Vertraulichkeitsschutzes insbesondere in den Fällen, in denen eine gesetzliche oder satzungsmäßige Geheimhaltungspflicht nicht besteht, die Daten aber ihrem Wesen nach geheim gehalten werden müssen.

Absatz 2 Satz 1 macht von der Öffnungsklausel des Artikels 90 Gebrauch, ihr entspricht Erwägungsgrund 164 der Verordnung. Nach Artikel 58 Absatz 1 Buchstabe 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 Berufsgeheimnisträgern zu regeln. 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, Urt. v. 12.4.05, NJW 2005, S. 1917). Absatz 2 Satz 2 verlängert die Geheimhaltungspflicht auf die Aufsichtsbehörde und schafft ein Beweisverwertungsverbot im Strafverfahren.

Zu § 27 (Datenübermittlung an Auskunfteien)

§ 27 Absätze 1 bis 3 entspricht § 28a BDSG-alt und § 27 Absatz 4 entspricht § 35 Absatz 2 Satz 3 BDSG-alt. So mit einer Übermittlung an Auskunfteien eine Änderung des Zweckes einhergeht, für den die Daten ursprünglich erhoben wurden, bedarf es für den Beibehalt der nationalen Regelung des § 28a BDSG-alt einer Öffnungsklausel. Diese ergibt sich aus der Zusammenschau der Artikel 6 Absatz 4 und Artikel 23 Absatz 1 der Verordnung (EU) 2016/679: Artikel 6 Absatz 4 regelt die Zulässigkeit der Verarbeitung personenbezogener Daten zu einem anderem Zweck als demjenigen, zu dem die Daten ursprünglich erhoben wurden. Für die Fälle, der Zweck der Weiterverarbeitung nicht mit dem ursprünglichen Zweck vereinbar ist, kann gemäß Artikel 6 Absatz 4 eine nationale Regelung erlassen werden, die eine „in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt“. Artikel 23 Absatz 1 Buchstabe e nennt hierzu den „Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses … eines Mitgliedstaats“. Die durch Auskunfteien erfolgende Datenverarbeitung müsste also einem solchen wichtigen Ziel des allgemeinen öffentlichen Interesses dienen. In der höchstrichterlichen Rechtsprechung ist anerkannt, dass „die Erteilung von Bonitätsauskünften für das Funktionieren der Wirtschaft von erheblicher Bedeutung ist“ (BGH, NJW 2011, 2204, 2206). Verbraucher vor Überschuldung zu schützen, liegt sowohl im Interesse der Verbraucher 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. Das erforderliche wichtige Ziel von allgemeinem öffentlichen Interesse ist gegeben.

Zu § 28 (Scoring)

Die Vorschrift erhält die wesentlichen Regelungen des § 28b BDSG-alt aufrecht. Eine mitgliedstaatliche Regelungsbefugnis ergibt sich aus der Zusammenschau der Artikel 6 Absatz 4 und Artikel 23 Absatz 1 Verordnung (EU) 2016/679. Voraussetzung ist, dass die nationale Vorschrift eine „in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt“. Artikel 23 Absatz 1 Buchstabe e nennt hierzu den „Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses … eines Mitgliedstaats“. Die beim Scoring erfolgende Datenverarbeitung müsste also einem solchen wichtigen Ziel des allgemeinen öffentlichen Interesses dienen. In der höchstrichterlichen Rechtsprechung ist anerkannt, dass „die Erteilung von Bonitätsauskünften für das Funktionieren der Wirtschaft von erheblicher Bedeutung ist“ (BGH, NJW 2011, 2204, 2206). Verbraucher vor Überschuldung zu schützen, liegt sowohl im Interesse der Verbraucher 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. Das erforderliche wichtige Ziel von allgemeinem öffentlichen Interesse ist gegeben.

Zu § 29 (Verbraucherkredite)

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

Zu §§ 30-35 (Kapitel 2) (Rechte der betroffenen Person)

Artikel 23 der Verordnung (EU) 2016/679 sieht vor, dass die in Kapitel III der Verordnung vorgesehenen Rechte und Pflichten (Artikel 12 bis 22) sowie die diesen entsprechenden Rechte und Pflichten der Artikel 34 (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person) und Artikel 5 (Grundsätze für die Verarbei-

tung personenbezogener Daten) durch Rechtsvorschriften der Union oder der Mitgliedstaaten in bestimmten Fällen 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 Absatz 1 der Verordnung (EU) 2016/679 ist die Nachfolgeregelung des Artikels 13 Absatz 1 der durch die Verordnung abgelösten Richtlinie 95/46/EG, auf welchem die bislang im BDSG-alt geregelten Ausnahmen und Einschränkungen der Betroffenenrechte (§§ 19, 19a, 20, 33, 34, 35 BDSG-alt) beruhen. Artikel 23 der Verordnung (EU) 2016/679 erweitert die eine Beschränkung der Rechte und Pflichten des Verantwortlichen oder Auftragsverarbeiters legitimierenden Ziele und Interessen (insb. um die Buchstaben d, f und j), verlangt im Vergleich zu Artikel 13 Absatz 1 der Richtlinie 95/46/EG aber zugleich besondere Schutzmaßnahmen zum Schutz der Grundrechte und Grundfreiheiten der von der Beschränkung betroffenen Person. Insbesondere muss gemäß Art. 23 Absatz 2 der Verordnung (EU) 2016/679 jede Gesetzgebungsmaßnahme zudem „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 knüpfen in Ergänzung zu den in der Verordnung (EU) 2016/679 teilweise unmittelbar vorgesehenen Ausnahmen an die bisher im BDSG-alt erfolgten Einschränkungen an. Sofern nicht im Einzelfall abweichend geregelt, gelten die Einschränkungen, „wenn und soweit“ Gründe für eine Beschränkung vorliegen. Die Beschränkungen der Rechte der betroffenen Person sind auf den zwingend erforderlichen Umfang zu begrenzen. Der Verantwortliche hat daher stets zu prüfen, ob dem Recht der betroffenen Person zumindest teilweise entsprochen werden kann.

Die Beschränkungen der Informationspflicht (§§ 30, 31) und des Auskunftsrechts (§ 32) entbinden den Verantwortlichen von der Pflicht zur Information der betroffenen Person, wenn und soweit die Voraussetzungen des Absatzes 1 erfüllt sind; dem Verantwortlichen steht es frei, in geeigneten Fällen, insbesondere im Fall der Unverhältnismäßigkeit, den betroffenen Personen die Information oder Auskunft dennoch auf freiwilliger Grundlage zu erteilen.

Die Beschränkungen der Betroffenenrechte in Kapitel 2 finden auch Anwendung auf die in Artikel 89 der Verordnung (EU) Nr. 679/2016 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 diesen Zwecken Mitgliedstaaten insoweit Ausnahmen von den Rechten gemäß der Artikel 15, 16, 18 und 21 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) Nr. 679/2016 möglich sein, da die Verarbeitung zu den in Artikel 89 genannten Zwecken anderenfalls 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) Nr. 679/2016 privilegieren wollte. Hieraus ergibt sich z.B. für den Fall, dass öffentliche Stellen personenbezogene Daten zu Archiv-, Forschungs- und Statistikzwecken verarbeiten, eine Beschränkung des Auskunftsrechts aus Gründen eines unverhältnismäßigen Aufwandes (§ 32 Absatz 1 Nr. 3) sowie eine Beschränkung wegen Gefährdung ordnungsgemäßer Aufgabenerfüllung bzw. erheblicher Gefährdung des Geschäftszweckes (§ 32 Absatz 1 Nr. 1 i. V. m. § 31 Absatz 2 Nr. 1 bzw. Absatz 3 Nr. 1).

Zu § 30 (Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person)

Absatz 1 schränkt die gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 bestehende Informationspflicht für öffentliche und nicht-öffentliche Stellen ein, wenn und soweit die Erteilung der Information sich als unmöglich erweist (Nummer 1), einen unverhältnismäßigen Aufwand erfordern würde (Nummer 2) oder die Verwirklichung des Verarbeitungszwecks voraussichtlich unmöglich machen oder ernsthaft beeinträchtigen würde und deshalb das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss (Nummer 3).

Die in Absatz 1 vorgesehene Beschränkung 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 mit der Verordnung (EU) 2016/679 erstmals eingeführte (Folge-)Informationspflicht des Verantwortlichen bei beabsichtigter Zweckänderung findet im BDSG-alt 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 bei der betroffenen Person typischerweise kein unmittelbarer Kontakt zwischen dem Verantwortlichen und der betroffenen Person, der es dem Verantwortlichen ohne Weiteres ermöglichen würde, die betroffene Person ohne unverhältnismäßig hohen Aufwand von der Absicht der weiteren Verarbeitung in Kenntnis zu setzen.

In diesen Fällen kann sich die Information der betroffenen Person als unmöglich oder unverhältnismäßig erweisen, beispielsweise wenn die Kontaktdaten des Betroffenen dem Verantwortlichen nicht bekannt und auch nicht ohne Weiteres zu ermitteln sind. Strukturell ist diese Situation mit der in Artikel 14 Absatz 4 der Verordnung (EU) 2016/679 vorgesehenen Informationspflicht über beabsichtigte Zweckänderungen vergleichbar. Eine Differenzierung danach, ob die personenbezogenen Daten bei der betroffenen Person erhoben (Artikel 13) oder nicht erhoben wurden (Artikel 14 der Verordnung (EU) 2016/679) ist nicht gerechtfertigt. Der in Artikel 14 Absatz 5 Buchstabe b Halbsatz 1 der Verordnung (EU) 2016/679 unmittelbar vorgesehene Ausschlussgrund der Unmöglichkeit oder Unverhältnismäßigkeit ist daher auf die vorliegende Situation übertragbar. Eine Unverhältnismäßigkeit kann sich insbesondere – wie bisher (§ 33 Absatz 2 Satz 1 Nummer 7a), 8 und 9 BDSG-alt) – aus der Zahl der betroffenen Personen ergeben. Auch das Alter der Daten oder das Bestehen geeigneter Garantien sind als Anhaltspunkte einzubeziehen (Erwägungsgrund 62 der Verordnung (EU) 2016/679).

Ebenfalls übertragbar ist der in Artikel 14 Absatz 5 Buchstabe b Halbsatz 2 Alternative 2 der Verordnung 2016/679 als Unterfall der Unmöglichkeit und Unverhältnismäßigkeit vorgesehene Ausschlussgrund der Zweckgefährdung und Zweckvereitelung, der um die Notwendigkeit einer Interessenabwägung ergänzt wird. Erfasst sind die Fallgruppen, in denen die Erteilung der Information gegenüber der betroffenen Person zu einer Vereitelung oder ernsthaften Beeinträchtigung des – legitimen – Verarbeitungszwecks führen würde, etwa wenn die zuständige Strafverfolungsbehörde über den Verdacht einer Straftat informiert werden soll. Erfasst sind weiterhin Weiterverarbeitungen, die aufgrund im Einzelfall bestehender besonderer Eilbedürftigkeit keinen Aufschub dulden, etwa wenn die Weiterverarbeitung erforderlich ist zur Abwehr einer unmittelbaren Gefahr für die öffentliche Sicherheit, erheblicher Nachteile für das Gemeinwohl oder einer schwerwiegenden Beeinträchtigung der Rechte der betroffenen oder einer anderen Person, wie dies aus dem Rechtsgedanken des § 14 Absatz 2 Nummer 3, 6 und 8 BDSG-alt folgt.

Die Einschränkung entspricht dem Rechtsgedanken des Artikel 23 Absatz 2 Buchstabe h der Verordnung (EU) 2016/679, nach welchem die betroffene Person über die Beschränkung ihrer Rechte nicht zu unterrichten ist, sofern dies dem Zweck der Beschränkung abträglich

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

ist. Sie findet sich zudem in Artikel 89 Absatz 2 und 3 der Verordnung (EU) 2016/679 für den speziellen Bereich der Datenverarbeitungen zu wissenschaftlichen oder historischen Forschungszwecken, statistischen Zwecken und für im öffentlichen Interesse liegende Archivzwecke. Auch das BDSG-alt kennt im Zusammenhang mit dem Auskunftsrecht gem. § 19 Absatz 5 Satz 1 den Beschränkungsgrund der Zweckgefährdung, welcher dazu führt, dass die Ablehnung der Auskunftserteilung keiner Begründung bedarf.

Die Einschränkung des Informationsrechts nach Absatz 1 beruht auf Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679. Der Schutz der Rechte und Freiheiten anderer Personen umfasst, wie schon unter der Anwendung des Artikel 13 Absatz 1 Buchstabe g der Richtlinie 95/46/EG (so Ehmann/Helfrich, EG-Datenschutzrichtlinie, Art. 13 Rn. 72f.), auch die Rechtspositionen des Verantwortlichen. Die Einbeziehung des Verantwortlichen in den Schutzbereich des Artikel 23 zeigt sich auch an Absatz 1 Buchstabe j der Verordnung (EU) 2016/679, welcher Einschränkungen der Betroffenenrechte und Verarbeiterpflichten zur Durchsetzung zivilrechtlicher Ansprüche für zulässig erachtet und in der genannten Fallkonstellation ebenfalls einschlägig sein kann.

Absatz 2 legt fest, dass der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person zu treffen hat, wenn eine Information der betroffenen Person nach Maßgabe des Absatzes 1 unterbleibt. Hierdurch wird Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 umgesetzt. Zu den geeigneten Maßnahmen kann die Bereitstellung dieser Informationen für die Öffentlichkeit zählen. 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). Im Fall der Informationspflicht nach Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 wird hiermit eine identische Regelung wie im Fall des Artikel 14 Absatz 5 Buchstabe b Satz 2 in Verbindung mit Artikel 14 Absatz 4 der Verordnung (EU) 2016/679 geschaffen.

Der Verantwortliche hat schriftlich festzulegen, unter welchen Voraussetzungen von einer Informationspflicht abgesehen wird. Die Stichhaltigkeit der Gründe und Fallgruppen unterliegt der Kontrolle durch die zuständige Aufsichtsbehörde, die durch die Dokumentationspflicht ermöglicht wird. Die Regelung setzt § 19a Absatz 2 Satz 2 und § 33 Absatz 2 Satz 2 BDSG-alt fort, welcher das Erfordernis „geeigneter Garantien“ gemäß Artikel 11 Absatz 2 der Richtlinie 95/46/EG in das BDSG-alt umsetzt. Die nach BDSG-alt bislang nur für bestimmte Fallgruppen vorgesehene Dokumentationspflicht wird in Absatz 2 Satz 2 auf sämtliche Gründe für die Beschränkung der Informationspflicht ausgedehnt.

Absatz 3 schränkt die Informationspflicht öffentlicher und nicht-öffentlicher Stellen gemäß Artikel 13 Absatz 1 bis 3 der Verordnung (EU) 2016/679 in zeitlicher Hinsicht ein. Wenn und soweit dem Verantwortlichen die Information der betroffenen Personen zum Zeitpunkt der Erhebung oder im Fall des Artikel 13 Absatz 3 zum Zeitpunkt der Weiterverarbeitung vorübergehend unmöglich ist, ist die Informationspflicht nach Entfallen des Hinderungsgrundes innerhalb einer angemessenen Frist, spätestens jedoch innerhalb von 14 Tagen, nachzuholen. Die Unmöglichkeit der Informationserteilung zum Zeitpunkt der Erhebung personenbezogener Daten bei der betroffenen Person ist häufig bei der großflächigen Videoüberwachung öffentlich zugänglicher Räume gegeben. Die Einschränkung ist insbesondere hier erforderlich, da dem Verantwortlichen eine umfassende Information der betroffenen Personen über alle in Artikel 13 Absatz 1 und 2 der Verordnung (EU) 2016/679 aufgezählten Aspekte zum Zeitpunkt der Erhebung der personenbezogenen Daten, also bei Betreten des Erfassungsbereichs der Videoüberwachung durch die betroffene Person, in aller Regel unmöglich ist.

Die im zeitlicher Hinsicht (Artikel 23 Absatz 2 Buchstabe c vorgesehene Einschränkung dient dem Schutz der Rechte und Freiheiten des Verantwortlichen (Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679, da dem Verantwortlichen Unmögliches nicht abverlangt wer-

den kann. Absatz 3 enthält spezifische Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person (Artikel 23 Absatz 2 der Verordnung (EU) 2016/679). Satz 1 stellt klar, dass das Entfallen der Informationspflicht lediglich zeitlich auf das Bestehen des Hinderungsgrundes beschränkt ist. Satz 2 stellt klar, dass bei der Videoüberwachung öffentlich zugänglicher Räume entsprechend § 6b Absatz 2 BDSG-alt in jedem Fallder Umstand der Beobachtung sowie der Verantwortliche erkennbar zu machen, um den betroffenenen Personen frühzeitig Transparenz über die Tatsache der Datenverarbeitung mittels Videoüberwachung zu vermitteln und ihnen zu ermöglichen, sich auf den Umstand der Videoüberwachung einzustellen (Satz 3).

Zu § 31 (Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden)

§ 31 Absatz 1 enthält über die sich unmittelbar aus Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 ergebenden Ausnahmen hinaus Einschränkungen der Informationspflicht des Verantwortlichen aus Artikel 14 Absätze 1 und 2 der Verordnung (EU) 2016/679, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden.

Absatz 1 Nummer 1, der nur für öffentliche Stellen gilt, enthält die Ausnahmeregelungen des § 19a Absatz 3 i. V. m. § 19 Absatz 4 Nummer 1 und 2 BDSG-alt.

Absatz 1 Nummer 1 Buchstabe a entspricht § 19a Absatz 3 i. V. m. § 19 Absatz 4 Nummer 1 BDSG-alt. Die Beschränkung der nach Artikel 14 Absätze 1 bis 3 der Verordnung (EU) 2016/679 bestehenden Informationspflicht dient der Gewährleistung der Funktionsfähigkeit und Aufgabenerledigung der öffentlichen Verwaltung und somit dem Schutz eines wichtigen Ziels des allgemeinen öffentlichen Interesses (Artikel 23 Absatz 1 Buchstabe e) der Verordnung (EU) 2016/679.

Absatz 1 Nummer 1 Buchstabe b entspricht §§ 19a Absatz 3 i. V. m. § 19 Absatz 4 Nummer 2 BDSG-alt. Die im konkreten Umfang (Artikel 23 Absatz 2 Buchstabe c vorgesehene Beschränkung der Informationspflicht dient dem Schutz der öffentlichen Sicherheit (Artikel 23 Absatz 1 Buchstaben c oder der Verhütung, Ermittlung, Ausdeckung oder Verfolgung von Straftaten oder Strafvollstreckung (Artikel 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679.

Absatz 1 Nummer 2, der nur für nicht-öffentliche Stellen geltende Ausnahmen von der Informationspflicht regelt, entspricht § 33 Absatz 2 Satz 1 Nummer 6 und 7b) BDSG-alt.

Absatz 1 Nummer 2 Buchstabe a entspricht § 33 Absatz 2 Satz 1 Nummer 7b) BDSG-alt. Die im konkreten Umfang (Artikel 23 Absatz 2 Buchstabe c vorgesehene Beschränkung der Informationspflicht dient dem Schutz der Rechte und Freiheiten des Verantwortlichen als „anderer Person“ im Sinne des Artikel 23 Absatz 1 Buchstabe i der Verordnung 2016/679. 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 Geschäftszwecke des Verantwortlichen insgesamt gefährdet werden.

Absatz 1 Nummer 2 Buchstabe b entspricht § 33 Absatz 2 Satz 1 Nummer 6 BDSG-alt. Die im konkreten Umfang (Artikel 23 Absatz 2 Buchstabe c vorgesehene Beschränkung der Informationspflicht dient dem Schutz der öffentlichen Sicherheit (Artikel 23 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679.

Die bislang für öffentliche Stellen in § 19a Absatz 3 i. V. m. § 19 Absatz 2 BDSG-alt und für nicht-öffentliche Stellen in § 33 Absatz 2 Satz 1 Nummer 2 BDSG-alt vorgesehene Ausnahme von der Benachrichtigungspflicht für personenbezogene Daten, die nur deshalb gespei-

chert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde, werden als Unterfall des Unverhältnismäßigkeit unmittelbar in Artikel 14 Absatz 5 Buchstabe b der Verordnung (EU) 2016/679 erfasst. Eine Regelungsnotwendigkeit besteht daher nicht.

Absatz 2 enthält eine § 30 Absatz 2 entsprechende Pflicht des Verantwortlichen, geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person zu ergreifen. Danach hat der Verantwortliche im Falle einer unterbleibenden Information der betroffenen Person geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person zu treffen. Mit der Regelung wird erreicht, dass bei den in Absatz 1 vorgesehenen Ausnahmen gleichlaufend zu Artikel 14 Absatz 5 Buchstabe b Satz 2 der Verordnung (EU) 2016/679 zu verfahren ist.

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

Zu § 32 (Auskunftsrecht der betroffenen Person)

§ 32 Absatz 1 und 2 enthält Einschränkungen des Auskunftsrechts der betroffenen Person, mit welchen die bereits im BDSG-alt bestehenden Regelungen im Rahmen des Artikel 23 der Verordnung (EU) 2016/679 weitgehend übernommen werden. Die Absätze 3 und 4 regeln, anknüpfend an die bisherige Regelung des § 19 Absätze 5 und 6 BDSG-alt, Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Person und weiten diese im Vergleich zur bisherigen Rechtslage deutlich aus.

Absatz 1 gilt sowohl für öffentliche als auch für nicht-öffentliche Stellen, wobei die für die Informationspflicht in § 31 vorgesehene Differenzierung der Ausschlussgründe nach öffentlichen und nicht-öffentlichen Stellen über den Verweis in Nummer 1 auch für das Auskunftsrecht gilt.

Absatz 1 Nummer 1 verweist für das Auskunftsrecht auf die Beschränkungen des § 31 Absätze 1 und 3. Durch den Verweis werden die bislang bestehenden Einschränkungen des Auskunftsrechts der betroffenen Person aus § 19 Absatz 3 und 4 und § 34 Absatz 7 i. V. m. § 33 Absatz 2 Satz 1 Nummer 3, 6 und 7b) BDSG-alt übernommen. Der ebenfalls über § 34 Absatz 7 BDSG-alt erfasste Ausschlussgrund des § 33 Absatz 2 Satz 1 Nummer 7a) BDSG-alt, nach welchem Auskunft nicht zu erteilen ist, wenn die für eigene Zwecke gespeicherten Daten aus allgemein zugänglichen Quellen entnommen sind und wegen der Viezahl der betroffenen Fälle eine Auskunftserteilung unverhältnismäßig ist, wird nicht übernommen. Auch eine Viehlzahl gleichzeitig gestellter Auskunftsansprüche vermag gegenüber der einzelnen betroffenen Person keine Unverhältnismäßigkeit für den Verantwortlichen zu begründen. Die Verordnung (EU) 2016/679 sieht bei einer Häufung geltend gemachter Auskunftsansprüche lediglich die Möglichkeit einer Verlängerung der in Artikel 12 Absatz 3 vorgesehenen Frist zur Beantwortung vor.

Absatz 1 Nummer 2 enthält eine spezifische Ausnahme bei unverhältnismäßigem Aufwand, wenn die Daten nur deshalb gepeichert sind, weil sie aufgrund von von Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder Datenschutzkontrolle dienen. Bei der Ermittlung des Aufwands hat der Verantwortliche die für sie bestehenden technischen Möglichkeiten, gesperrte und archivierte Daten der betroffenen Person im Rahmen der Auskunftserteilung verfügbar zu machen, zu berücksichtigen. In Erweiterung der bisherigen inhaltsgleichen Regelungen des § 19 Absatz 2 und des § 33 Absatz 2 Satz 1 Nummer 2 BDSG-alt hat der Verantwortliche sicherzustellen, dass durch geeignete technische und organisatorische Maßnahmen eine Verwendung der Daten zu anderen Zwe-

cken ausgeschlossen ist. Im Fall der Speicherung ausschließlich aufgrund von Aufbewahrungsvorschriften ist die Verarbeitung der Daten einzuschränken (§ 33 Absatz 3). Die Beschränkung des Auskunftsrechts schützt den Verantwortlichen vor unverhältnismäßiger Inanspruchnahme (Artikel 23 Absatz 1 Buchstabe i der Verordnung 2016/679). Sofern die Speicherung ausschileßlich der Datensicherung oder Datenschutzkontrolle bei öffentlichen Stellen dient, ist zusätzlich Artikel 23 Absatz 1 Buchstabe h der Verordnung 2016/679 einschlägig.

Absatz 1 Nummer 3 schützt den Verantwortlichen vor unverhältnismäßigem Aufwand, wenn sich im Wege der Interessenabwägung feststellen lässt, dass der Aufwand der Recherche außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Die Einschränkung des Auskunftsrechts dient dem Schutz der Rechte und Freiheiten des Verantwortlichen (Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679). Sie entspricht Erwägungsgrund 63 Satz 6 der Verordnung (EU) 2016/679, nach welcher der Verantwortliche verlangen kann, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor der Verantwortliche Auskunft erteilt. Statt einer allgemeinen Regelung, die das Auskunftsrecht der betroffenen Person bei jeglicher Form des unverhältnismäßigen Aufwands für den Verantwortlichen einschränkt, werden wie schon in Nummer 2 spezielle Fallgruppen des BDSG-alt übernommen. Die Regelung ist an § 19 Absatz 1 Satz 3 BDSG-alt angelehnt und wird auf nicht-öffentliche Stellen erweitert. Wie bisher hat es die betroffene Person – im Gegensatz zur Informationspflicht – weitgehend selbst in der Hand, durch die Konkretisierung ihres Auskunftsverlangens, etwa durch Angabe des Aktenzeichens oder den Gegenstand des Auskunftsbegehrens, das Auffinden der Daten durch den Verantwortlichen zu ermöglichen oder zu vereinfachen und hierdurch einen unverhältnismäßig hohen Aufwand des Verantwortlichen zu vermeiden. Im Rahmen der technischen Möglichkeiten wird sich der Aufwand der Auskunft bei (teil-)automatisierter oder dateibasierter Datenverarbeitung in aller Regel nicht als unverhältnismäßig erweisen.

Absatz 2 greift die bisher in § 34 Absatz 1 Satz 4 BDSG-alt enthaltene Regelung zum Schutz der Wahrung von Betriebs- und Geschäftsgeheimnissen des Verantwortlichen auf. Die Regelung beruht auf Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679 und schränkt den Auskunftsanspruch der betroffenen Person hinsichtlich der Herkunft der Daten und der Empfänger ein (Artikel 23 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679).

Absatz 3 ist an § 19 Absatz 5 BDSG-alt angelehnt und erweitert diesen auf nicht-öffentliche Stellen. Satz 1 bestimmt, dass die Gründe der Auskunftsverweigerung zu dokumentieren sind. Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen. Dies gilt abweichend von Artikel 12 Absatz 4 in Verbindung mit Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 jedoch nicht, soweit durch die Mitteilung der Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

Die Dokumentationspflicht und die Begründungspflicht 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. Nach Artikel 12 Absatz 4 der Verordnung (EU) 2016/679 hat der Verantwortliche die betroffene Person zudem auf die Möglichkeit der Beschwerde bei der zuständigen Aufsichtsbehörde und des gerichtlichen Rechtsschutzes hinzuweisen (bislang § 19 Absatz 5 Satz 2 BDSG-alt). Satz 3 enthält die bisher in § 34 Absatz 5 BDSG-alt enthaltene strenge Zweckbindung der zum Zweck der Auskunftserteilung an die betroffene Person und zu deren Vorbereitung gespeicherten Daten.

Absatz 4 entspricht § 19 Absatz 6 BDSG-alt. Unterbleibt eine Auskunftserteilung an die betroffene Person, ist die Auskunft auf Verlangen der oder dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die zuständige oberste Bundesbehörde im Einzelfall

feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Beschränkung dient dem Schutz der öffentlichen Sicherheit (Artikel 23 Absatz 1 Buchstabe c) und der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten (Artikel 23 Absatz 1 Buchstabe d).

Zu § 33 (Recht auf Löschung)

§ 33 schränkt das Recht der betroffenen Person auf Löschung und die damit korrespondierende Pflicht des Verantwortlichen aus Artikel 17 Absatz 1 sowie die Pflicht des Verantwortlichen zur Speicherbegrenzung aus Artikel 5 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 dahingehend ein, dass unter den abschließend genannten Voraussetzungen der Absätze 1 bis 3 an die Stelle der Löschung die Einschränkung der Verarbeitung („Sperrung“) tritt. Die in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten weiteren Ausnahmen bleiben hiervon unberührt. Die Regelung gilt sowohl für öffentliche als auch für nichtöffenltiche Stellen. Die bisherige Rechtslage (§§ 20 Absatz 3, 35 Absatz 3 BDSG-alt) wird im Rahmen des Artikel 23 der Verordnung (EU) 2016/679 fortgeführt.

Durch die Rechtsfolge der Einschränkung der Verarbeitung (Artikel 18 der Verordnung (EU) 2016/679) 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 finden Anwendung und vermitteln effektive Garantien gegen Missbrauch und unrichtige Übermittlung im Sinne des Artikel 23 Absatz 2 Buchstabe d der Verordnung (EU) 2016/679.

Nach Absatz 1 tritt an die Löschung die Einschränkung der Verarbeitung, wenn und soweit aufgrund der besonderen Art der Verarbeitung die Löschung unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde. Die Ausnahme von Artikel 17 der Verordnung (EU) 2016/679 entspricht der bisherigen Regelung des § 20 Absatz 3 Nummer 3 und § 35 Absatz 3 Nummer 3 BDSG-alt. Die Regelung erfolgt zum Schutz der Rechte und Freiheiten des Verantwortlichen gemäß Artikels 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679. Dem Verantwortlichen kann nichts Unmögliches oder Unverhältnismäßiges abverlangt werden. Der vertretbare Aufwand für den Verantwortlichen bemisst sich nach dem jeweiligen Stand der Technik und erfasst insbesondere nicht veränderbare oder löschbare Datenspeicher.

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-alt. 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 korrespondierende Regelung in 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 auch ohne Verlangen der betroffenen Person nach Artikel 17 der Verordnung (EU) 2016/679 verpflichtet ist, nicht mehr erforderliche oder unrechtmäßig verarbeitete Daten auf eigene Initiative zu löschen.

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

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 entgegen stehen. Die Regelung korrespondiert mit der Einschränkung der Auskunftspflicht des Verantwortlichen gemäß § 33 Absatz 1 Nummer 2. Die dort und auch in § 20 Absatz 3 Nummer 1 und § 35 Absatz 3 Nummer 1 BDSG-alt vorgesehene ergäneznde Einschränkung der gesetzlichen Aufbewahrungsfrist ist in § 34 über die sich unmittelbar aus der Verordnung (EU) 2016/679 ergebende Ausnahme des Artikel 17 Absatz 3 Buchstabe b – Erfüllung einer rechtlichen Verpflichtung nach dem Recht der Union oder der Mitgliedstaaten – erfasst. Die Ausnahme beruht ebenfalls auf Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679 und schützt den Verantwortlichen vor einer Pflichtenkollision. Durch die Einschränkung der Verarbeitung der Konflikt zwischen satzungsmäßigen oder vertraglichen Aufbewahrungsfristen, denen der Verantwortliche unterliegt, und dem Verlangen der betroffenen Person nach Löschung der Daten im Wege eines schonenden Ausgleichs der widerstreitenden Rechte und Interessen gelöst.

Zu § 34 (Widerspruchsrecht)

§ 34 schränkt das Recht auf Widerspruch nach Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 ein, wenn die Verarbeitung zu einem der in § 22 Absatz 1 genannten Zwecke erforderlich ist und der Widerspruch die Verwirklichung des Zwecks der Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen würde. Durch die Bezugnahme auf die Verarbeitungszwecke des § 22 Absatz 1 wird sichergestellt, dass ein Widerspruch gegen die Verarbeitung personenbezogener Daten nur unter den Bedingungen ausgeschlossen ist, unter denen der Verantwortliche die von der Verordnung (EU) 2016/679 besonders geschützten „besonderen Kategorien personenbezogener Daten“ im Sinne des Artikel 9 Absatz 1 der Verordnung verarbeiten dürfte. § 34 setzt jedoch nicht voraus, dass sich der Widerspruch auf die Verarbeitung besonderer Kategorien personenbezogener Daten bezieht, sondern lediglich, dass eine Verarbeitung personenbezogener Daten auf der Grundlage der hohen Anforderungen des § 22 Absatz 1 zulässig wäre.

Durch die Anknüpfung an die in § 22 Absatz 1 genannten Ziele wird sichergestellt, dass ein Widerspruchsrecht nur bei Vorliegen besonders wichtiger öffentlicher Interessen ausgeschlossen sein soll. Unterliegt der Verantwortliche aufgrund des Unionsrechts oder einer anderweitigen Rechtsvorschrift einer rechtlichen Verpflichtung zur Verarbeitung personenbezogener Daten (Artikel 6 Absatz 1 Buchstabe c in Verbindung mit Artikel 6 Absatz 3 der Verordnung (EU) 2016/679), steht der betroffenen Person bereits nach dem Anwendungsbereich des Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 kein Widerspruchsrecht zu. Dies entspricht der geltenden Rechtslage nach § 20 Absatz 5 Satz 2 und § 35 Absatz 5 Satz 2 BDSG-alt). Das gilt auch dann, wenn die Rechtsgrundlage der Verarbeitung sowohl auf Art. 6 Absatz 1 Buchstabe c als auch Buchstabe e gestützt ist. Die Einschränkung des Rechts auf Widerspruch folgt aus Artikel 23 Absatz 1 Buchstabe b, d und e der Verordnung (EU) 2016/679.

Satz 2 enthält Maßnahmen zum Schutz der Rechte und Freiheiten sowie der schutzwürdigen Interessen der betroffenen Personen. Die Daten unterliegen einer strengen Bindung in Bezug auf die in § 22 Absatz 1 genannten Verarbeitungszwecke; für andere Zwecke dürfen die Daten nur verarbeitet werden, soweit zugunsten des Verantwortlichen Artikel 23 Absatz 1

Satz 2 der Verordnung (EU) 2016/679 (zwingende schutzwürdige Gründe oder die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen) greift.

Zu § 35 (Automatisierte Einzelentscheidungen im Einzelfall einschließlich Profiling)

§ 35 Satz 1 erlaubt eine automatisierte Einzelentscheidung über die in Artikel 22 Absatz 2 Buchstaben a und c der Verordnung (EU) 2016/679 genannten Fälle hinaus, wenn die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren der betroffenen Person stattgegeben wird. Die Regelung ergänzt Artikel 22 Absatz 2 Buchstabe a um die in § 6a Absatz 2 Nummer 1 BDSG-alt vorgesehene Alternative des „sonstigen Rechtsverhältnisses“. Rechtsgrundlage für die Regelung ist Artikel 22 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679. Im Gegensatz zu der von Artikel 22 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 erfassten Ausnahme setzt die Regelung weder ein Vertrags- oder sonstiges Rechtsverhältnis zwischen der betroffen Person und dem Verantwortlichen voraus noch die (zwingende) Erforderlichkeit der automatisierten Einzelfallentscheidung für den Abschluss oder die Erfüllung des Vertrags. Die Regelung ist notwendig, um insbesondere Konstellationen zu erfassen, in denen weder ein Vertrags- noch ein sonstiges Rechtsverhältnis zwischen dem Verantwortlichen und der betroffenen Person besteht. Dies trifft beispielsweise im Versicherungsbereich für die Schadensregulierung in der Haftpflichtversicherung zu, bei der kein rechtsgeschäftliches Verhältnis zwischen dem Versicherungsunternehmen des Schädigers und dem Geschädigten besteht.

Den Rechten und Freiheiten sowie den berechtigten Interessen der betroffenen Person wird dadurch Rechnung getragen, dass eine automatisierte Entscheidung im Einzelfall nur zulässig ist, wenn dem Begehren der betroffenen Person stattgegeben wurde. Ist dies nicht der Fall, hat der Verantwortliche nach Satz 2 die in Artikel 22 Absatz 3 der Verordnung (EU) 2016/679 vorgesehenen Maßnahmen zu treffen, wozu mindestens das Recht auf Erwirkung des Eingreifens einer natürlichen Person durch den Verantwortlichen, auf Darlegung des eigenen Standpunkts der betroffenen Person und auf Anfechtung der Entscheidung gehört. Zudem finden die Informationspflichten des Artikel 13 Absatz 2 Buchstabe f bzw. 14 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679, welche für Ausnahmen nach Artikel 22 Absatz 2 nur im Fall des Absatzes 4 (zulässige Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 Buchstabe a oder g der Verordnung (EU) 2016/679) gilt, Anwendung.

Zu § 36 (Datenschutzbeauftragte nicht-öffentlicher Stellen)

§ 36 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 nicht-öffentlichen 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-alt angelehnt. Danach haben nicht-öffentliche 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-alt.

Absatz 2 verweist für die betrieblichen Datenschutzbeauftragten, sofern aufgrund der Verordnung (EU) 2016/679 oder Absatz 1 eine Pflicht zur Benennung besteht, auf den besonde-

ren Kündigungsschutz des § 5 Absatz 6. Die in § 6 Absatz 4 Satz 2 und Absatz 5 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 § 37 (Akkreditierung)

Gemäß Artikel 43 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 stellen die Mitgliedstaaten sicher, dass die für die Zertifizierung von Verantwortlichen oder Auftragsverarbeitern zuständigen Zertifizierungsstellen durch die Aufsichtsbehörden und/oder die gemäß Verordnung (EG) Nr. 765/2008 benannten nationalen Akkreditierungsstellen akkreditiert werden. Artikel 58 Absatz 3 Buchstabe e der Verordnung (EU) 2016/679 weist den Aufsichtsbehörden die Befugnis zur Akkreditierung der Zertifizierungsstellen gemäß Artikel 43 der Verordnung mit unmittelbarer Geltung zu. Die Vorschrift sieht in Ausübung des durch Artikel 43 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 eröffneten mitgliedstaatlichen Gestaltungsspielraums alternativ die Deutsche Akkreditierungsstelle (DAkkS) als Akkreditierungsstelle vor, welche die in der Bundesrepublik gemäß der Verordnung (EG) Nr. 765/2008 benannte nationale Akkreditierungsstelle ist. Dies ist sachgerecht, weil die DAkkS über hohe Kompetenz und Erfahrung bei der Akkreditierung verfügt. Die Zertifizierungsstellen erhalten hierdurch ein Wahlrecht, die Akkreditierung entweder bei der zuständigen Aufsichtsbehörde oder bei der DAkkS vornehmen zu lassen.

Satz 2 stellt sicher, dass die Aufsichtsbehörden und die Deutsche Akkreditierungsstelle sich gegenseitig über die Erteilung, Versagung oder den Widerruf einer Akkreditierung einschließlich der tragenden Gründe informieren.

Zu § 38 (Aufsichtsbehörden der Länder)

§ 38 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 nicht-öffentlichen Stellen. Die Regelung orientiert sich weitgehend an der bisherigen Regelung des § 38 BDSG-alt. Die Regelungen zur Amtshilfe (§ 38 Absatz 1 Satz 5 BDSG-alt), zum Beschwerderecht (§ 38 Absatz 1 Satz 8 erste Alternative BDSG-alt), zur Registerführung meldepflichtiger Datenverarbeitungen (§ 38 Absatz 2), zum Einsichtsrecht geschäftlicher Unterlagen (§ 38 Absatz 4 Satz 2 BDSG-alt) und zu den Anordnungs- und Beseitigungsverfügungen (§ 38 Absatz 5 Satz 1 und 2 BDSG-alt) 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-alt) nicht übernommen.

Für die Zugangs- und Betretensrechte von Wohnungen gilt § 16 Absatz 5 unter den einschränkenden Maßgaben des Artikels 13 GG. Demnach muss entweder das Einverständnis des Verantwortlichen oder Auftragsverarbeiters vorliegen oder eine richterliche Anordnung bestehen und das Betreten der Grundstücke und Diensträume zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen, zur Verhütung der durch Datenschutzverstöße begründeten dringenden Gefahren für die öffentliche Sicherheit erforderlich sein.

Zu § 39 (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 § 39 Abs. 1 das Gesetz über Ordnungswidrigkeiten grundsätzlich auch auf Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679.

§ 39 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 §§ 9, 17, 30, 35, 36 und 130 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung. Die Anwendung der §§ 9, 30 und 130 des Gesetzes über Ordnungswidrigkeiten ist ausgeschlossen, da die Verordnung (EU) 2016/679 hinsichtlich der Frage der Zurechnung von Handlungen abschließend ist. § 17 des Gesetzes über Ordnungswidrigkeiten kommt nicht zur Anwendung, da die Verordnung (EU) 2016/679 auch 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 Straf- und Bußgeldverfahren 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. § 39 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.

In Absatz 2 Satz 3 ist ob der hohen Bußgeldbeträge, die die Verordnung (EU) 2016/679 ermöglicht, in Anlehnung an § 23 Nummer 1 des Gerichtsverfassungsgesetzes die Zuständigkeit des Landgerichts vorgesehen, wenn der Betrag einer Geldbuße die Summe von fünftausend Euro übersteigt.

Absatz 2 Satz 4 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 § 40 (Weitere Vorschriften für die Verhängung von Geldbußen)

Absatz 1 greift die bisher geltende Rechtslage auf, nach der Geldbußen auch gegenüber Mitarbeitern öffentlicher oder nicht-öffentlicher Stellen möglich waren. Die Öffnungsklausel hierfür bietet Artikel 84 Absatz 1 der Verordnung (EU) 2016/679: Danach legen die Mitgliedstaaten „insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 unterliegen“, Vorschriften über Sanktionen fest. Verstöße durch Mitarbeiter unterliegen keiner Geldbuße gemäß Artikel 83, da dieser nur Verantwortliche und Auftragsverarbeiter adressiert. Für Dritte, die in Ausübung ihrer Tätigkeit für den Verantwortlichen oder Auftragsverarbeiter eine datenschutzrechtliche Ordnungswidrigkeit begehen, werden § 8 und §§ 10 bis 16 des Geset-

zes über Ordnungswidrigkeiten für anwendbar erklärt, da die dort festgelegten Grundlagen der Ahndung auch weiterhin Bestand haben sollen. Die mögliche Bußgeldhöhe wird in Absatz 1 Satz 2 entsprechend § 43 Absatz 1 Satz 3 a.E. BDSG-alt auf bis zu dreihunderttausend EUR beschränkt.

Absatz 2 gibt die Bußgeldtatbestände des § 43 Absatz 1 Nr. 7a und b BDSG-alt wieder; mit diesen Tatbeständen war Artikel 9 der Verbraucherkreditrichtlinie 2008/48/EG umgesetzt worden.

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. Mit Satz 2 soll sichergestellt werden, dass öffentliche Stellen, die im Rahmen ihrer Tätigkeit im Wettbewerb mit anderen Verarbeitern stehen, 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-alt 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 § 41 (Strafbare Handlungen)

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 § 41 Gebrauch.
Der Verweis auf die Bußgeldtatbestände in Artikel 83 Absatz 5 der Verordnung (EU) 2016/679 entspricht der bisherigen Regelungssystematik des BDSG-alt, dessen § 44 Absatz 1 auf die in § 43 Absatz 2 BDSG-alt geregelten Handlungen verwies: Artikel 83 Absatz 5 der Verordnung (EU) 2016/679 enthält gegenüber Absatz 4 die schwerwiegenderen Bußgeldtatbestände der Verordnung.

Zu § 42 (Strafantrag und Verwendung von Meldungen)

Absatz 1 entspricht § 45 Absatz 2 BDSG-alt. Absatz 2 dient dem verfassungsrechtlichen Verbot einer Selbstbezichtigung und ist § 42a Satz 6 BDSG-alt 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 (Anwendungsbereich)

Der 3. Teil dient im Wesentlichen der Umsetzung der Richtlinie (EU) 2016/680. § 43 regelt den Anwendungsbereich des 3. Teils. Er gilt nur für Verarbeitungen durch öffentliche Stellen des Bundes und, vgl. Artikel 3 Absatz 7 Buchstabe b Richtlinie (EU) 2016/680 und § 2 Absatz 1 Nummer 3, 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 3. Teils und damit auch der Richtlinie (EU) 2016/680 genügt also eine Verarbeitung zu den o. g. Zwecken allein nicht; daneben muss

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

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 Bundesbehörden, 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.

zu § 44 (Verarbeitung personenbezogener Daten)

§ 44 trifft grundsätzliche Aussagen zur Zulässigkeit der Verarbeitung personenbezogener Daten im Kontext des Teils 3.

Absatz 1 setzt Artikel 8 Absatz 1 Richtlinie (EU) 2016/680 um und schafft in Satz 1 gleichzeitig eine eigene Rechtsgrundlage für die Verarbeitung; danach ist die Verarbeitung zulässig, wenn diese für die Aufgabenerfüllung zu den in § 43 genannten Zwecken erforderlich ist. Ferner wird in Satz 2 Artikel 8 Absatz 2 der Richtlinie (EU) 2016/680 umgesetzt, indem für im bereichsspezifischen Recht vorhandene Rechtsgrundlagen inhaltliche Mindestanforderungen formuliert werden. Dies schließt spezielle Rechtsgrundlagen in den jeweiligen Fachgesetzen nicht aus.

Absatz 2 greift Artikel 4 Absatz 3 Richtlinie (EU) 2016/680 auf, wonach Verantwortliche Daten auch zu wissenschaftlichen, statistischen und historischen Zwecken verarbeiten dürfen, solange diese Verarbeitung unter die in § 43 genannten Zwecke gefasst werden kann. Voraussetzung hierfür ist das Vorliegen geeigneter Vorkehrungen zugunsten der Rechtsgüter der betroffenen Person; hierzu können insbesondere die frühestmögliche Anonymisierung von Daten oder die räumliche und organisatorische Abtrennung der Forschung betreibenden Stellen gehören. Als Beispiel kann hier die im Bundeskriminalamt durchgeführte kriminologische oder kriminaltechnische Forschung angeführt werden.

Absatz 3 wiederum setzt Artikel 9 Absatz 3 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 4 erklärt eine Verarbeitung auch im Kontext der in § 43 genannten Zwecke für zulässig, wenn der Betroffene hierzu eingewilligt hat und verweist auf die Voraussetzungen einer Einwilligung auf § 47. Hiermit werden die bisherige Rechtslage, vgl. § 4 Absatz 1 am Ende BDSG-alt, § 4a BDSG-alt, fortgeführt. Auch die Richtlinie (EU) 2016/680 erkennt die Möglichkeit der Verarbeitung auf Grundlage einer Einwilligung grundsätzlich an, wie aus Erwägungsgrund 35 hervorgeht. Absatz 1, der die Zulässigkeit der Verarbeitung grundsätzlich unter die Voraussetzung der Erforderlichkeit für die Aufgabenerfüllung stellt, bleibt auch bei einer Verarbeitung aufgrund einer Einwilligung anwendbar.

zu § 45 (Verarbeitung besonderer personenbezogener Daten)

§ 45 dient der Umsetzung von Artikel 10 Richtlinie (EU) 2016/680. Absatz 1 legt fest, unter welchen Voraussetzungen die Verarbeitung besonderer personenbezogener Daten - die in Absatz 2 legaldefiniert werden - zulässig ist. Über Artikel 10 hinausgehend ist die Verarbeitung auch bei Vorliegen einer wirksamen Einwilligung zulässig. Damit wird zum einen die Regelung aus § 44 Absatz 4 konsequent fortgeführt. Zum anderen entspricht die Regelung der bisherigen Rechtslage nach § 13 Absatz 2 Nummer 2 BDSG-alt. Für diese Fälle statuiert § 7 Absatz 7 - wie § 4a Absatz 3 BDSG-alt - besondere Anforderungen an die Einwilligung.

Zu § 46 (Zweckbindung und Zweckänderung)

Absatz 1 setzt Artikel 4 Absatz 2 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 § 43 genannten Zwecke handelt und diese Verarbeitung erforderlich und verhältnismäßig ist. Grundsätzlich eröffnet Artikel 4 Absatz 2 Richtlinie (EU) 2016/680 stets die Möglichkeit, die Daten für einen der in § 43 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 § 43 genannten Zwecke aufgrund nationalen Verfassungsrechts (so etwa der Grundsatz der hypothetischen Datenneuerhebung, vgl. BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 - 1 BvR 1140/06) werden in den Fachgesetzen umgesetzt. In Absatz 1 Nummer 3 wird der in § 14 Absatz 3 BDSG-alt enthaltene Gedanken aufgenommen und klargestellt, dass der Verantwortliche zu den dort genannten Zwecken zulässigerweise zweckändernd verarbeiten darf.

Absatz 2 setzt Artikel 9 Absatz 1 Richtlinie (EU) 2016/680 um und stellt insofern klar, dass sich die Zulässigkeit der Verarbeitung zu anderen, außerhalb der in § 43 genannten, Zwecken nach § 23 richtet.

Zu § 47 (Einwilligung)

In § 47 finden sich die Voraussetzungen für eine wirksame Einwilligung. Hierbei wurden Elemente aus Artikel 7 Verordnung (EU) 2016/679 mit dort nicht enthaltenen Elementen des § 4a BDSG-alt kombiniert.

Absatz 1 entspricht Artikel 7 Absatz 1, Absatz 2 Artikel 7 Absatz 2 und Absatz 3 Artikel 7 Absatz 3 Verordnung (EU) 2016/679. In Absatz 4 wurde der Ansatz aus § 4a Absatz 1 BDSG-alt mit dem Gedanken aus Artikel 7 Absatz 4 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-alt.

Zu § 48 (Verarbeitung unter Weisung des Verantwortlichen oder Auftragsverarbeiters)

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

Zu § 49 (Datengeheimnis)

§ 49 greift die Regelung des § 5 BDSG-alt auf.

Zu § 50 (Automatisierte Einzelentscheidung)

§ 50 setzt Artikel 11 Richtlinie (EU) 2016/680 um und regelt das Verbot automatisierter Einzelentscheidungen. Die Regelung nimmt Elemente aus § 6a Absatz 1 am Ende BDSG-alt auf. 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. Verantwortlicheninterne Zwischenfestlegungen oder -auswertungen, die Ausfluss automatisierter Prozesse sind, fallen nicht hierunter.

Zu § 51 (Auskunftsrecht)

§ 51 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 § 67 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 3 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-alt in das BDSG-neu und sorgt darüber hinaus für einen Gleichlauf mit § 32 Absatz 1 Nummer 2.

Absatz 3 überführt die Regelung des § 19 Absatz 1 Satz 3 BDSG-alt in das BDSG-neu und sorgt darüber hinaus für einen Gleichlauf mit § 32 Absatz 1 Nummer 3.

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. Satz 2 nimmt § 19 Absatz 3 BDSG-alt auf.

Absatz 5 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-alt entnommenen Gedanken auf.

Absatz 6 thematisiert die Möglichkeiten, die der betroffenen Person im Falle des Absehens von einer Begründung für die vollständige oder teilweise Einschränkung des Auskunftsrechts oder im Falle der überhaupt ausbleibenden Beantwortung des Auskunftsverlangens bleiben. Nach Satz 1 kann die betroffene Person ihr Auskunftsrecht nach Auskunftsverweigerung durch den Verantwortlichen über die Bundesbeauftragte 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-alt und nun auch in § 55 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 voraus, die allerdings nicht auf Fälle Anwendung findet, in denen der Verantwortliche nach Absatz 5 berechtigt ist, von einer Information des Antragstellers ganz abzusehen. Satz 3 nimmt § 19 Absatz 6 Satz 1 BDSG-alt auf. Sätze 4 und 5 betreffen den Inhalt der der betroffenen Person seitens der oder dem Bundesbeauftragten oder den 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 nimmt § 19 Absatz 6 Satz 1 BDSG-alt auf. Satz 7 setzt Artikel 17 Absatz 3 Satz 2 der Richtlinie (EU) 2016/680 um.

Absatz 7 setzt Artikel 15 Absatz 4 der Richtlinie (EU) 2016/680 um.

Zu § 52 (Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung)

In § 52 werden die Betroffenenrechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung und deren Ausnahmen zusammengeführt. § 52 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 Erwägungsgrund 47 der Richtlinie (EU) 2016/680 wird klargestellt, 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 2 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. Die in Satz 4 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 § 70 Absatz 1 für Fälle enthalten, in denen der Verantwortliche von sich aus, also unabhängig von der Geltendmachung eines Betroffenenrechts, eine Berichtigung durchführt.

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 Satz 1 betrifft - insofern parallel zu § 70 Absatz 2 Satz 2 - 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-alt (§ 52 Absatz 3 Satz 1 Nummern 1 und 3), ergänzt um Artikel 16 Absatz 3 Satz 1 Buchstabe b (§ 52 Absatz 3 Satz 1 Nummer 2) der Richtlinie (EU) 2016/680 aufgenommen. § 52 Absatz 3 Satz 1 Nummer 1 übernimmt zudem einen in Erwägungsgrund 47 Satz 4 der Richtlinie (EU) 2016/680 enthaltenen Gedanken. Satz 2 nimmt einen in § 32 Absatz 2 Satz 3 BKAG enthaltenen Gedanken auf.

Absatz 4 verweist im Hinblick auf die Benachrichtigung von Stellen, an die Daten übermittelt wurden, über die Berichtigung, Löschung oder Verarbeitungseinschränkung auf § 70 Absatz 4.

Absatz 5 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 § 51 Absatz 5 nachgebildet; folgerichtig wird - so auch in Absatz 6 - weitgehend auf die entsprechenden Vorschriften in § 51 zur vollständigen oder teilweisen Einschränkung des Auskunftsrechts verwiesen.

Zu § 53 (Zweckbindung für Daten über die Ausübung von Betroffenenrechten)

§ 53 überführt § 6 Absatz 3 BDSG-alt in das BDSG-neu.

Zu § 54 (Verfahren für die Ausübung der Betroffenenrechte)

In § 54 werden Elemente des Artikels 12 der Richtlinie (EU) 2016/680 umgesetzt.

Absatz 1 setzt Artikel 12 Absatz 3, Absatz 2 setzt Artikel 12 Absatz 4 und Absatz 3 setzt Artikel 12 Absatz 5 der Richtlinie (EU) 2016/680 um.

Wenngleich es Absatz 5 dem Verantwortlichen in begründeten Zweifelsfällen ermöglicht, zusätzliche Informationen zur Identitätsklärung anzufordern, ist hierdurch keine Änderung der bisherigen verbreiteten Praxis angezeigt, den Nachweis der Identität (etwa durch eine beglaubigte Kopie des Bundespersonalausweises) auch weiterhin als Grundvoraussetzung für die Antragsstellung anzusehen.

Zu § 55 (Anrufung der oder des Bundesbeauftragten)

§ 55 stellt auch für den Bereich der Verarbeitung durch Verantwortliche zu den in § 43 genannten Zwecken klar, dass sich Betroffene mit Beschwerden über die bei Verantwortlichen durchgeführte Verarbeitung an die Bundesbeauftragte oder den Bundesbeauftragten wenden können. Insbesondere mit Absatz 1 dieser Vorschrift werden gleichzeitig Art. 52 der Richtlinie (EU) 2016/680 umgesetzt als auch § 21 BDSG-alt in das BDSG-neu überführt. Absatz 2 setzt Artikel 52 Absatz 2 der Richtlinie (EU) 2016/680 um.

Zu § 56 (Rechtsschutz gegen Anordnungen der oder des Bundesbeauftragten oder bei deren oder dessen Untätigkeit)

§ 56 setzt Artikel 53 der Richtlinie (EU) 2016/680 um und thematisiert, dass Adressaten von Anordnungen der oder des Bundesbeauftragten Rechtsschutz gegen diese suchen können.

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

Auf die Anwendbarkeit von § 20 in Bezug auf das Rechtsschutzverfahren wird in Absatz 1 Satz 2 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 § 57 (Auftragsverarbeitung)

§ 57 dient der Umsetzung von Artikel 22 der Richtlinie (EU) 2016/680 und stellt Anforderungen auf, wenn der Verantwortliche Auftragsdatenverarbeitungsverhältnisse eingehen will. Gleichzeitig werden Elemente des § 11 BDSG-alt in das BDSG-neu 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-alt 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 Unterauftragsdatenverarbeitungsverhältnissen 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 Verordnung (EU) 2016/679 die Überführung von den Auftragsverarbeiter treffenden Pflichten auf einen Unterauftragnehmer thematisiert.

In Absatz 5 wird Artikel 28 Absatz 5 Verordnung (EU) 2016/679 im Hinblick auf Elemente zur Beurteilung der Geeignetheit eines Auftragsverarbeiters übernommen.

In Absatz 6 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 Verordnung (EU) 2016/679 als auch § 11 Absatz 2 und 3 BDSG-alt entnommen; so werden in Satz 2 Nummer 1 Elemente aus Artikel 28 Absatz 3 Buchstabe a Verordnung (EU) 2016/679 und § 11 Absatz 3 Satz 2 BDSG-alt, 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 Verordnung (EU) 2016/679 aufgenommen.

Absatz 7 trifft in Umsetzung von Artikel 22 Absatz 4 der Richtlinie(EU) 2016/680 Aussagen zur Form der Vereinbarung und nimmt bezüglich der Möglichkeit der Auftragserteilung durch die zuständige Fachaufsichtsbehörde § 11 Absatz 2 Satz 3 BDSG-alt auf.

Absatz 8 dient der Umsetzung von Artikel 22 Absatz 5 der Richtlinie (EU) 2016/680.

Absatz 9 entspricht § 11 Absatz 2 Satz 4 und 5 BDSG-alt.

Absatz 10 entspricht § 11 Absatz 5 BDSG-alt.

Zu § 58 (Anforderungen an die Sicherheit der Datenverarbeitung)

§ 58 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. Weiterhin wird der in § 9 Satz 2 BDSG-alt enthaltene Gedanke, 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 Art. 32 Absatz 1 Buchstaben a bis d Verordnung (EU) 2016/679 übernommen.

Absatz 3 nimmt den wesentlichen Inhalt von § 9 BDSG-alt und dem Anhang zu § 9 Satz 1 BDSG-alt auf und überführt ihn in das BDSG-neu. 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-alt enthaltenen Gedanken auf.

Zu § 59 (Meldung von Datensicherheitsvorfällen an die Bundesbeauftragte oder den Bundesbeauftragten)

§ 59 dient der Umsetzung von Artikel 30 der Richtlinie (EU) 2016/680 und legt Umfang und Modalitäten der Meldung von Datensicherheitsvorfällen im Sinne einer „Verletzung des Schutzes personenbezogener Daten“ nach § 2 Absatz 2 Nummer 10 an die Bundesbeauftragte oder den Bundesbeauftragten fest. Ansatzpunkt der Meldung sind, wie sich auch aus der systematischen Stellung der Vorschrift im Bereich Sicherheit der Verarbeitung ergibt, Datensicherheitsvorfälle wie etwa Datenabflüsse. Die Meldepflicht wird mithin nicht durch rechtswidrige Verarbeitungen ausgelöst.

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 der in § 42a Satz 6 BDSG-alt enthaltene Gedanke in das BDSG-neu überführt, wonach die Motivation zur Meldung eines Datensicherheitsvorfalls nicht dadurch verringert werden soll, dass die durch die Meldung verfügbar werdenden Informationen zur Verarbeitung zur Einleitung eines Straf- oder Ordnungswidrigkeitenverfahrens führen können.

Absatz 8 stellt klar, dass die in § 59 enthaltene Meldepflicht an die Bundesbeauftragte oder den Bundesbeauftragten andere Meldepflichten, etwa solchen 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, ausschließt bzw. diesen nicht vorgeht.

Zu § 60 (Benachrichtigung der betroffenen Person bei Datensicherheitsvorfällen)

§ 60 setzt Artikel 31 der Richtlinie(EU) 2016/680 um.

Zu § 61 (Durchführung einer Datenschutzfolgenabschätzung)

§ 61 dient der Umsetzung von Artikel 27 der Richtlinie (EU) 2016/680. Die Datenschutzfolgenabschätzung ist ein zentrales Element der strukturellen Stärkung des Datenschutzes. Die Voraussetzungen zur Durchführung einer Datenschutzfolgenabschätzung 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 Datenschutzfolgenabschätzung 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 Bundesbeauftrag-

ten 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 Datenschutzfolgenabschätzung nur für neue Verarbeitungssysteme oder wesentliche Veränderungen an bestehenden gilt und aus § 62 keine Pflicht erwächst, alle tatbestandlich einschlägigen bestehenden Systeme, die zum Zeitpunkt des Inkrafttretens dieses Gesetzes bei der Verarbeitung eingesetzt werden, neu zu untersuchen.

Absatz 2 nimmt Art. 35 Absatz 1 Nummer 2, Absatz 3 Artikel 35 Absatz 2 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 Verordnung (EU) 2016/679 enthaltenen Punkte. Absatz 5 nimmt Artikel 35 Absatz 11 Verordnung (EU) 2016/679 auf.

Zu § 62 (Anhörung der oder des Bundesbeauftragten)

§ 62 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, die ein erhöhtes Gefährdungspotential für Rechtsgüter der betroffenen Personen in sich bergen. Insofern besteht eine enge inhaltliche Verbindung zum Instrument der Datenschutzfolgenabschätzung (§ 61). Prozedural wird diese Verbindung dadurch hergestellt, dass nach Absatz 1 Nummer 1 eine Anhörung durchzuführen ist, wenn im Ergebnis einer Datenschutzfolgenabschätzung 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 Art. 36 Absatz 3 Verordnung (EU) 2016/679 angeglichen.

Die in Absatz 4 vorgesehene Eilfallregelung in Abweichung von Absatz 3 Satz 1 trägt operativen und (polizei-)fachlichen Erfordernissen 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 § 63 (Verzeichnis von Verarbeitungstätigkeiten)

§ 63 dient der Umsetzung von Artikel 24 der Richtlinie (EU) 2016/680 und verpflichtet den Verantwortlichen zur Führung eines Verzeichnisses über bei ihm durchgeführte Datenverarbeitungen. 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 (§ 62), Einsicht in das Verfahrensverzeichnis (§ 63 Absatz 3) und Zurverfügungstellung von Protokolldaten (§ 71 Absatz 2 Satz 1) 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 Kon-

trolltätigkeit 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.

In Absatz 1 werden die in das Verzeichnis aufzunehmenden Angaben benannt. Die Begrifflichkeit „Kategorien von Datenverarbeitungen“ stellt hierbei klar, dass sich das Verzeichnis nicht auf einzelne Datenverarbeitungsvorgänge, sondern auf sinnvoll abgrenz- und kategorisierbare Teile der beim Verantwortlichen durchgeführten Datenverarbeitungen bezieht.

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 sowie dazu getroffen, dass das Verzeichnis und seine Aktualisierungen der oder dem Bundesbeauftragten auf Anfrage zur Verfügung zu stellen ist.

Zu § 64 (Gemeinsam Verantwortliche)

§ 64 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-alt übernommen.

Zu § 65 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen)

Durch § 65 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. Zur Konkretisierung und Handhabbarmachung der Vorgaben wurden in Absatz 1 Elemente des § 3a BDSG-alt aufgenommen.

Zu § 66 (Allgemeine Informationen zu Datenverarbeitungen)

§ 66 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 § 67 (Benachrichtigung betroffener Personen)

§ 67 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 BDSG-neu 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 bereitgestellt 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. Satz 2 statuiert ein § 19 Absatz 3 BDSG-alt 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 § 68 (Unterscheidung verschiedener Kategorien betroffener Personen; Unterscheidung zwischen Tatsachen und Bewertungen)

§ 68 dient bei Absatz 1 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 § 69 (Qualitätssicherung personenbezogener Daten vor deren Übermittlung)

§ 69 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 § 69 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.

Zu § 70 (Berichtigung und Löschung personenbezogener Daten sowie die Einschränkung der Verarbeitung)

§ 70 dient der Umsetzung von Artikel 16 der Richtlinie(EU) 2016/680 in seiner Ausformung als Verantwortlichenpflicht. Systematisch werden in § 70 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 §§ 51 und 52.

In Absatz 1 wird neben der Verantwortlichenpflicht zur Berichtigung Artikel 16 Absatz 5 der Richtlinie (EU) 2016/680 umgesetzt.

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

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 § 52 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 2016/680.

Zu § 71 (Protokollierung)

§ 71 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.

In Absatz 2 wird festgelegt, dass die Protokolle dem Datenschutzbeauftragten und der oder dem Bundesbeauftragten zum Zwecke der Datenschutzkontrolle zur Verfügung stehen müssen. Zudem wird 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.

Zu § 72 (Vertrauliche Meldung von Verstößen)

§ 72 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 § 73 (Allgemeine Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten und internationalen Organisationen)

§ 73 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. In Absatz 1 werden Artikel 35 Absatz 1 Buchstaben a, b und d der Richtlinie(EU) 2016/680 umgesetzt. Absatz 2 dient der Umsetzung von Artikel 35 Absatz 1 Buchstabe c und Absatz 2 der Richtlinie(EU) 2016/680. In Absatz 3 wird Artikel 35 Absatz 1 Buchstabe e der Richtlinie(EU) 2016/680 umgesetzt. Absatz 4 ordnet die entsprechende Geltung von § 45 Absatz 3 an, weil ausweislich Erwägungsgrund 36 der dort in Bezug genommene Artikel 9 Absatz 3 der Richtlinie(EU) 2016/680 auch für Übermittlungen nach Kapitel 4 gilt.

Zusätzliche Anforderungen an die Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen - auch an die insbesondere nach den §§ 74 bis 76 erforderliche Abwägungsentscheidung - aufgrund nationalen Verfassungsrechts (so etwa in BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 - 1 BvR 1140/06) werden in den Fachgesetzen umgesetzt.

Zu § 74 (Datenübermittlung ohne Angemessenheitsbeschluss und mit geeigneten Garantien)

§ 74 dient der Umsetzung von Artikel 37 der Richtlinie(EU) 2016/680. In § 74 werden 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 § 74 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.

Absatz 2 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 § 75 (Datenübermittlung ohne Angemessenheitsbeschluss und ohne geeignete Garantien)

§ 75 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 § 76 erwähnten Garantien in Form eines rechtsverbindlichen Instruments oder nach Beurteilung durch den übermittelnden Verantwortlichen bestehen.

Zu § 76 (Übermittlung an nicht für Zwecke der Richtlinie (EU) 2016/680 zuständige und nicht-öffentliche Stellen in Drittstaaten)

§ 76 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 § 76 Absatz 1 genannten strengen Voraussetzungen. Absatz 2 dient der Umsetzung von Artikel 39 Absatz 3 der Richtlinie (EU) 2016/680, der die Unterrichtung der oder des Bundesbeauftragten über Übermittlungen gemäß § 76 vorsieht. Im Gegensatz zur Pflicht zur Unterrichtung der oder des Bundesbeauftragten aus § 74 Absatz 2 bezieht sich die Pflicht in § 76 auf jede Übermittlung; die Unterrichtung sollte im Unterschied zu § 74 auch in engem zeitlichem Zusammenhang zur Übermittlung erfolgen.

Zu § 77 (Gegenseitige Amtshilfe)

§ 77 dient der Umsetzung des Artikels 50 der Richtlinie (EU) 2016/680.

Zu § 78 (Schadenersatz)

Mit dieser Vorschrift wird die bisher im BDSG-alt (§§ 7 und 8) enthaltene und auf die Verarbeitung bei öffentlichen Stellen anwendbare Systematik der Vorschriften zum Schadensersatz in das BDSG-neu überführt. Gleichzeitig dient die Vorschrift der Umsetzung von Artikel 56 der Richtlinie (EU) 2016/680. Lediglich die noch in § 8 Absatz 3 BDSG-alt enthaltene Deckelung der Ersatzbeträge entfällt.

Zu § 79 (Bußgeld- und Strafvorschriften)

Die Vorschrift setzt Artikel 57 der Richtlinie (EU) 2016/680 um. Durch § 79 wird keine dem deutschen Recht grundsätzlich fremde Strafbarkeit juristischer Personen des öffentlichen Rechts oder die Möglichkeit, diese mit Bußgeldern zu belegen, eingeführt.

In Absatz 1 werden die bisher auf den öffentlichen Bereich anwendbaren bußgeldbewehrten Tatbestände aus § 43 BDSG-alt übernommen, im Einzelnen: § 43 Absatz 1 Nummer 2 BDSG-alt (Absatz 1 Nummer 1); § 43 Absatz 1 Nummer 2b BDSG-alt (Absatz 1 Nummer 2); § 43 Absatz 2 Nummer 1 BDSG-alt (Absatz 1 Nummer 3); § 43 Absatz 2 Nummer 2 BDSG-alt (Absatz 1 Nummer 4); § 43 Absatz 2 Nummer 3 BDSG-alt (Absatz 1 Nummer 5); § 43 Absatz 2 Nummer 4 BDSG-alt (Absatz 1 Nummer 6); § 43 Absatz 2 Nummer 5 BDSG-alt (Absatz 1 Nummer 7).

Absatz 2 übernimmt im Hinblick auf die Bußgeldhöhe § 43 Absatz 3 BDSG-alt.

Absatz 3 ordnet unter Nutzung der durch § 36 Absatz 1 Satz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten eröffneten Möglichkeit für alle Tatbestände außer Absatz 1 Nummer 7 die Zuständigkeit für die Ahndung und Verfolgung der Ordnungswidrigkeiten dem Verantwortlichen zu, um das ansonsten fachlich zuständige Bundesministerium von dieser Aufgabe zu entlasten.

Absatz 4 überführt im Hinblick auf die datenschutzrechtlichen Strafvorschriften § 44 Absätze 1 und 2 BDSG-alt in das BDSG-neu.

Zu Artikel 2 (Änderung des Bundesverfassungsschutzgesetzes)

Zu Nummer 1

Zu Buchstabe a

Die Änderungen sind überwiegend Folgeänderungen der neuen Begriffsdefinitionen in § 2 Absatz 2 Nummern 2 und 3 des BDSG-neu (Artikel 1) zum Umgang mit personenbezogenen Daten. Inhaltlich bedeutsam sind folgende Änderungen:

Zu Buchstabe b

Es handelt sich um eine Folgeregelung zum neuen § 27 Absatz 1 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-alt geregelt war und nunmehr in Artikel 6 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 niedergelegt ist. Die Einzelheiten der Einwilligung sind in § 47 BDSG-neu geregelt, der über § 27 Absatz 1 Nummer 2 entsprechende Anwendung findet (ohne § 47 Absatz 5 BDSG-neu, der bereichsspezifisch nicht passt, weil der Umgang mit solchen Daten für das BfV geradezu aufgabentypisch ist).

Zu Nummer 3 bis 5

Die Änderungen sind Folgeänderungen der neuen Begriffsdefinitionen in § 2 Absatz 2 Nummern 2 und 3 des BDSG-neu (Artikel 1) zum Umgang mit personenbezogenen Daten.

Zu Nummer 6

Die Ergänzung greift die Regelung des § 63 BDSG-neu bereichsspezifisch im Bundesverfassungsschutzgesetz auf.

Zu Nummer 7

Zu Buchstabe a

Die Änderung ist eine Folgeänderung der neuen Begriffsdefinitionen in § 2 Absatz 2 Nummern 2 und 3 des BDSG-neu (Artikel 1) zum Umgang mit personenbezogenen Daten.

Zu Buchstabe b

Es handelt sich um eine Folgeänderung zum neuen § 27 Absatz 1 Nummer 2.

Zu Nummer 8

Es handelt sich um Folgeänderungen der neuen §§ 26a, 27 Absatz 1 Nummer 2.

Zu Nummer 9

Die Änderung ist eine Folgeänderung der neuen Begriffsdefinitionen in § 2 Absatz 2 Nummern 2 und 3 des BDSG-neu (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-alt, 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 4 BDSG-alt jedoch nicht vor Kenntnisnahme durch den Bundesbeauftragten bzw. 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 Art. 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 bzw. 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 bzw. der BfDI eine diesbetreffende Querschnittsprüfung durchführt, kann sie bzw. 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.

Zu Nummer 11

Es handelt sich um eine Folgeregelung zur Neufassung des BDSG.

Die Differenzierung des Absatzes 1 in zwei Nummern folgt dem Regelungssystem des neugefassten BDSG. Dessen Teil 1 gilt ohne Beschränkung auf den Anwendungsbereich von Gemeinschaftsrecht. In § 27 Absatz 1 Nummer 1 BVerfSchG werden folglich – wie bisher – Anwendungsausschlüsse bestimmt, soweit das Bundesverfassungsschutzgesetz bereichsspezifische Spezialregelungen trifft, die damit als abschließend im Sinne des § 1 Absatz 2 BDSG-neu klargestellt werden. Dies betrifft § 4 und § 16 Absatz 4 BDSG-neu, 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-neu 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.

Die Teile 2 und 3 des BDSG-neu sind bereits im BDSG-neu 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 Absatz 1 Nummer 2 entsprechend. Entsprechende Anwendung bedeutet, dass nachrichtendienstliche Besonderheiten berücksichtigt werden. Das bedeutet z. B. dass die „entsprechende“ Anwendung der Vorschrift des § 58 dem gesetzlichen Auftrag des BfV gemäß § 3 BVerfSchG Rechnung tragen muss. Danach ist es gerade Aufgabe des BfV (u. a.) personenbezogene Auskünfte, Nachrichten und Unterlagen über Bestrebungen und Tätigkeiten zu sammeln und auszuwerten, weshalb zwangsläufig auch die in § 58 Absatz 1 Satz 1 BDSG-neu angesprochenen „besonderen Kategorien personenbezogener Daten“ i. S. d. § 45 Absatz 2 BDSG-neu einbezogen sind und zulässigerweise verarbeitet werden dürfen. Spezielle Regelungen zur Thematik im Bundesverfassungsschutzgesetz (etwa § 13 Absatz 4 Satz 5 BVerfSchG) sind gemäß § 1 Absatz 2 BDSG-neu vorrangig.

Absatz 2 regelt komplementär zu Absatz 1 die fachneutralen Verwaltungsaufgaben des BfV, wie etwa Personalverwaltung. Auf diese allgemeinen Verwaltungstätigkeiten, die nicht spezifisch durch die Besonderheiten der Fachaufgabe nach § 3 BVerfSchG geprägt sind, soll neben dem BDSG-neu (dessen Anwenbarkeit bereits aus dessen § 1 Absatz 1 folgt) auch die Datenschutzgrundverordnung Anwendung finden, soweit nicht im Bundesverfassungsschutzgesetz - mit § 26a Absatz 4 Satz 3 - spezielle Regelungen getroffen sind.

Zu Artikel 3 (Änderung des MAD-Gesetzes)

….

Zu Artikel 4 (Änderung des BND-Gesetzes)

….

Zu Artikel 5 (Änderung des Sicherheitsüberprüfungsgesetzes)

….

RACK
RECHTSANWÄLTE

PRÄVENTIVE RECHTSBERATUNG SEIT 26 JAHREN!

SOFTWARE MIT INHALTEN AUS EINER HAND!

Die rechtliche Vorsorgeuntersuchung für Unternehmen.

Nutzen Sie unsere gespeicherten **Erfahrungen aus 26 Jahren Complianceberatung.** Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. **Systematisch senken wir den Complianceaufwand durch Standardisierung um 60 %.** Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt. Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 18.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 7.500 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 57.000 vorformulierte Betriebspflichten. **44.000 Unternehmensrisiken sind mit 59.000 Rechtspflichten drei Millionen Mal verlinkt und gespeichert.** Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de

Zu Artikel 6 (Änderung des Artikel 10-Gesetzes)

Die Änderungen sind Folgeänderungen der neuen Begriffsdefinitionen in § 2 Absatz 2 Nummern 2 und 3 des BDSG-neu zum Umgang mit personenbezogenen Daten. 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-alt). Darüberhinaus enthält Absatz 4 spezielle Regelungen für die Übermittlung zu den dort genannten Zwecken. Gemeint ist damit die Weitergabe 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 BfV in § 19 BVerfSchG. Die Befugnis des BfV 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 Betroffeninteressen 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)

Mit der Änderung des Bundesdatenschutzgesetzes 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.

Zu Artikel 8 (Änderung des Bundesstatistikgesetzes)

§ 17a regelt für die Bundesstatistik die Rechte der Betroffenen nach den Artikeln 15 und 16 der Verordnung (EU) Nr. 679/2016. Der besonderen Verarbeitungssituation der Statistik wird in der Verordnung (EU) Nr. 679/2016 teilweise bereits Rechnung getragen, indem zu einigen Betroffenenrechten Spezialregelungen für die Datenverarbeitung zu statistischen Zwecken verankert sind (Art. 14 Absatz 5 Buchstabe b, Artikel 17 Absatz 3 Buchstabe d und Artikel 21 Absatz 6) oder allgemeine Ausnahmebestimmungen auf die Bundesstatistik angewandt werden können (Artikel 18 Absatz 2, Artikel 20 Absatz 3 Satz 2).

Darüber hinaus sieht die Verordnung weitere Möglichkeiten vor, Ausnahmen und Beschränkungen von den Betroffenenrechten entsprechend den fachspezifischen Erfordernissen zu regeln. Dabei kann § 17a bereits auf Artikel 23 Absatz 1 Buchstabe e der Verordnung gestützt werden, der den Mitgliedsaaten Beschränkungen der Betroffenenrechte zum Schutz eines wichtigen öffentlichen Interesses erlaubt.

§ 17a beschränkt nur die in den Artikeln 15 und 16 der Verordnung vorgesehenen Betroffenenrechte. Eine weitergehende Regelung der Rechte aus den Artikeln 18 und 21 der Verordnung ist nicht notwendig, da das öffentliche Interesse, das an der statistischen Aufbereitung von Daten im Rahmen der Bundesstatistik besteht, bereits durch Artikel 18 Absatz 2 sowie Artikel 21 Absatz 6 der Verordnung ausreichend gewahrt wird.

§ 17a stellt zum einen klar, dass die Rechte auf Auskunft und Berichtigung nur bis zum Zeitpunkt der Löschung der Hilfsmerkmale (identifizierende Angaben, wie beispielsweise Name und Anschrift, die ausschließlich der technischen Durchführung von Bundesstatistiken dienen) geltend gemacht werden können, da nach der Löschung der Hilfsmerkmale eine Identifizierung einer einzelnen Person durch die Statistikämter in aller Regel nicht mehr möglich ist. Eine Verpflichtung, zu diesem Zweck aufwendige Versuche der Zuordnung von Datensätzen zu unternehmen oder Zusatzinformationen aus anderen Quellen heranzuziehen, besteht nicht. Zum anderen sieht die Regelung vor, dass das Auskunfts- und Berichtigungsersuchen nicht die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben gefährden darf. Dies betrifft insbesondere das Berichtigungsverfahren.

§ 17a trägt den besonderen Zwecken und Rahmenbedingungen der Datenverarbeitung in der Bundesstatistik Rechnung. Ziel der Bundesstatistik ist nicht die Erfassung der persönlichen Verhältnisse von Einzelpersonen oder die Regelung von Einzelfällen, sondern die Beschreibung von Massenphänomenen anhand zusammengefasster statistischer Ergebnisse. Angaben über einzelne Personen sind darin nicht mehr erkennbar. Aus diesem Grund werden personenbezogene Daten nur dann und nur so lange gespeichert, wie dies für die Erhebung und statistische Aufbereitung erforderlich ist (§ 12 Bundesstatistikgesetz). Außerdem dürfen nach den rechtlichen Vorgaben in der Bundesstatistik Daten über einzelne Personen weder veröffentlicht werden noch in den Verwaltungsvollzug fließen (Statistikgeheimnis, Rückspielverbot). Da die Daten des Einzelnen durch die Verarbeitung in den aggregierten statistischen Ergebnissen untergehen, ist die Korrektheit der verarbeiteten Angaben für den Einzelnen ohne Belang und besteht regelmäßig kein nachvollziehbares Interesse der betroffenen Personen an einer Berichtigung von Daten.

Um große Datenvolumen verarbeiten zu können, kommen in der Bundesstatistik weitgehend automatisierte Verfahren zum Einsatz. Dazu gehören u.a. auch Plausibilitätsprüfungen, bei denen fehlende oder offenkundig unplausible Angaben durch spezielle Schätzverfahren maschinell vervollständigt oder berichtigt werden. Einzelne Berichtigungsbegehren und umfangreiche Auskunftswünsche können daher mit Aufwand verbunden sein, der außer Verhältnis zu den Interessen der betroffenen Personen steht. Um die Funktionsweise der Bundesstatistik zu gewährleisten, ist daher für die Ansprüche auf Auskunft und Berichtigung eine Einschränkung unter dem Gesichtspunkt der ordnungsgemäßen Aufgabenerfüllung vorgesehen.

Zu Artikel 9 (Weitere Folgeänderungen)

…..

Zu Artikel 10 (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 Artikel 7) zu diesem Zeitpunkt in Kraft. Gleichzeitig tritt das geltende Bundesdatenschutzgesetz 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.