

Handbuch Datenschutz

Handbuch Datenschutz

Wien, April 2020

Impressum

MedieninhaberIn, VerlegerIn und HerausgeberIn:
Bundeskanzleramt
Ballhausplatz 1, 1010 Wien
+43 1 531 15-0
bundeskanzleramt.gv.at

Verlags- und Herstellungsort: Wien, April 2020
Redaktion und Gesamtumsetzung: Datenschutzbeauftragte
Gestaltung: BKA Grafik & Design
Druck: Digitalprintcenter BMI

Alle Rechte vorbehalten: Jede Verwertung (auch auszugsweise) ist ohne schriftliche Zustimmung der Medieninhaberin unzulässig. Dies gilt insbesondere für jede Art der Vervielfältigung, der Übersetzung, der Mikroverfilmung, der Wiedergabe in Fernsehen und Hörfunk sowie der Verarbeitung und Einspeicherung in elektronische Medien, wie z. B. Internet oder CD-Rom.

Rückmeldungen:

Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an die Datenschutzbeauftragte des Bundeskanzleramtes.

Inhalt

| | |
|--|-----------|
| Einleitung | 7 |
| 1 Zuständigkeiten, wichtige Abläufe, Fristen | 8 |
| 1.1 Datenschutzbeauftragte/r..... | 8 |
| 1.2 LeiterInnen der Organisationseinheiten..... | 8 |
| 1.3 DatenschutzkoordinatorInnen..... | 8 |
| 1.4 Anfragen und Anträge..... | 9 |
| 1.5 Datenschutzverletzungen..... | 9 |
| 2 Anwendungsbereich und Grundbegriffe der DSGVO | 10 |
| 2.1 Anwendungsbereich..... | 10 |
| 2.2 Grundbegriffe..... | 10 |
| 3 Grundprinzipien der DSGVO | 11 |
| 3.1 Rechtmäßigkeit der Verarbeitung..... | 11 |
| 3.2 Verarbeitung nach Treu und Glauben („faire Verarbeitung“)..... | 11 |
| 3.3 Transparenz..... | 11 |
| 3.4 Zweckbestimmung..... | 11 |
| 3.5 Datenminimierung..... | 11 |
| 3.6 Richtigkeit..... | 12 |
| 3.7 Speicherbegrenzung..... | 12 |
| 3.8 Integrität und Vertraulichkeit..... | 12 |
| 3.9 Rechenschaftspflicht..... | 12 |
| 4 Betroffenenrechte | 13 |
| 4.1 Information über die Verarbeitung personenbezogener Daten, Erforderlichkeit von Zustimmungserklärungen..... | 13 |
| 4.2 Ersuchen um Auskunftserteilung..... | 13 |
| 4.3 Recht auf Berichtigung, Löschung etc..... | 13 |
| 4.4 Beschwerderecht, Schadenersatz..... | 13 |

| | |
|---|-----------|
| 5 Das Verarbeitungsverzeichnis | 14 |
| 5.1 Allgemeines..... | 14 |
| 5.2 Inhalt..... | 14 |
| 6 Übermittlung von Daten ins Ausland | 18 |
| 6.1 Datentransfer innerhalb der EU..... | 18 |
| 6.2 Datentransfer in Drittländer / an internationale Organisationen..... | 18 |
| 7 Die Datenschutz-Folgenabschätzung | 20 |
| 7.1 Grundsätzliches..... | 20 |
| 7.2 Zuständigkeit..... | 20 |
| 7.3 Vorfrage: Ist eine DSFA erforderlich?..... | 21 |
| 7.4 Ablauf der DSFA..... | 21 |
| 7.5 Umgang mit hohen Restrisiken..... | 22 |
| 7.6 Muster zur Durchführung einer DSFA..... | 22 |
| 8 Vertragsgestaltung gemäß der DSGVO | 23 |
| 9 FAQs zum Thema Datenschutz | 24 |
| 9.1 Anwendungsbereich der DSGVO..... | 24 |
| 9.2 Auskunftsbefahren gemäß Artikel 15 DSGVO..... | 25 |
| 9.3 Bilder von Personen..... | 30 |
| 9.4 Datenschutz-Folgenabschätzung (DSFA)..... | 36 |
| 9.5 Datensicherheitsmaßnahmen..... | 38 |
| 9.6 Einladungen..... | 39 |
| 9.7 E-Mails..... | 40 |
| 9.8 Verhängung von Geldbußen wegen Verstoßes gegen die DSGVO..... | 43 |
| 9.9 Lösungsbegehren gemäß Artikel 17 DSGVO..... | 43 |
| 9.10 Übermittlung an Drittstaaten und internationale Organisationen..... | 46 |
| 9.11 Verzeichnis von Verarbeitungstätigkeiten gemäß Artikel 30 DSGVO..... | 48 |

| | |
|--|------------|
| 10 Beispiele aus der Praxis | 54 |
| 11 Musterdokumente | 58 |
| 11.1 Newsletter-Versand | 59 |
| 11.2 Einladungen zu Veranstaltungen | 60 |
| 11.3 Hinweistafeln bei Veranstaltungen | 63 |
| 11.4 Zustimmung zur Veröffentlichung von Fotos | 64 |
| 11.5 Verwendung von Outlook-Verteilern | 67 |
| 11.6 Beantwortung der Anfragen von BürgerInnen (Bürgerservice) | 68 |
| 11.7 Musterdokument zur Beantwortung von Anträgen auf Löschung von digitalen Schriftstücke und Unterlagen bzw. personenbezogenen Daten im ELAK | 69 |
| 11.8 Beantwortung von Auskunftsbegehren | 70 |
| 11.9 Durchführung einer Datenschutz-Folgenabschätzung | 72 |
| 11.10 Datenschutzinformation für Förderverträge | 77 |
| 11.11 Hinweistafeln bei Videoüberwachung | 79 |
| Anhang | 81 |
| 12 Text der Datenschutz-Grundverordnung | 81 |
| 13 Text des Datenschutzgesetzes | 171 |
| 14 Text der Datenschutz-Folgenabschätzung-Ausnahmenverordnung | 205 |
| 15 Text der Datenschutz-Folgenabschätzung-Verordnung | 213 |

Einleitung

Am 25. Mai 2018 sind die EU-Datenschutz-Grundverordnung (DSGVO) und die das Datenschutzgesetz 2000 ändernden Bestimmungen des Datenschutz-Anpassungsgesetzes 2018 in Kraft getreten.

Die durch die DSGVO eingeführten Änderungen gelten unmittelbar, verschärfen gegenüber der bisherigen Rechtslage die Pflichten von Stellen, die personenbezogene Daten verarbeiten und räumen den Betroffenen, deren personenbezogene Daten verarbeitet werden, größere Rechte ein.

Das vorliegende Handbuch enthält wichtige Informationen zu den datenschutzrelevanten Regelungen, die ab 25. Mai 2018 von allen Bediensteten des BKA zu beachten sind. Besonders hilfreich für die Praxis sind die im Handbuch enthaltenen umfassenden FAQs, Fallbeispiele und Muster, die auf Grund der im BKA aufgetretenen Fragen und Problemstellungen speziell für den behördlichen Bereich entwickelt wurden.

Im letzten Teil des Handbuches finden Sie die derzeit geltenden Textfassungen der EU-Datenschutz-Grundverordnung, des österreichischen Datenschutzgesetzes sowie der Datenschutz-Folgenabschätzung-Ausnahmenverordnung und der Datenschutz-Folgenabschätzung-Verordnung.

1 Zuständigkeiten, wichtige Abläufe, Fristen

1.1 Datenschutzbeauftragte/r

Die DSGVO verlangt, dass für jede öffentliche Stelle eine / ein **Datenschutzbeauftragte/r** zu benennen ist. Für den Bereich des BKA ist das:

Datenschutzbeauftragte

MR Dr. Ulrike Wimmer-Heller

E-Mail: ulrike.wimmer-heller@bka.gv.at

Telefon: +43 1 531 15-202313

Die Aufgaben der / des Datenschutzbeauftragten sind:

- Unterrichtung und Beratung des Verantwortlichen (Bundekanzler, Bundesministerin) und der MitarbeiterInnen hinsichtlich ihrer Pflichten nach dem Datenschutzrecht,
- Überwachung und Überprüfung der Einhaltung der Datenschutzvorschriften und Strategien für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, Sensibilisierung und Schulung der MitarbeiterInnen,
- auf Anfrage Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung,
- Zusammenarbeit mit der Aufsichtsbehörde,
- Anlaufstelle für die Aufsichtsbehörde.

1.2 LeiterInnen der Organisationseinheiten

Die LeiterInnen der einzelnen Organisationseinheiten sind verantwortlich für die korrekte Befüllung des Verarbeitungsverzeichnisses.

Sie leiten außerdem in den einzelnen Organisationseinheiten einlangende Anfragen und Anträge von Betroffenen (BürgerInnen, Bedienstete) zum Thema Datenschutz an die Datenschutzbeauftragte weiter. Da die DSGVO kurze Fristen für die Beantwortung vorsieht (grundsätzlich ein Monat ab Einlangen), **müssen Anfragen und Anträge zum Thema Datenschutz unverzüglich an die Datenschutzbeauftragte übermittelt werden.**

1.3 DatenschutzkoordinatorInnen

Erste Anlaufstelle für Fragen zur Befüllung des Verarbeitungsverzeichnisses sind die DatenschutzkoordinatorInnen:

Sektion I: Mag. Michael Böhm, Claus Ryavec, MA

Sektion II: Mag. Elke Springer-Schueller

Sektion III: Mag. Dietmar Hillbrand, MPA, Mag. Karin Maurer

Sektion IV: Mag. Dr. Helmut Schnitzer, Ines Ettl, BA MA

Sektion V: Dr. Gerhard Kunnert

Medienbetreuung und Europakommunikation: Mag. Irene Kaufmann, Dr. Alice Karrer-Brunner

Für das Bundesdenkmalamt und die Bundestheater-Holding wurden eigene Datenschutzbeauftragte bestellt:

Bundesdenkmalamt: Sylvia Preinsperger

Bundestheater-Holding: Dr. Günther Lackenbacher

1.4 Anfragen und Anträge

Die Datenschutzbeauftragte protokolliert Anfragen und Anträge zum Thema Datenschutz und entscheidet über die weitere Bearbeitung / Beantwortung, die sich nach dem konkreten Inhalt der Anliegen richtet. In Frage kommt eine Bearbeitung / Beantwortung durch die jeweilige Organisationseinheit, durch die Datenschutzbeauftragte, durch ExpertInnen aus dem IT-Bereich oder durch die genannten Stellen gemeinsam.

1.5 Datenschutzverletzungen

Bei Vorliegen einer **Datenschutzverletzung** muss die **Datenschutzbehörde unverzüglich und möglichst binnen 72 Stunden verständigt werden**, wenn die Verletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten des / der Betroffenen führt.

Auch die / der **Betroffene** ist im Falle eines voraussichtlich hohen Risikos **unverzüglich von der Datenschutzverletzung zu informieren**.

Auf Grund der besonders kurzen Fristen ist bei einer Datenschutzverletzung die **sofortige Verständigung der zuständigen Abteilungsleiterin / des zuständigen Abteilungsleiters und der Datenschutzbeauftragten** erforderlich, um die nötigen Schritte unverzüglich einzuleiten.

Unter einer Datenschutzverletzung sind z. B. zu verstehen: ein Vorfall, durch den Unbefugten der Zugriff auf Daten möglich wird (Verlust des Datenträgers, Hackerangriff, ...); die unbeabsichtigte oder unrechtmäßige Vernichtung oder Veränderung der Daten; der Verlust der Daten.

2 Anwendungsbereich und Grundbegriffe der DSGVO

2.1 Anwendungsbereich

Die DSGVO findet Anwendung auf **alle Verarbeitungen personenbezogener Daten in der EU** ohne Rücksicht darauf, ob ein/e EU-BürgerIn betroffen ist.

Ausgenommen sind lediglich folgende Bereiche:

- ausschließlich persönliche oder familiäre Tätigkeiten,
- Tätigkeiten der Behörden in Zusammenhang mit Straftaten, Strafvollstreckung und öffentlicher Sicherheit,
- Tätigkeiten der Mitgliedstaaten im Rahmen der gemeinsamen Außen- und Sicherheitspolitik,
- Tätigkeiten außerhalb des Anwendungsbereiches des Unionsrechts (z. B. Ordensrecht, Verfassungsschutz).

2.2 Grundbegriffe

Personenbezogene Daten sind alle Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen (Menschen) 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 (bezogen auf die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität) identifiziert werden kann.

Verarbeitung ist jede ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten und die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Es fallen darunter das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, Anpassung oder Veränderung, das Auslesen, Abfragen, die Verwendung, Offenlegung durch Übermittlung, Verbreitung oder andere Art der Bereitstellung, der Abgleich, die Einschränkung, das Löschen oder Vernichten.

Dateisystem ist 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.

Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im Bundeskanzleramt sind das der Bundeskanzler oder der / die zuständige BundesministerIn.

Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden.

3 Grundprinzipien der DSGVO

3.1 Rechtmäßigkeit der Verarbeitung

Für jede Verarbeitung muss eine **Rechtsgrundlage** vorliegen. Es kommen im behördlichen Bereich in Frage: gesetzliche Verpflichtung des Verantwortlichen, Erforderlichkeit zur Vertragserfüllung, Einwilligung der / des Betroffenen, öffentliches Interesse, lebenswichtige Interessen.

Die Verarbeitung **besonderer Kategorien von Daten** (ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, Gesundheitsdaten, Sexualleben oder sexuelle Orientierung) unterliegt weiteren Beschränkungen.

3.2 Verarbeitung nach Treu und Glauben („faire Verarbeitung“)

Bei der Verarbeitung sind die **vernünftigen Erwartungen** der betroffenen Person, die auf ihrer Beziehung zum Verantwortlichen beruhen, zu berücksichtigen.

3.3 Transparenz

Die Verarbeitung muss in einer für die Betroffenen **nachvollziehbaren und vorhersehbaren** Weise stattfinden.

3.4 Zweckbestimmung

Der Zweck muss vor Beginn der Verarbeitung festgelegt werden, **eindeutig bestimmt und legitim** sein. Zweckfreie Verarbeitungen sind unzulässig, ebenso Globaleinwilligungen.

3.5 Datenminimierung

Die Datenverarbeitung muss **erheblich** (= geeignet, das Ziel zu erreichen), **erforderlich** (= auf die Verfolgung des Zwecks minimiert) und **angemessen** (= Ergebnis einer Abwägung zwischen dem verfolgten Zweck und der Bedeutung der beeinträchtigten Rechte der / des Betroffenen) sein.

3.6 Richtigkeit

Aus diesem Prinzip ergibt sich u. a., dass Daten auf dem **neuesten Stand** zu halten sind.

3.7 Speicherbegrenzung

Aus diesem Prinzip ist abzuleiten, dass **bereits bei Erhebung eine Datenminimierung** stattzufinden hat und Daten dann nur so lange **aufzubewahren** sind, als das **angemessen und erforderlich** ist.

3.8 Integrität und Vertraulichkeit

Es ist **angemessene Sicherheit** in technischer und organisatorischer Hinsicht zu gewährleisten.

3.9 Rechenschaftspflicht

Der Verantwortliche muss die **Einhaltung** der genannten Grundsätze **darlegen und nachweisen** können.

Jede Verarbeitung personenbezogener Daten muss den angeführten Grundsätzen entsprechen. Das muss durch rechtliche, technische und organisatorische Maßnahmen gewährleistet werden. Der Verantwortliche muss die Einhaltung der genannten Grundsätze darlegen und nachweisen können.

4 Betroffenenrechte

4.1 Information über die Verarbeitung personenbezogener Daten, Erforderlichkeit von Zustimmungserklärungen

Die Betroffenen müssen bei Vorliegen einer **gesetzlichen oder vertraglichen Grundlage für die Datenverarbeitung** bereits im Zeitpunkt der Erhebung, also vorab, detailliert darüber informiert werden, dass ihre personenbezogenen Daten erhoben / verarbeitet werden. Diese Informationspflicht umfasst Namen und Kontaktdaten des Verantwortlichen, der / des Datenschutzbeauftragten, Zweck(e) und Rechtsgrundlage der Datenverarbeitung, mögliche Empfänger oder Empfängerkategorien, beabsichtigte Übermittlungen in ein Drittland, Informationen zur Speicherdauer und zu den Betroffenenrechten.

Gibt es für die personenbezogene Datenverarbeitung keine gesetzliche oder vertragliche Grundlage, muss die **Zustimmung der Betroffenen** nachweislich eingeholt werden.

Es wurden gemeinsam mit den DatenschutzkoordinatorInnen und den einzelnen Organisationseinheiten bereits zahlreiche Muster entworfen, deren genaue Formulierung sich nach der konkreten Verarbeitung richtet.

4.2 Ersuchen um Auskunftserteilung

Ersuchen um Auskunftserteilung von Betroffenen sind **innerhalb eines Monats ab Einlangen zu beantworten**.

4.3 Recht auf Berichtigung, Löschung etc.

Betroffene haben ein Recht auf **Berichtigung**, ein Recht auf **Einschränkung** der Verarbeitung, ein Recht auf **Löschung**, ein Recht auf **Datenübertragbarkeit** und ein **Widerspruchsrecht**.

4.4 Beschwerderecht, Schadenersatz

Betroffene können **Beschwerde bei der Datenschutzbehörde** erheben und die Bescheide der Datenschutzbehörde beim Bundesverwaltungsgericht bekämpfen sowie **Schadenersatzansprüche** geltend machen.

5 Das Verarbeitungsverzeichnis

5.1 Allgemeines

Die DSGVO verpflichtet den Verantwortlichen ein „**Verzeichnis von Verarbeitungstätigkeiten**“ zu erstellen und zu führen.

Das Verarbeitungsverzeichnis ist wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dem Verantwortlichen beim Nachweis der Einhaltung der DSGVO. Es ist auf Anfrage der Aufsichtsbehörde (Datenschutzbehörde) unverzüglich zur Verfügung zu stellen.

Zur einheitlichen Führung des Verarbeitungsverzeichnisses wurde für das Bundeskanzleramt ein **elektronisches tool („DataReg“)** entwickelt. Die Verantwortung für die Befüllung fällt in die Zuständigkeit der LeiterInnen der einzelnen Organisationseinheiten im Bundeskanzleramt, sie werden dabei von der Datenschutzbeauftragten und den DatenschutzkoordinatorInnen unterstützt.

Die Erstellung des Verarbeitungsverzeichnisses stellt **eine** Dokumentationspflicht nach der DSGVO dar. Hinzu kommen z. B. das Vorhandensein von Zustimmungserklärungen und Datenschutz-Folgenabschätzungen.

5.2 Inhalt

Das Verarbeitungsverzeichnis muss folgende Informationen enthalten:

- **Name und Kontaktdaten des Verantwortlichen, Name und Kontaktdaten der / des Datenschutzbeauftragten**

- **Bezeichnung der Verarbeitungstätigkeit**

Einzutragen sind alle ganz oder teilweise automatisierten Verarbeitungen und nicht-automatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Für jede einzelne Verarbeitungstätigkeit ist eine eigene Beschreibung zu erstellen.

Unter Verarbeitungstätigkeit wird ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden.

Ändert sich der Zweck einer Verarbeitung, so handelt es sich dabei grundsätzlich um eine eigene Verarbeitungstätigkeit. Bei einer nur geringfügigen Änderung des Zwecks muss geprüft werden, ob eine bereits bestehende Beschreibung einer Verarbeitungstätigkeit lediglich anzupassen ist, oder ob eine vollständige neue Beschreibung anzufertigen ist.

Neu hinzukommende Verarbeitungen sind laufend ins Verarbeitungsverzeichnis einzutragen.

- **Zweck(e) der Verarbeitung**

Für jede Verarbeitung ist / sind vorab der Zweck / die Zwecke festzulegen. Je Beschreibung einer Verarbeitungstätigkeit ist / sind der Verarbeitungszweck / die Verarbeitungszwecke zu dokumentieren.

Die Zwecke müssen eindeutig und so aussagekräftig sein, dass die Aufsichtsbehörde die Angemessenheit der getroffenen Schutzmaßnahmen und die Zulässigkeit der Verarbeitung vorläufig einschätzen kann. Als Beispiele sind zu nennen:

- Personalaktenführung
- Abrechnung der Bezüge
- Arbeitszeiterfassung
- Nutzungsprotokollierungen IT / Internet / E-Mail
- Bewerbungsverfahren
- Telefondatenerfassung
- Videoüberwachung
- Beschaffung / Einkauf
- Buchhaltung
- Antragsbearbeitung
- Bürgerinformationssysteme
- Anlegen und Verwalten diverser Listen für Einladungen, Newsletter, Versand von Informationsmaterial

- **Betroffenengruppe**

Als Beispiele sind zu nennen:

- Beschäftigte
- Anfragende im Bereich der Abteilung X
- AntragstellerInnen im Bereich der Abteilung X
- BezieherInnen des Newsletters der Abteilung X
- TeilnehmerInnen an der Veranstaltung X
- TeilnehmerInnen an den Veranstaltungen der Abteilung X

- **Datenkategorien**

Für die jeweilige Betroffenengruppe sind die verarbeiteten Datenkategorien anzuführen, z. B. für die Betroffenengruppe „Beschäftigte“:

- Mitarbeiter-Stammdaten
- Bewerbungen mit Qualifikationsdaten, Tätigkeiten etc.
- Arbeitszeugnisse mit Adressdaten, Leistungsdaten, Beurteilungsdaten etc.
- Ermahnungen mit Daten zum Arbeitsverhalten
- ärztliche Untersuchungen
- Videoüberwachung an Arbeitsplätzen

Die Verarbeitung besonderer Kategorien von Daten ist gesondert zu beschreiben.

- **Empfänger**

Zu beschreiben sind die Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen. Es sind darunter auch „Zugriffsberechtigte“ zu verstehen, die nicht namentlich anzuführen sind, aber über eine Rollen- oder Funktionsbeschreibung eindeutig bestimmbar sein müssen.

Hinsichtlich der Abrechnung der Bezüge von Bediensteten sind beispielsweise zu nennen:

- Banken
- Sozialversicherungsträger
- Finanzämter
- behördeninterne Datenempfänger
- Gläubiger

- **Übermittlung in Drittländer / an internationale Organisationen**

Es ist das betroffene Drittland / die betroffene internationale Organisation anzugeben. Wenn keine Übermittlung stattfindet, ist das ebenfalls zu vermerken.

Empfänger in Drittländern und internationalen Organisationen sind gesondert konkret zu benennen.

- **Löschfrist**

In dieser Rubrik sind die vorgesehenen Fristen für die Löschung der einzelnen Datenkategorien anzugeben.

Ausschlaggebend ist der Zweck der Datenerhebung und der Datennutzung. Zu löschen ist grundsätzlich unverzüglich nach Erfüllung des Zwecks, es sei denn es gibt gesetzliche Aufbewahrungspflichten oder vom Verantwortlichen entsprechend den Grundsätzen der DSGVO festgelegte Löschfristen.

Ein allgemeiner Hinweis auf Aufbewahrungspflichten genügt nicht, es sind präzise Angaben erforderlich.

- **Technische und organisatorische Maßnahmen**

Angesprochen sind Maßnahmen, die hinsichtlich der Sicherheit der Verarbeitung getroffen werden ebenso wie Maßnahmen zur Gewährleistung von Betroffenenrechten.

Dazu zählen die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Gewährleistung der Integrität und Vertraulichkeit sowie der Verfügbarkeit und Belastbarkeit der Systeme und Dienste, die Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu ihnen nach einem physischen oder technischen Zwischenfall sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen.

Es wird hier in Bezug auf die Standardanwendungen ein Verweis auf das allgemeine Sicherheitskonzept im BKA erfolgen, sodass nur Abweichungen davon für die jeweilige Verarbeitungstätigkeit extra angeführt werden müssen. In diesem Fall

ist eine allgemeine, einfach nachvollziehbare Beschreibung der getroffenen Maßnahmen aufzunehmen. Soweit innerhalb einer Verarbeitungstätigkeit hinsichtlich der Personen- bzw. Datenkategorien differenziert wird, sind auch die entsprechenden Maßnahmen differenziert darzustellen.

- **AnsprechpartnerIn**

In dieser Rubrik ist der/die AnsprechpartnerIn in der jeweils zuständigen Organisationseinheit für die Verarbeitung anzuführen.

- **Rechtliche Grundlage**

Gemeint ist die konkrete Rechtsgrundlage der Verarbeitung bezogen auf den festgelegten Zweck.

In Frage kommen eine gesetzliche Verpflichtung des Verantwortlichen, die Erforderlichkeit der Verarbeitung zur Vertragserfüllung, die Einwilligung der/des Betroffenen, ein öffentliches Interesse oder lebenswichtige Interessen.

- **allfälliger Auftragsverarbeiter**

In dieser Rubrik sind vom BKA verschiedene Auftragsverarbeiter anzugeben, die im Auftrag des Verantwortlichen Verarbeitungen durchführen. Das kann ein anderes Ressort sein oder auch ein externer Dienstleister.

Die Befüllung durch die einzelnen Organisationseinheiten ist auch hier nur erforderlich, soweit es sich nicht um eine Standardanwendung handelt.

6 Übermittlung von Daten ins Ausland

6.1 Datentransfer innerhalb der EU

Mit der DSGVO liegt eine gemeinsame materielle Rechtsgrundlage für die Verarbeitung personenbezogener Daten innerhalb der EU vor. Eine Datenübermittlung (auch diese ist eine Art der Verarbeitung) von Österreich in einen anderen EU-Mitgliedstaat unterliegt daher denselben Anforderungen wie eine Datenübermittlung innerhalb Österreichs und keinen darüber hinausgehenden Beschränkungen.

6.2 Datentransfer in Drittländer / an internationale Organisationen

Das Schutzniveau der DSGVO darf bei der Übermittlung von personenbezogenen Daten in Drittländer / an internationale Organisationen nicht untergraben werden. Es müssen vorhanden sein: eine **Rechtsgrundlage** für die in Aussicht genommene Datenübermittlung und ein **angemessenes Schutzniveau beim Empfänger**.

Grundsätzlich muss vorab eine **Genehmigung des Datentransfers durch die Datenschutzbehörde** eingeholt werden. Wichtige Ausnahmen von diesem Grundsatz sind z. B.:

- **Es gibt einen Angemessenheitsbeschluss der Europäischen Kommission.**
Ein solcher existiert derzeit bis auf Widerruf für die Schweiz, Kanada, Andorra, Argentinien, Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Uruguay und jene US-Unternehmen, die sich zu den „Safe Harbor“-Bestimmungen verpflichtet haben.

Bis auf Widerruf durch die EU-Kommission sind Datentransfers in die genannten Drittstaaten / an die genannten Unternehmen ohne weitere formale Voraussetzungen zulässig. Nach der DSGVO kann die EU-Kommission künftig auch für ein Gebiet, einen Sektor und internationale Organisationen Angemessenheitsbeschlüsse fassen.

Die Veröffentlichung der Angemessenheitsbeschlüsse erfolgt im Amtsblatt der EU und auf ihrer Website.

Exkurs: Datentransfer in die USA („Safe Harbor“, „Privacy Shield“)

Die Entscheidung der EU-Kommission, wonach eine Datenübermittlung an Unternehmen in den USA, die nach den „Safe Harbor“-Bestimmungen zertifiziert sind, ohne weiteres zulässig ist, wurde vom EuGH für ungültig erklärt.

Der von der EU-Kommission vorgestellte Entwurf eines „Privacy Shield“ wird von der Artikel-29-Datenschutzgruppe als unzureichend angesehen, sodass derzeit Rechtsunsicherheit bei Datentransfers in die USA besteht.

- Es sind Daten betroffen, die **im Inland zulässigerweise veröffentlicht** wurden.
- Die / der **Betroffene hat ohne jeden Zweifel ihre / seine Zustimmung** zur Übermittlung ihrer / seiner Daten ins Ausland gegeben.
- Ein **eindeutig im Interesse der / des Betroffenen abgeschlossener Vertrag** kann nur durch Übermittlung der Daten ins Ausland erfüllt werden.
- Es handelt sich um Datenverkehr mit **österreichischen Dienststellen im Ausland**.
- Die Datenübermittlung ins Ausland ist zur Wahrung eines **wichtigen öffentlichen Interesses** oder zur **Wahrung eines lebenswichtigen Interesses einer Person** notwendig und so dringlich, dass eine Genehmigung der Datenschutzbehörde nicht rechtzeitig eingeholt werden kann. **Die Datenschutzbehörde ist in einem solchen Fall umgehend von der Datenübermittlung zu verständigen.**

7 Die Datenschutz-Folgenabschätzung

7.1 Grundsätzliches

Die DSGVO führt verpflichtend das Instrument der Datenschutz-Folgenabschätzung (DSFA) ein.

Die DSFA dient der **systematischen Eindämmung von Risiken** für die Rechte und Freiheiten Betroffener und hilft, die eigenen Prozesse bei der Verarbeitung personenbezogener Daten besser zu verstehen und die Pflichten nach der DSGVO umzusetzen.

Zentrale Frage für die Entscheidung, ob eine DSFA durchzuführen ist, ist jene nach der **Intensität des Eingriffs in die Rechte Betroffener**, denn auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten entstehen Risiken für die Betroffenen.

Eine DSFA ist zwingend erforderlich, wenn ein Verarbeitungsvorgang **voraussichtlich ein hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Die DSGVO zählt beispielhaft folgende Fälle auf, in denen eine Datenschutzfolgenabschätzung „**insbesondere**“ **erforderlich** ist:

- Verarbeitung zur systematischen, umfassenden Bewertung persönlicher Aspekte (u. a. „Profiling“),
- umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten („sensible Daten“),
- Verarbeitung zur systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche (z. B. Videoüberwachung);

Die Notwendigkeit einer DSFA ergibt sich aber auch in anderen Fällen, wie

- Verarbeitung großer Mengen personenbezogener Daten,
- Verarbeitung betrifft eine große Anzahl an Personen,
- Ausübung der Rechte betroffener Personen ist erschwert,
- Einsatz neuer Technologien im großen Umfang im Rahmen der Verarbeitung;

Die Pflicht zur Durchführung einer DSFA entsteht bereits **vor Aufnahme des Verarbeitungsvorganges**, und zwar für Verarbeitungen, die ab 25. Mai 2018 eingeführt werden.

Wenn mehrere ähnliche Verarbeitungsvorgänge voraussichtlich ein ähnliches Risiko aufweisen, können sie zusammen bewertet werden. Das ist der Fall, wenn ähnliche Technologien zur Verarbeitung vergleichbarer Daten(-kategorien) zu gleichen Zwecken eingesetzt werden.

Die DSFA ist **kein einmaliger Vorgang**, sondern sie ist bei neuen Risiken zu überprüfen und anzupassen.

7.2 Zuständigkeit

Verantwortlich für die Prüfung der Notwendigkeit einer DSFA (hohes Risiko?) sowie für ihre Durchführung ist jede Organisationseinheit für die dort eingesetzten Verarbeitungsvorgänge.

Sowohl die Entscheidung für oder gegen die Durchführung einer DSFA als auch ihre Durchführung selbst werden im Normalfall IT-Kenntnisse erfordern, sodass die IT-FachexpertInnen des BKA hinzuziehen sind.

7.3 Vorfrage: Ist eine DSFA erforderlich?

In einem ersten Schritt ist zu prüfen, ob ein Verarbeitungsvorgang voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat („Schwellwertanalyse“).

Die Datenschutzbehörde hat zunächst durch Verordnung jene Arten von Verarbeitungsvorgängen bestimmt, für die keine Datenschutz-Folgenabschätzung erforderlich ist (siehe Datenschutz-Folgenabschätzung-Ausnahmenverordnung, DSFA-AV, BGBl. II Nr. 108/2018).

In Folge wurden mit Verordnung der Datenschutzbehörde auch jene Arten von Verarbeitungsvorgängen festgelegt, für die jedenfalls eine Datenschutz-Folgenabschätzung durchgeführt werden muss (siehe Datenschutz-Folgenabschätzung-Verordnung, DSFA-V, BGBl. II Nr. 278/2018). Die genannten Verordnungen finden sich im Anhang dieses Handbuches.

In jedem Fall sind die Entscheidung für oder gegen eine DSFA und die Gründe dafür schriftlich zu dokumentieren.

7.4 Ablauf der DSFA

Vorbereitung

Es ist zu prüfen, ob der durch den Verarbeitungsvorgang bewirkte Eingriff in die Rechte Betroffener zum Erreichen der verfolgten Zwecke tatsächlich notwendig ist oder ob Alternativen zur Verfügung stehen, die weniger stark in die Rechte der Betroffenen eingreifen.

Gibt es solche Alternativen, so sind die Verarbeitungsvorgänge zu adaptieren, z. B. durch die (inhaltliche) Beschränkung der verarbeiteten Daten, die Beschränkung der Zugriffsberechtigungen oder den Einsatz anderer Technologien.

Nachdem der Verarbeitungsvorgang festgelegt wurde, ist die Rechtsgrundlage dafür zu dokumentieren.

Durchführung

Die Risikoquellen für die Rechte und Freiheiten Betroffener müssen ermittelt werden. Eine wesentliche Frage ist, welche Personen warum motiviert sein könnten, die Daten unrechtmäßig zu nutzen und wie hoch die Wahrscheinlichkeit dafür ist.

Darauf aufbauend ist festzulegen, wie hoch das Risiko für die Rechte und Freiheiten Betroffener in Bezug auf Art, Umfang, Umstände und Zwecke der Verarbeitung ist. Für die Höhe des Risikos sind die Schwere der Beeinträchtigung der Rechte und Freiheiten, die Schwere potenzieller Schäden (physische, materielle, immaterielle) und die Eintrittswahrscheinlichkeit zu berücksichtigen.

Die ermittelten Risiken müssen durch geeignete Abhilfemaßnahmen eingedämmt werden, das sind insbesondere technisch-organisatorische Maßnahmen.

Verbleibende Restrisiken sind zu ermitteln und zu dokumentieren. Es ist festzulegen, wie mit diesen Restrisiken umgegangen wird.

Es ist ein DSFA-Bericht zu erstellen. Dieser ist Teil der Dokumentations- und Rechenschaftspflicht des Verantwortlichen.

Der DSFA-Bericht enthält:

- die (geplanten) Verarbeitungsvorgänge,
- ihre Zwecke,
- die Bewertung ihrer Notwendigkeit und Verhältnismäßigkeit,
- die Beschreibung der Risiken,
- die Bewertung der Risiken,
- die Abhilfemaßnahmen zur Risikoeindämmung,
- die Darstellung der Restrisiken samt Entscheidung über den Umgang mit diesen.

Umsetzung

Die erforderlichen technisch-organisatorischen Maßnahmen sind vor Einsatz der geplanten Datenverarbeitung umzusetzen, auf ihre Wirksamkeit zu testen sowie gegebenenfalls anzupassen.

In Folge ist auch die Wirksamkeit der umgesetzten Abhilfemaßnahmen zu dokumentieren.

Überprüfung

Die / der Datenschutzbeauftragte prüft die DSFA abschließend und teilt das Ergebnis der Leitungsebene mit.

Bei Änderung der Risiken ist die DSFA erneut durchzuführen.

7.5 Umgang mit hohen Restrisiken

Wenn eine DSFA trotz technisch-organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Restrisiko ergibt, muss der Verantwortliche die Datenschutzbehörde informieren, die Empfehlungen abgeben kann. Die Datenschutzbehörde kann auch z. B. eine Anweisung aussprechen.

7.6 Muster zur Durchführung einer DSFA

Ein Muster zur formal richtig aufgebauten Durchführung einer Datenschutz-Folgenabschätzung findet sich unter Punkt 11.9. dieses Handbuchs.

8 Vertragsgestaltung gemäß der DSGVO

Werden personenbezogene Daten für das BKA von externen Stellen (anderes Ressort, externe Dienstleister) verarbeitet, ist eine schriftliche Vereinbarung über diese Auftragsverarbeitung abzuschließen.

Diese beinhaltet:

- den Gegenstand des Auftrages,
- Art und Zweck der Datenverarbeitung,
- Art der Daten (Datenkategorien),
- Kategorie(n) betroffener Personen,
- Dauer der Verarbeitung,
- Pflichten des Auftragnehmers,
- Technisch-organisatorische Maßnahmen,
- Ort der Durchführung der Datenverarbeitung,
- Bestimmungen zur Hinzuziehung von Sub-Auftragsverarbeitern.

Bei Bedarf kann von der Datenschutzbeauftragten ein Muster zur Formulierung der Vereinbarung über die Auftragsverarbeitung zur Verfügung gestellt werden.

9 FAQs zum Thema Datenschutz

9.1 Anwendungsbereich der DSGVO

Kommt die DSGVO über den Umweg des DSG auch auf juristische Personen zur Anwendung?

Das in § 1 (1) DSG als Verfassungsbestimmung normierte Grundrecht auf Datenschutz gilt auch nach Inkrafttreten der DSGVO für juristische Personen unverändert weiter, zumal sich die DSGVO nur auf natürliche Personen bezieht. Das wiederum bedeutet, dass die über § 1 (1) DSG hinausgehenden in der DSGVO geregelten Rechte für juristische Personen somit nicht gelten. Insbesondere sind sie auch nicht nach dem Regime der DSGVO, also über Beschwerde an die Datenschutzbehörde, durchsetzbar.

Ist die Sozialversicherungsnummer ein sensibles Datum?

Es kommt darauf an, ob die Sozialversicherungsnummer einen Bezug zu sensiblen Daten herstellt oder nicht.

Werden z. B. in einem Formular die Sozialversicherungsnummer und Gesundheitsdaten abgefragt und in Folge verarbeitet, sodass mit der Sozialversicherungsnummer die Gesundheitsdaten abrufbar sind, dann ist die Sozialversicherungsnummer selbst auch als sensibles Datum zu bewerten.

Werden in einem Formular aber z. B. Name, Adresse und Sozialversicherungsnummer abgefragt und diese Daten in Folge verarbeitet, ist die Sozialversicherungsnummer mangels Verknüpfung mit sensiblen Daten auch selbst nicht als sensibles Datum einzustufen.

Ist die E-Mail-Adresse ein personenbezogenes Datum?

Ja, die E-Mail-Adresse ist ein personenbezogenes Datum, wenn in irgendeiner Form die Zuordnung zu einer bestimmten Person möglich ist, was regelmäßig auch bei Postfach-Adressen der Fall ist.

Kommt die DSGVO rückwirkend zur Anwendung?

Das Bundesverwaltungsgericht (BVwG) hat im Erkenntnis vom 1.10.2018, W253 2140428-1/9E, der Beschwerde gegen einen Bescheid der Datenschutzbehörde (DSB) aus dem Jahr 2016 stattgegeben und festgestellt, dass der Beschwerdeführer durch den gerügten Verarbeitungsvorgang im Dezember 2014 im Geheimhaltungsrecht verletzt worden ist. Das BVwG hat dabei zur Beurteilung der Rechtmäßigkeit der Verarbeitung die (strengere) DSGVO, insbesondere Artikel 6 Abs. 1 letzter Satz, herangezogen.

Die DSB hat dieses Erkenntnis in einer ordentlichen Revision beim Verwaltungsgerichtshof bekämpft, da sie von der Unzulässigkeit dieser rückwirkenden Anwendung ausgeht.

In Fällen, in denen ein Leistungsanspruch (z.B. Löschung) zu beurteilen ist, ist aber nach Auffassung der DSB die Rechtslage im Zeitpunkt der Entscheidung maßgeblich.

9.2 Auskunftsbegehren gemäß Artikel 15 DSGVO

Was ist Inhalt einer Auskunft gemäß Artikel 15 DSGVO?

Wenn es zutrifft, dass personenbezogene Daten der Antragstellerin/des Antragstellers verarbeitet werden, hat die Auskunft folgende Informationen zu beinhalten:

1. die Bestätigung, dass personenbezogene Daten verarbeitet werden
2. die Verarbeitungszwecke
3. die Kategorien personenbezogener Daten, die verarbeitet werden und der konkrete Inhalt der gespeicherten Daten, also z. B. welcher Name, welche Gehaltseinstufung etc.
4. die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden
5. bei Übermittlung an ein Drittland oder eine internationale Organisation Information über die geeigneten Garantien gemäß Art. 46 DSGVO
6. die Dauer der Speicherung oder, falls das nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
7. die Belehrung über die Rechte nach der DSGVO
8. wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten
9. das Bestehen einer automatisierten Entscheidungsfindung

Wenn es nicht zutrifft, dass personenbezogene Daten der Antragstellerin/des Antragstellers verarbeitet werden:

1. Information, dass keine personenbezogene Daten verarbeitet werden
2. die Belehrung über die Rechte nach der DSGVO

Wie ist die Beantwortung des Auskunftsbegehrens zu formulieren?

Wenn es zutrifft, dass personenbezogene Daten der Antragstellerin/des Antragstellers verarbeitet werden, ist die Beantwortung folgendermaßen abzufassen und inhaltlich je nach dem vorliegenden Sachverhalt zu ergänzen:

Das Bundeskanzleramt hat Ihren Antrag auf Auskunft vom ... am ... erhalten und teilt Ihnen innerhalb der vorgesehenen Frist von einem Monat folgendes mit:

Das Bundeskanzleramt (eventuell, je nach Anfrage: Sektion ..., Abteilung ...) verarbeitet Sie betreffende personenbezogene Daten.

Zweck dieser Verarbeitung ist ...

Es werden folgende Kategorien Sie betreffender personenbezogener Daten verarbeitet: Name, ...

(Anmerkung: Hier sind auch die Inhalte der Daten konkret anzuführen, d. h. der konkrete Name, ...)

Ausdrucke der relevanten Datenverarbeitungen finden Sie im Anhang. ODER Beiliegend werden Ihnen die relevanten Datenverarbeitungen elektronisch übermittelt.

(Falls zutreffend:) Ihre Daten wurden dem Bundeskanzleramt von ... übermittelt.

(Falls zutreffend:) Die Sie betreffenden personenbezogenen Daten werden gegenüber folgenden Empfängern offengelegt: ...

Die Sie betreffenden personenbezogenen Daten werden gespeichert und ... (z. B. Verweis auf ELAK-Skartierungsfrist) gelöscht. ODER Die Sie betreffenden personenbezogenen Daten werden gespeichert und nicht gelöscht, weil ... (z. B. Verweis auf Archivwürdigkeit).

(Anmerkung: Bitte entsprechend dem Eintrag ins DataReg formulieren und gesetzliche Grundlage für die Löschfrist angeben, wenn eine solche besteht.)

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Wenn es nicht zutrifft, dass personenbezogene Daten der Antragstellerin/ des Antragstellers verarbeitet werden, ist die Beantwortung folgendermaßen abzufassen:

Das Bundeskanzleramt hat Ihren Antrag auf Auskunft vom ... am ... erhalten und teilt Ihnen innerhalb der vorgesehenen Frist von einem Monat folgendes mit:

Das Bundeskanzleramt *(eventuell, je nach Anfrage: Sektion ..., Abteilung ...)* verarbeitet keine Sie betreffenden personenbezogene Daten.

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie

glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

In welchem Verhältnis steht das DSGVO-Auskunftsrecht zum Recht auf Akteneinsicht?

Akteneinsicht und Auskunftsrecht müssen keineswegs konform sein. Die Akteneinsicht kann weiter gehen bzw. mehr Auskünfte gewähren, als das Auskunftsrecht nach DSGVO, weil dieses auf die eigenen personenbezogenen Daten beschränkt ist.

Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Wenn in Dokumenten Informationen über die Antragstellerin / den Antragsteller und auch andere Personen enthalten sind, würde die Übermittlung an die Antragstellerin / den Antragsteller in die Rechte und Freiheiten dieser Personen eingreifen, sie dürfen ihr / ihm daher nicht übermittelt werden.

Zu berücksichtigen ist aber, dass auch der hoheitlich handelnde Verantwortliche selbst geschützt ist: Das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO besteht gegenüber einem hoheitlich tätigen Verantwortlichen unbeschadet anderer gesetzlicher Beschränkungen dann nicht, wenn durch die Erteilung dieser Auskunft die Erfüllung einer dem Verantwortlichen gesetzlich übertragenen Aufgabe gefährdet wird.

Welche Unterlagen kann die / der Betroffene verlangen?

Zu übermitteln ist auf Verlangen eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen.

Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Wenn in Dokumenten Informationen über die Antragstellerin / den Antragsteller und auch andere Personen enthalten sind, würde die Übermittlung an die Antragstellerin / den Antragsteller in die Rechte und Freiheiten dieser Personen eingreifen, sie dürfen ihr / ihm daher nicht übermittelt werden.

Geschützt ist aber auch der hoheitlich handelnde Verantwortliche selbst: Das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO besteht gegenüber einem hoheitlich tätigen Verantwortlichen unbeschadet anderer gesetzlicher Beschränkungen dann nicht, wenn durch die Erteilung dieser Auskunft die Erfüllung einer dem Verantwortlichen gesetzlich übertragenen Aufgabe gefährdet wird.

Ob und inwieweit das Auskunftsrecht zu beschränken ist, muss jeweils im Einzelfall bewertet werden.

Unabhängig davon ist das Recht auf Akteneinsicht zu beurteilen, das im Einzelfall nach § 17 AVG zu bewerten ist.

Wie ist mit Auskunftsbegehren von BewerberInnen um ausgeschriebene Stellen und in damit zusammenhängenden Verfahren umzugehen?

Betroffene haben nach der DSGVO das Recht zu erfahren, welche ihrer personenbezogenen Daten das BKA verarbeitet, zu welchem Zweck etc. (siehe „Was ist Inhalt einer Auskunft gemäß § 15 DSGVO?“).

Die DSGVO gibt daher betroffenen BewerberInnen um eine Stelle nur das Recht, die sie betreffenden personenbezogenen Daten zu erfahren. Informationen über andere BewerberInnen dürfen nach der DSGVO nicht verlangt werden.

Wenn in Dokumenten Informationen über die Antragstellerin / den Antragsteller und auch andere Personen enthalten sind, würde die Übermittlung an die Antragstellerin / den Antragsteller in die Rechte und Freiheiten dieser Personen eingreifen, sie dürfen ihr / ihm daher nicht ohne entsprechende Schwärzungen übermittelt werden.

Auch die Übermittlung der Gründe für den Ausgang des Bewerbungsverfahrens greift potentiell in Rechte der anderen BewerberInnen ein. Außerdem besteht das Recht auf Auskunft gegenüber einem hoheitlich tätigen Verantwortlichen dann nicht, wenn durch die Erteilung dieser Auskunft die Erfüllung einer dem Verantwortlichen gesetzlich übertragenen Aufgabe gefährdet wird.

Der Übermittlung eines im Zuge eines Bewerbungsverfahrens erstellten Gutachtens, welches nur die Antragstellerin / den Antragssteller betrifft, an diese/n greift zwar nicht in die Rechte von MitbewerberInnen ein, kann aber im Einzelfall die Erfüllung der gesetzlich übertragenen Aufgabe gefährden.

Ob und inwieweit das Auskunftsrecht zu beschränken ist, muss daher jeweils im Einzelfall bewertet werden.

Konkrete Unterlagen, die der / dem Betroffenen regelmäßig zu übermitteln sind können z. B. sein: ihr / sein Lebenslauf, ihre / seine Bewerbung, ihre / seine Zeugnisse, ihre / seine persönlichen Dokumente.

Unabhängig davon ist das Recht auf Akteneinsicht zu beurteilen, das im Einzelfall nach § 17 AVG zu bewerten ist.

Wie kann man Auskunftsbegehren nach § 15 DSGVO allgemein von solchen nach dem Auskunftspflichtgesetz abgrenzen?

Zunächst können sich Auskunftsbegehren nach der DSGVO immer nur auf Informationen beziehen, die die personenbezogenen Daten der Antragstellerin / des Antragstellers betreffen.

Wird eine derartige Auskunft begehrt, so sind als Rechtsgrundlage dafür gemäß § 6 Auskunftspflichtgesetz die Bestimmungen der DSGVO und des DSG heranzuziehen:

§ 6 Auskunftspflichtgesetz

Soweit nach anderen Bundesgesetzen besondere Auskunftspflichten bestehen, ist dieses Bundesgesetz nicht anzuwenden.

Bezieht sich ein Auskunftsbegehren hingegen auf Informationen, die andere Personen als die Antragstellerin / den Antragsteller oder z. B. Vorgänge in der Behörde betreffen, ist nach dem Auskunftspflichtgesetz zu prüfen, ob und in welchem Umfang die Auskunft zu erteilen ist.

Wie ist mit Auskunftsbegehren nach § 15 DSGVO umzugehen, die eine völlig andere Auskunft begehren, als von dieser Bestimmung umfasst ist?

Es ist sinnvoll, derartige Anträge nicht einfach unbegründet zurückweisen, sondern wie ein „normales“ Auskunftsbegehren zu behandeln. In diesem Fall gilt die einmonatige Beantwortungsfrist nicht und die Antragstellerin / der Antragsteller wäre auch darauf hinzuweisen, dass sie / er kein Beschwerderecht bei der DSB hat.

In welcher Form sind Auskunftsbegehren nach § 15 DSGVO zu beantworten?

Die Beantwortung per E-Mail außerhalb der sicheren Bereiche des Bundesdienstes ist aus Sicherheitsgründen problematisch, bis zu einer anderen Lösung (Einrichtung eines Abholdienstes in elektronischer Form) aber wohl zu akzeptieren. Aus AVG-Sicht ist eine Beantwortung per E-Mail kein Problem, weil in diesem Fall keine Verfahren durchgeführt werden. Die Übermittlung von sensiblen Daten sollte außerhalb der sicheren Bereiche aber keinesfalls per E-Mail erfolgen.

9.3 Bilder von Personen

Wie ist DSGVO-konform vorzugehen, wenn ein/e PolitikerIn eine Schule besucht (Foto- und Videoaufnahmen)?

Sämtliche SchulleiterInnen werden vom BMBWF informiert und angewiesen, zu Schulbeginn eine generelle Zustimmung der Eltern einzuholen, dass ihre Kinder im Zuge von Schulveranstaltungen fotografiert werden und die Fotos auf die Internethomepage gestellt werden können. Wenn Eltern keine Zustimmung erteilen oder diese widerrufen, werden die Kinder auch nicht fotografiert.

Wenn es sich um besondere Veranstaltungen handelt, wie z.B. einen Besuch einer/eines Bundesministerin/Bundesministers oder des HBK in der Schule, wird für diesen Anlassfall eine gesonderte Einwilligung der Eltern eingeholt. Wenn das Kind das 14. Lebensjahr vollendet hat, kann es im Sinne des § 4 (4) DSGVO die Einwilligung selbst erteilen.

Nachdem die SchulleiterInnen dafür zuständig sind, die Einwilligungen einzuholen, schlägt der Datenschutzbeauftragte des BMBWF vor, dass die Ministerbüros im Zuge der Planungen eines Besuches in einer Schule dieser mitteilen, dass geplant ist, Fotos mit SchülerInnen zu machen und darüber zu informieren, wo diese veröffentlicht werden sollen und weiters zu fragen, ob die Eltern entsprechend gebrieft werden.

In diesem Zusammenhang sei erwähnt, dass das Recht am eigenen Bild laut Judikatur nicht mehr besteht, wenn das Bild mehr als 20 Personen umfasst.

Wie ist DSGVO-konform vorzugehen, wenn anlässlich von Veranstaltungen des Ressorts (z. B. Tag der offenen Tür) Foto-, Video- oder Tonaufnahmen von TeilnehmerInnen gemacht werden?

In jedem Fall sind die TeilnehmerInnen über eine Hinweistafel im Eingangsbereich darüber zu informieren, dass Foto- bzw. Video- bzw. Tonaufnahmen gemacht werden.

Empfohlen wird die Verwendung folgenden Textes, der jeweils für den Einzelfall zu adaptieren wäre:

Sehr geehrte Besucherin,
sehr geehrter Besucher!

Bei der heutigen Veranstaltung werden Fotos, Ton- und Filmaufnahmen gemacht. Verantwortlicher für die Datenverarbeitung ist das Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Tel.: +43 1 531 15-0, E-Mail: post@bka.gv.at.

Wir speichern und verarbeiten Daten ausschließlich im Sinne der EU-Datenschutz-Grundverordnung (DSGVO) und des österreichischen Datenschutzgesetzes idgF.

Zweck der Aufnahmen ist die interne Dokumentation der Veranstaltung und gegebenenfalls auch ihre Veröffentlichung.

Rechtsgrundlage für die Speicherung und Verarbeitung der Aufnahmen ist das Vorliegen eines öffentlichen Interesses an der Dokumentation gemäß Artikel 6 Abs. 1 lit. e DSGVO.

Mit der Teilnahme an der Veranstaltung stimmen Sie der Veröffentlichung der Fotos, Ton- und Filmaufnahmen zu, die im Rahmen der Veranstaltung entstehen. Wenn Sie mit der Veröffentlichung dieser Aufnahmen nicht einverstanden sind, ist Ihre Teilnahme an der Veranstaltung leider nicht möglich.

Die heute aufgenommenen Fotos, Ton- und Filmaufnahmen werden an folgende Empfänger weitergeleitet: ...

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

Laut Judikatur besteht kein Recht am eigenen Bild und es ist keine Zustimmung der / des Aufgenommenen erforderlich, wenn ein Gruppenfoto gemacht wird.

Anders sind Fälle zu beurteilen, in denen einzelne Personen fotografiert werden (z. B. am Tag der offenen Tür mit HBK oder dem / der BundesministerIn) und mit einer Veröffentlichung dieser Fotos zu rechnen bzw. eine solche nicht auszuschließen ist. In diesen Fällen ist eine Einverständniserklärung der Betroffenen erforderlich, da ein öffentliches Interesse an der Veröffentlichung von Fotos Einzelner nicht argumentierbar ist.

Wenn ein Kind fotografiert wird und eine Veröffentlichung möglich ist, ist eine Einwilligung erforderlich, und zwar vor Vollendung des 14. Lebensjahres durch die / den Erziehungsberechtigte/n.

Empfohlen wird die Verwendung folgender Texte, die jeweils für den Einzelfall zu adaptieren wären:

Zustimmungserklärung für Personen über 14 Jahre

Zustimmungserklärung für die Veröffentlichung von Foto- bzw. Videomaterial vom Tag der offenen Tür des Bundeskanzleramtes am ... Datenschutzrechtliche Informationen gemäß Art 13 DSGVO

Ich,, (Vor- und Zuname in Druckbuchstaben), geboren am (TT.MM.JJJJ), erteile hiermit meine Zustimmung zur Veröffentlichung der Foto- bzw. Videoaufnahmen, die beim heutigen Tag der offenen Tür von mir gemacht werden.

Verantwortlicher

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Telefon: +43 1 531 15-0, E-Mail: post@bka.gv.at.

Eine Veröffentlichung ist auf der Website des Bundeskanzleramtes, seinen Social-Media-Kanälen sowie gegebenenfalls in Printmedien vorgesehen.

Das Bundeskanzleramt speichert und verarbeitet Daten ausschließlich im Sinne 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 (DSGVO) sowie des durch das Datenschutz-Anpassungsgesetz novellierten Datenschutzgesetzes in der geltenden Fassung.

Die heute aufgenommenen Fotos werden archiviert. Daher ist keine Löschung vorgesehen.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

Wien, ... 2020

Unterschrift

Zustimmungserklärung für Personen unter 14 Jahre

Zustimmungserklärung für die Veröffentlichung von Foto- bzw. Videomaterial vom Tag der offenen Tür des Bundeskanzleramtes am ... Datenschutzrechtliche Informationen gemäß Art 13 DSGVO

Ich,, (Vor- und Zuname in Druckbuchstaben), erteile hiermit meine Zustimmung zur Veröffentlichung der Foto- bzw. Videoaufnahmen, die beim heutigen Tag der offenen Tür von meinem Kind (Ich bin erziehungsberechtigt), geboren am (TT.MM.JJJJ) gemacht werden.

Verantwortlicher

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Telefon: +43 1 531 15-0, E-Mail: post@bka.gv.at.

Eine Veröffentlichung ist auf der Website des Bundeskanzleramtes, seinen Social-Media-Kanälen sowie gegebenenfalls in Printmedien vorgesehen.

Das Bundeskanzleramt speichert und verarbeitet Daten ausschließlich im Sinne 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 (DSGVO) sowie des durch das Datenschutz-Anpassungsgesetz novellierten Datenschutzgesetzes in der geltenden Fassung.

Die heute aufgenommenen Fotos werden archiviert. Daher ist keine Löschung vorgesehen.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

Wien, ... 2020

Unterschrift

9.4 Datenschutz-Folgenabschätzung (DSFA)

Wann ist eine DSFA verpflichtend?

Zentrale Frage für die Entscheidung, ob eine DSFA durchzuführen ist, ist jene nach der Intensität des Eingriffs in die Rechte Betroffener.

Eine DSFA ist zwingend erforderlich, wenn ein Verarbeitungsvorgang voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Die DSGVO zählt beispielhaft folgende Fälle auf, in denen eine Datenschutzfolgenabschätzung „insbesondere“ erforderlich ist:

- Verarbeitung zur systematischen, umfassenden Bewertung persönlicher Aspekte (u. a. „Profiling“),
- umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten („sensible Daten“),
- Verarbeitung zur systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche (z. B. Videoüberwachung);

Die Notwendigkeit einer DSFA ergibt sich aber auch in anderen Fällen, wie

- Verarbeitung großer Mengen personenbezogener Daten,
- Verarbeitung betrifft eine große Anzahl an Personen,
- Ausübung der Rechte betroffener Personen ist erschwert,
- Einsatz neuer Technologien im großen Umfang im Rahmen der Verarbeitung;

Zu welchem Zeitpunkt ist die DSFA durchzuführen?

Die Pflicht zur Durchführung einer DSFA entsteht bereits vor Aufnahme des Verarbeitungsvorganges, und zwar für Verarbeitungen, die ab 25. Mai 2018 eingeführt werden.

Die DSFA ist kein einmaliger Vorgang, sondern sie ist bei neuen Risiken zu überprüfen und anzupassen.

Wer ist für die DSFA zuständig?

Verantwortlich für die Prüfung der Notwendigkeit einer DSFA (hohes Risiko?) sowie für ihre Durchführung ist jede Organisationseinheit für die dort eingesetzten Verarbeitungsvorgänge.

Sowohl die Entscheidung für oder gegen die Durchführung einer DSFA als auch ihre Durchführung selbst werden im Normalfall IT-Kenntnisse erfordern, sodass IT-Fachexperten hinzuziehen sind.

In welchen Schritten soll eine DSFA praktisch ablaufen?

1. Prüfung der Vorfrage – DSFA oder keine DSFA?

Als Vorfrage zur DSFA ist zu prüfen, ob ein Verarbeitungsvorgang voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat („Schwellwertanalyse“).

Die Datenschutzbehörde hat zunächst durch Verordnung jene Arten von Verarbeitungsvorgängen bestimmt, für die keine Datenschutz-Folgenabschätzung erforderlich ist (siehe Datenschutz-Folgenabschätzung-Ausnahmenverordnung, DSFA-AV, BGBl. II Nr. 108/2018).

In Folge wurden mit Verordnung der Datenschutzbehörde auch jene Arten von Verarbeitungsvorgängen festgelegt, für die jedenfalls eine Datenschutz-Folgenabschätzung durchgeführt werden muss (siehe Datenschutz-Folgenabschätzung-Verordnung, DSFA-V, BGBl. II Nr. 278/2018). Die genannten Verordnungen finden sich im Anhang dieses Handbuchs.

Die Entscheidung für oder gegen eine DSFA und die Gründe dafür sind schriftlich zu dokumentieren.

2. Vorbereitung der DSFA

Bei Entscheidung für die DSFA ist in Folge zu prüfen, ob der durch den Verarbeitungsvorgang bewirkte Eingriff in die Rechte Betroffener zum Erreichen der verfolgten Zwecke tatsächlich notwendig ist oder ob Alternativen zur Verfügung stehen, die weniger stark in die Rechte der Betroffenen eingreifen.

Gibt es solche Alternativen, so sind die Verarbeitungsvorgänge zu adaptieren, z. B. durch die (inhaltliche) Beschränkung der verarbeiteten Daten, die Beschränkung der Zugriffsberechtigungen oder den Einsatz anderer Technologien.

Nachdem der Verarbeitungsvorgang festgelegt wurde, ist die Rechtsgrundlage dafür zu dokumentieren.

3. Durchführung der DSFA

Die Risikoquellen für die Rechte und Freiheiten Betroffener müssen ermittelt werden. Eine wesentliche Frage ist, welche Personen warum motiviert sein könnten, die Daten unrechtmäßig zu nutzen und wie hoch die Wahrscheinlichkeit dafür ist.

Darauf aufbauend ist festzulegen, wie hoch das Risiko für die Rechte und Freiheiten Betroffener in Bezug auf Art, Umfang, Umstände und Zwecke der Verarbeitung ist. Für die Höhe des Risikos sind die Schwere der Beeinträchtigung der Rechte und Freiheiten, die Schwere potenzieller Schäden (physische, materielle, immaterielle) und die Eintrittswahrscheinlichkeit zu berücksichtigen.

Die ermittelten Risiken müssen durch geeignete Abhilfemaßnahmen eingedämmt werden, das sind insbesondere technisch-organisatorische Maßnahmen.

Verbleibende Restrisiken sind zu ermitteln und zu dokumentieren. Es ist festzulegen, wie mit diesen Restrisiken umgegangen wird.

Es ist ein DSFA-Bericht zu erstellen. Dieser ist Teil der Dokumentations- und Rechenschaftspflicht des Verantwortlichen.

Der DSFA-Bericht enthält:

- die (geplanten) Verarbeitungsvorgänge,
- ihre Zwecke,
- die Bewertung ihrer Notwendigkeit und Verhältnismäßigkeit,
- die Beschreibung der Risiken,
- die Bewertung der Risiken,
- die Abhilfemaßnahmen zur Risikoeindämmung,
- die Darstellung der Restrisiken samt Entscheidung über den Umgang mit diesen.

Ein Muster zur formal richtig aufgebauten Durchführung einer Datenschutz-Folgenabschätzung findet sich unter Punkt 11.9. dieses Handbuchs

4. Umsetzung der DSFA

Die erforderlichen technisch-organisatorischen Maßnahmen sind vor Einsatz der geplanten Datenverarbeitung umzusetzen, auf ihre Wirksamkeit zu testen sowie gegebenenfalls anzupassen.

In Folge ist auch die Wirksamkeit der umgesetzten Abhilfemaßnahmen zu dokumentieren.

5. Überprüfung der DSFA

Der Datenschutzbeauftragte prüft die DSFA abschließend und teilt das Ergebnis der Leitungsebene mit.

Wann muss eine neue DSFA durchgeführt werden?

Bei Änderung der Risiken ist die DSFA erneut durchzuführen.

Wie ist mit hohen Restrisiken umzugehen?

Wenn eine DSFA trotz technisch-organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Restrisiko ergibt, muss der Verantwortliche die Datenschutzbehörde informieren, die Empfehlungen abgeben kann. Die Datenschutzbehörde kann auch z. B. eine Anweisung aussprechen.

9.5 Datensicherheitsmaßnahmen

Können Betroffene von einem Verantwortlichen spezifische Datensicherheitsmaßnahmen verlangen?

Aus der DSGVO ist kein Recht abzuleiten, wonach eine betroffene Person spezifische Datensicherheitsmaßnahmen im Sinne von Art. 32 DSGVO von einem Verantwortlichen verlangen kann. Die betroffene Person hat also kein subjektives Recht auf Wahl einer spezifischen Datensicherheitsmaßnahme.

Der zur Sicherheit der Verarbeitung verpflichtete Verantwortliche kann die Datensicherheit auf mehrere Arten gewährleisten (vgl. den Bescheid der Datenschutzbehörde vom 13.9.2018, GZ DSB-D123.070/0005-DSB/2018, den Bescheid der Datenschutzkommission vom 2.8.2005, GZ K121.038/0006-DSK/2005, die Erkenntnisse des Bundesverwaltungsgerichts vom 11.7.2017, Zl. W214 2117640-1 und vom 20.4.2017, Zl. W214 2007810-1).

Ob der Verantwortliche hinsichtlich der Datensicherheit seine Verpflichtungen erfüllt hat, kann nur die Datenschutzbehörde im Rahmen eines amtswegig eingeleiteten Prüfverfahrens untersuchen (Art. 55 Abs. 1 iVm Art. 57 Abs. 1 lit. a und h DSGVO). Die Datenschutzbehörde kann den Verantwortlichen bei Vorliegen entsprechender Anhaltspunkte zur Einhaltung der Verordnung anweisen (Art. 58 Abs. 2 lit. d DSGVO).

9.6 Einladungen

Müssen AdressatInnen von Einladungen der Verarbeitung ihrer personenbezogenen Daten zustimmen?

Wenn für den laufenden Versand von Einladungen personenbezogene Daten eines bestimmten Personenkreises gesammelt, strukturiert gespeichert, aktualisiert etc. werden, so handelt es sich dabei um eine Verarbeitung personenbezogener Daten nach der DSGVO.

Die Datenverarbeitung muss daher einem konkret bestimmten Zweck dienen und auf einer geeigneten Rechtsgrundlage basieren.

Dabei ist der verfolgte Zweck auch ausschlaggebend dafür, ob eine aktive Einwilligung der Betroffenen erforderlich ist: Wenn als Rechtsgrundlage eine rechtliche Verpflichtung des Verantwortlichen in Betracht kommt, entfällt das Erfordernis einer Einwilligung. Daran ist etwa zu denken, wenn der verwendete Adressverteiler für Einladungen zu Arbeitsgruppen-Sitzungen, dienstlich erforderlichen Arbeitssitzungen, Vernetzungstreffen, Treffen mit MedienvertreterInnen u.ä. herangezogen wird. Wenn sich keine speziellere Rechtsgrundlage anbietet, kann in den genannten Fällen die Informations- und Koordinationstätigkeit der Bundesregierung nach dem Bundesministeriengesetz eine geeignete Rechtsgrundlage bieten.

Die Betroffenen der Datenverarbeitung sind einmalig über die Datenverarbeitung zu informieren, ohne dass eine aktive Zustimmung eingeholt werden muss.

Anders sind jene Fälle zu behandeln, in denen Einladungen zu Veranstaltungen nicht aus einer rechtlichen Verpflichtung des Verantwortlichen abgeleitet werden können wie z. B. sportliche und kulturelle Veranstaltungen. In diesen Fällen müssen Personen, die in entsprechenden Adressverteilern geführt werden, aktiv zustimmen.

Es werden sich in der Praxis diverse Graubereiche zeigen, in denen sich die Zuordnung nicht eindeutig ergibt. Ein maßgeblicher Entscheidungsparameter wird sein, ob die Einladungen in einem rein dienstlichen Kontext aller Beteiligten erfolgen (dann wird in der Regel eine gesetzliche Grundlage für die Einladung vorliegen) oder nicht.

9.7 E-Mails

Ist die E-Mail-Adresse ein personenbezogenes Datum?

Ja, die E-Mail-Adresse ist ein personenbezogenes Datum, wenn in irgendeiner Form die Zuordnung zu einer bestimmten Person möglich ist, was regelmäßig auch bei Postfach-Adressen der Fall ist.

Wie ist der Versand von E-Mails DSGVO-konform zu gestalten?

Werden im dienstlichen Betrieb E-Mails versandt, so muss das, um DSGVO-konform zu sein, auf einer Rechtsgrundlage beruhen. Dabei ist nicht der Versand des E-Mails isoliert zu betrachten, sondern der gesamte Vorgang.

Die Zulässigkeit der Datenverarbeitung ergibt sich im behördlichen Bereich häufig daraus, dass eine gesetzliche Verpflichtung des Verantwortlichen besteht. Ein Beispiel dafür ist die Bearbeitung von Anfragen und Anträgen von BürgerInnen. Diese sind über die Datenverarbeitung zu informieren (siehe Beispiel 1). Wenn die Erledigung der Anfrage oder des Antrages nicht zeitnah erfolgt, ist eine Zwischenerledigung erforderlich.

Der Austausch über E-Mail zwischen KollegInnen im Bereich des Bundes ist erforderlich zur Erledigung der dienstlichen Aufgaben und beruht daher ebenfalls auf der gesetzlichen Verpflichtung des Verantwortlichen und außerdem den Dienstpflichten der Bediensteten, die sich aus dem Dienstvertrag ergeben. In der im ESS auffindbaren Datenschutzerklärung (für alle Bundesbediensteten) ist verankert, dass die Kontaktdaten der Bediensteten zum Zweck der Personalverwaltung verarbeitet und im Telefonverzeichnis / Geschäftseinteilung veröffentlicht sind. Damit wurden die Bundesbediensteten DSGVO-konform informiert.

Zum E-Mail-Versand an Nicht-Bundesbedienstete z.B. im Rahmen von Arbeitsgruppen, Kommissionen, an Journalisten etc., ist zu sagen, dass es Sache von deren jeweiligem Dienstgeber ist, sie zu informieren, dass ihre Kontaktdaten für dienstliche Zwecke verarbeitet und veröffentlicht werden. Eine gesonderte Information an diese Personen bundesseitig ist erforderlich, wenn E-Mail-Verteiler, sonstige Kontaktlisten etc. erstellt und diese Verteiler oder Listen in Folge genutzt werden (siehe Beispiel 2). Einzelne E-Mails fallen nicht unter diese Verpflichtung.

Beispiel 1:

Ein Bürger richtet eine Anfrage an das Bürgerservice des BKA. Im Antwortschreiben oder – wenn dieses nicht zeitnah geschickt wird in einer Zwischenerledigung – ist der anfragende Bürger entsprechend der DSGVO zu informieren. Folgendes Muster enthält die nach der DSGVO wesentlichen Elemente:

Unsere Zusendung erfolgt auf der Rechtsgrundlage des ... (z.B.:) Bundesministerien-gesetzes 1986, BGBl. Nr. 76/1986 idgF, Teil 2 der Anlage zu § 2 (Informationstätigkeit der Bundesregierung). Hierfür speichern wir Ihren (z.B.) Vor- und Zunamen, Ihre E-Mail-Adresse und ggf. sonstige personenbezogene Daten, die Sie im Zuge Ihres Schreibens an das Bundeskanzleramt übermitteln. Ihre Daten werden nach der gesetzlichen Aufbewahrungsfrist für elektronische Akten im Bundeskanzleramt (Skartierungsfrist 10 Jahre) gelöscht.

Für die zutreffende Beantwortung Ihres Anliegens werden relevante Auszüge Ihrer Daten (insbesondere Vor- und Zuname, E-Mail, Anschrift und ggf. Telefonnummern) – wenn organisationstechnisch erforderlich – an Dienststellen des Bundeskanzleramts (die Kabinette und jeweiligen Fachabteilungen) weitergeleitet, sowie ggf. an andere Bundesministerien übermittelt.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

Beispiel 2:

Die Presseabteilung führt einen laufenden E-Mail-Verteiler für JournalistInnen. Diese sind entsprechend der DSGVO zu informieren. Folgendes Muster enthält die nach der DSGVO wesentlichen Elemente:

Datenverarbeitung im Rahmen eines E-Mail-Verteilers des Bundeskanzleramtes Datenschutzrechtliche Informationen gemäß Art 13 DSGVO

Verantwortlicher

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Telefon: +43 1 531 15-0,
E-Mail: post@bka.gv.at

Wir speichern und verarbeiten Daten ausschließlich im Sinne 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 (DSGVO) sowie des österreichischen Datenschutzgesetzes, BGBl. I Nr. 165/1999, idgF.

Die Verarbeitung Ihrer personenbezogenen Daten, konkret Ihrer E-Mail-Adresse, erfolgt zum Zweck ... auf folgender Rechtsgrundlage: Informations- und Koordinationstätigkeit der Bundesregierung gemäß Teil 2 der Anlage zu § 2 Bundesministeriengesetz 1986 (BMG), idgF.

Sie können den Bezug unserer Aussendungen jederzeit stornieren. Senden Sie Ihre Stornierung an folgende E-Mail-Adresse: ...@bka.gv.at. Wir löschen anschließend umgehend Ihre Daten im Zusammenhang mit dem angeführten Zweck.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

Dürfen E-Mails so verschickt werden, dass die E-Mail-Adressen aller EmpfängerInnen sichtbar sind?

Das hängt von den genauen Umständen ab. Wenn die Weitergabe der E-Mail-Adressen absichtlich erfolgt und nach Artikel 6 DSGVO zulässig ist, so ist diese Weitergabe zulässig. Das ist etwa der bei internen E-Mails oder zur internen Koordination von Projekten der Fall, wenn die Absenderin / der Absender bezweckt, dass Antworten von EmpfängerInnen wieder alle Personen im E-Mail-Verteiler erreichen. Hier kommen bundesintern gesetzliche und dienstvertragliche Grundlagen in Frage.

In allen anderen Fällen empfiehlt es sich, die Empfängerliste zu verbergen. Das ist möglich, indem die Absenderin / der Absender im Outlook sich selbst als EmpfängerIn eingibt und die weiteren EmpfängerInnen unter BCC (Blind Copy) setzt.

9.8 Verhängung von Geldbußen wegen Verstoßes gegen die DSGVO

Kann die Datenschutzbehörde über eine verantwortliche Behörde Geldbußen verhängen?

Nein, die DSGVO und das DSG sehen keine Verhängung von Geldbußen über Behörden vor.

Gilt das nur für hoheitliches Handeln oder auch für Verstöße gegen die DSGVO im Bereich der Privatwirtschaftsverwaltung?

Ein Verantwortlicher des öffentlichen Bereichs, wie der Leiter einer Behörde, ist auch dann dem öffentlichen Bereich zuzuordnen, wenn er im Rahmen der Privatwirtschaftsverwaltung handelt.

Somit kann gegen eine Behörde auch dann keine Geldbuße verhängt werden, wenn sie im Rahmen der Privatwirtschaftsverwaltung handelt.

9.9 Lösungsbegehren gemäß Artikel 17 DSGVO

Wann kann die Löschung von personenbezogenen Daten verlangt werden?

In folgenden Fällen besteht grundsätzlich ein Recht auf Löschung personenbezogener Daten:

1. Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
2. Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
3. Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein (die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt) und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.

4. Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
5. Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
6. Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben (Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird).

Welche Ausnahmen erlauben, dass dem Löschungsbegehren nicht gefolgt werden muss?

Wenn die Verarbeitung aus einem der folgenden Gründe erforderlich ist, muss dem Löschungsbegehren nicht gefolgt werden:

1. zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
2. zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
3. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3 (Verarbeitung besonderer Kategorien personenbezogener Daten);
4. für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das Recht auf Löschung voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt;
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Wie können Anträge auf Löschung von digitalen Unterlagen beantwortet werden, wenn diese Unterlagen in einem elektronischen Aktensystem gespeichert sind?

Es wird die Verwendung des folgenden Antwortmusters (hier: für den ELAK) empfohlen. Bei Verwendung eines anderen elektronischen Aktensystems ist dieses Muster entsprechend zu adaptieren:

Gemäß § 12 Bundesministeriengesetz, BGBl. Nr. 76/1986 idgF, ist die formale Behandlung der von den Bundesministerien zu besorgenden Geschäfte von der Bundesregierung in einer für alle Bundesministerien einheitlichen Kanzleiordnung (Büroordnung) festzulegen. Desgleichen sind die notwendigen Maß-

nahmen zum Schutz personenbezogener Daten anzuordnen. Aufgrund dieser Gesetzesbestimmung erging die Büroordnung 2004, die in § 25 festlegt, dass die Aufbewahrungsfrist des elektronischen Aktes grundsätzlich mit dem Ablauf des zehnten Kalenderjahres nach dem letzten Bearbeitungsvorgang festgesetzt wird. Gemäß § 26 Abs. 2 ist zudem das Österreichische Staatsarchiv vor einer beabsichtigten Vernichtung von Akten zu verständigen, um diesem die Gelegenheit zu geben, solche Akten zu sichten und bei Bedarf zu übernehmen.

Ihrem Antrag auf Löschung der digitalen Schriftstücke und Unterlagen, die im ELAK verarbeitet wurden, kann daher nicht entsprochen werden, weil die mindestens 10-jährige bzw. bei Archivzwecken darüber hinaus gehende Speicherung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der das Bundeskanzleramt aufgrund des Bundesministeriengesetzes und der Büroordnung unterliegt. Darüber hinaus widerspricht der Löschung, dass die Verarbeitung zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, erforderlich ist (Art 17 Abs.3 lit. b) DSGVO).

Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Datenschutzbehörde beschweren. In Österreich ist die Datenschutzbehörde zuständig.

Kann die Löschung auf Grund fehlender Informationen nach Artikel 14 DSGVO verlangt werden?

Die Datenschutzbehörde (DSB) hat dazu in ihrem Bescheid vom 30.11.2018, GZ: DSB-D122.954/0010-DSB/2018, entschieden:

Im gegenständlichen Fall verlangte der Beschwerdeführer die Löschung von Einträgen über ein Insolvenzverfahren in der Konsumenten- und Warenkreditevidenz, da der Beschwerdegegner ihn über diese Einträge nicht informiert hatte und die Gläubigerforderung darüber hinaus bereits zur Gänze beglichen worden war.

Die DSB gab der Beschwerde statt, da aufgrund des in Art. 5 Abs.1 lit. a DSGVO verankerten Grundsatzes von Treu und Glauben eine entsprechende Information des Beschwerdeführers gemäß Art. 14 DSGVO erforderlich ist. Ansonsten sind die Einträge rechtswidrig.

Die Rechtswidrigkeit ergab sich zusätzlich aus dem Grund, dass die eingetragenen Informationen auch nicht richtig waren - es entstand der Eindruck, dass ein Insolvenzverfahren eröffnet und abgeschlossen worden war, wohingegen ein solches mangels kostendeckenden Vermögens gar nicht eröffnet wurde.

Der Bescheid ist nicht rechtskräftig.

Haben Betroffene ein Recht auf „partielle“ Löschung?

Die Datenschutzbehörde (DSB) hat dazu in ihrem Bescheid vom 5.12.2018, GZ: DSB-D123.211/0004-DSB/2018, entschieden:

Im gegenständlichen Fall behauptete der Beschwerdeführer, in seinen Rechten auf Geheimhaltung und Löschung verletzt worden zu sein, weil der Beschwerdegegner seinem partiellen Löschantrag nicht entsprochen hat. Stattdessen wurden die gesamten personenbezogenen Daten des Beschwerdeführers gelöscht.

Die DSB stellte fest, dass (nach der anzuwendenden Rechtslage, somit § 27 Abs. 1 Z 2 DSG 2000) dem Betroffenen freistehen muss, als „Minus“ auch die Löschung bloß eines Teiles der Daten zu begehren (partielles Löschrrecht). Ist ein Verantwortlicher der Ansicht, dass einem partiellen Löschrbegehren nicht entsprochen werden kann, sind die dafür maßgeblichen Gründe dem Betroffenen nachvollziehbar und fristgerecht mitzuteilen.

Die Vorgehensweise der Löschung der gesamten personenbezogenen Daten des Beschwerdeführers widerspricht der Verwendung von Daten nach Treu und Glauben und verletzt den Beschwerdeführer durch die überschießende Löschung auch in seinem Recht auf Löschung nach § 1 Abs. 3 Z 2 iVm § 27 DSG 2000.

Der Bescheid ist nicht rechtskräftig.

9.10 Übermittlung an Drittstaaten und internationale Organisationen

Unter welchen Voraussetzungen ist die Übermittlung personenbezogener Daten an ein Drittland zulässig?

Es muss eine zweistufige Prüfung stattfinden: Einerseits muss die innerhalb der EU stattfindende Datenverarbeitung nach der DSGVO zulässig sein, andererseits müssen bei der Übermittlung der Daten die (zusätzlichen) Bestimmungen von Kapitel V der DSGVO eingehalten werden.

Grundsätzlich muss vorab eine Genehmigung des Datentransfers durch die Datenschutzbehörde eingeholt werden. Für den Bundesbereich wichtige Ausnahmen von diesem Grundsatz sind v.a.:

- Es gibt einen Angemessenheitsbeschluss der Europäischen Kommission. Ein solcher existiert bis auf Widerruf für die Schweiz, Kanada, Andorra, Argentinien, Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Uruguay und jene US-Unternehmen, die sich zu den „Safe Harbor“-Bestimmungen verpflichtet haben. Bis auf Widerruf durch die EU-Kommission sind Datentransfers in die genannten Drittstaaten / an die genannten Unternehmen ohne weitere formale Voraussetzungen zulässig. Nach der DSGVO kann die EU-Kommission künftig auch für ein Gebiet, einen Sektor und internationale Organisationen Angemessenheitsbeschlüsse fassen. Die Veröffentlichung der Angemessenheitsbeschlüsse erfolgt im Amtsblatt der EU und auf ihrer Website.

- Der Verantwortliche oder der Auftragsverarbeiter hat geeignete Garantien vorgesehen. Im Behördenbereich sind insbesondere rechtsverbindliche Verwaltungsvereinbarungen angesprochen, z. B. eine gemeinsame Absichtserklärung, mit der den betroffenen Personen durchsetzbare und wirksame Rechte eingeräumt werden. Möglich ist auch der Einsatz von Standarddatenschutzklauseln (erlassen von der Kommission oder angenommen von der Aufsichtsbehörde und genehmigt von der Kommission). Diese können individuell ergänzt werden, wofür aber die Genehmigung der Aufsichtsbehörde erforderlich ist.
- Die betroffene Person hat in die Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die möglichen Risiken unterrichtet wurde.
Für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen, gilt diese Ausnahme nicht.
- Die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.
- Die Übermittlung ist zur Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung vorvertraglicher Maßnahmen auf Antrag der betroffenen Person erforderlich.
Für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen, gilt diese Ausnahme nicht.
- Die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person vom Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrages erforderlich. Für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen, gilt diese Ausnahme nicht.
- Die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig. Die Erwägungsgründe nennen als Beispiele den internationalen Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten.
Das öffentliche Interesse muss nach Unionsrecht oder nach dem Recht der Mitgliedstaaten vorliegen, nicht nach dem Recht der Drittländer.
- Die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben.
- Die Übermittlung erfolgt aus einem öffentlich zugänglichen Register, sei es, dass die Daten der gesamten Öffentlichkeit bereitgestellt werden oder Personen, die

ein berechtigtes Interesse haben. Die Übermittlung ist zulässig, wenn im Einzelfall die Voraussetzungen für die Einsichtnahme gegeben sind.

- Wenn keine der bisher genannten Ausnahmen greift:
Die Übermittlung erfolgt nicht wiederholt, betrifft nur eine begrenzte Zahl von betroffenen Personen, ist für die Wahrung zwingender berechtigter Interessen des Verantwortlichen erforderlich, die Interessen und Freiheiten der betroffenen Person überwiegen nicht, der Verantwortliche beurteilt alle Umstände der Datenübermittlung und sieht geeignete Garantien vor, setzt die Aufsichtsbehörde in Kenntnis und unterrichtet die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen (zusätzlich zur allgemeinen Informationspflicht gemäß Artikel 13 und 14 DSGVO). Für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen, gilt diese Ausnahme nicht.

Unter welchen Voraussetzungen ist die Übermittlung personenbezogener Daten an eine internationale Organisation zulässig?

Es gilt grundsätzlich das unter der FAQ „Unter welchen Voraussetzungen ist die Übermittlung personenbezogener Daten an ein Drittland zulässig?“ Gesagte.

Allerdings existiert für internationale Organisationen derzeit kein Angemessenheitsbeschluss der Europäischen Kommission, sodass – wenn die weiteren Ausnahmen, die eine Übermittlung erlauben, nicht vorliegen – vorab eine Genehmigung des Datentransfers durch die Datenschutzbehörde eingeholt werden muss.

Im Hinblick auf Übermittlungen an europäische Organisationen (z. B. im Rahmen der EU-Präsidentschaft) kann bei entsprechender Nachvollziehbarkeit auf wichtige Gründe des öffentlichen Interesses Bezug genommen werden.

Die Erwägungsgründe nennen als Beispiele für das Vorliegen eines wichtigen öffentlichen Interesses den internationalen Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten.

Das öffentliche Interesse muss nach Unionsrecht oder Recht der Mitgliedstaaten vorliegen. Sofern kein hoheitliches Handeln vorliegt, kann auch mit Einwilligungen vorgegangen werden.

9.11 Verzeichnis von Verarbeitungstätigkeiten gemäß Artikel 30 DSGVO

Warum ist ein Verarbeitungsverzeichnis zu führen?

Die Datenschutz-Grundverordnung (DSGVO), die am 25. Mai 2018 in Kraft getreten ist, verpflichtet den Verantwortlichen (den Bundeskanzler bzw. den / die BundesministerIn) ein „Verzeichnis von Verarbeitungstätigkeiten“ zu erstellen und zu führen.

Das Verarbeitungsverzeichnis ist wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dem Verantwortlichen beim Nachweis der Einhaltung der DSGVO. Es ist auf Anfrage der Aufsichtsbehörde (Datenschutzbehörde) unverzüglich zur Verfügung zu stellen.

Die Erstellung des Verarbeitungsverzeichnisses stellt **eine** Dokumentationspflicht nach der DSGVO dar. Hinzu kommen z. B. das Vorhandensein von Einwilligungen und Datenschutz-Folgenabschätzungen.

Wie ist das Verarbeitungsverzeichnis zu führen?

Zur einheitlichen Führung des Verarbeitungsverzeichnisses wurde für das Bundeskanzleramt ein elektronisches tool („DataReg“) entwickelt.

Die Verantwortung für die Befüllung fällt in die Zuständigkeit der LeiterInnen der einzelnen Organisationseinheiten. Die Inhalte des Verarbeitungsverzeichnisses gemäß DSGVO sind:

Name und Kontaktdaten des Verantwortlichen und der / des Datenschutzbeauftragten

(nicht von den Organisationseinheiten zu befüllen)

Bezeichnung der Verarbeitungstätigkeit

Einzutragen sind alle ganz oder teilweise automatisierten Verarbeitungen und nicht-automatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Für jede einzelne Verarbeitungstätigkeit ist eine Beschreibung gemäß Artikel 30 DSGVO zu erstellen (siehe dazu die nachfolgenden Punkte).

Unter Verarbeitungstätigkeit wird ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden.

Ändert sich der Zweck einer Verarbeitung, so handelt es sich dabei grundsätzlich um eine eigene Verarbeitungstätigkeit. Bei einer nur geringfügigen Änderung des Zwecks muss geprüft werden, ob eine bereits bestehende Beschreibung einer Verarbeitungstätigkeit lediglich anzupassen ist, oder ob eine vollständige neue Beschreibung anzufertigen ist.

Zwecke der Verarbeitung

Für jede Verarbeitung ist / sind vorab der Zweck / die Zwecke festzulegen.

Je Beschreibung einer Verarbeitungstätigkeit ist / sind der Verarbeitungszweck / die Verarbeitungszwecke zu dokumentieren.

Die Zwecke müssen eindeutig und so aussagekräftig sein, dass die Aufsichtsbehörde die Angemessenheit der getroffenen Schutzmaßnahmen und die Zulässigkeit der Verarbeitung vorläufig einschätzen kann.

Als Beispiele sind zu nennen:

- Personalaktenführung
- Abrechnung der Bezüge
- Arbeitszeiterfassung
- Nutzungsprotokollierungen IT / Internet / E-Mail
- Bewerbungsverfahren
- Telefondatenerfassung
- Videoüberwachung
- Beschaffung / Einkauf
- Buchhaltung
- Antragsbearbeitung
- Bürgerinformationssysteme
- Anlegen / Verwalten diverser Listen (Einladungen, Newsletter, Versand Informationsmaterial)

Betroffenengruppe

Als Beispiele sind zu nennen:

- Beschäftigte
- Anfragende im Bereich der Abteilung X / des Referats X / Y
- AntragstellerInnen im Bereich der Abteilung X / des Referats X / Y
- BezieherInnen der Newsletters X
- TeilnehmerInnen an der Veranstaltung X

Datenkategorien

Für die jeweilige Betroffenengruppe sind die verarbeiteten Datenkategorien anzuführen, z. B. für die Betroffenengruppe „Beschäftigte“:

- Mitarbeiter-Stammdaten
- Bewerbungen mit Qualifikationsdaten, Tätigkeiten etc.
- Arbeitszeugnisse mit Adressdaten, Leistungsdaten, Beurteilungsdaten etc.
- Ermahnungen mit Daten zum Arbeitsverhalten
- ärztliche Untersuchungen
- Videoüberwachung an Arbeitsplätzen

Die Verarbeitung besonderer Kategorien von Daten ist gesondert zu beschreiben. Es ist empfehlenswert, hinsichtlich der einzelnen Datenkategorien laufende Nummern zu vergeben, um eine Zuordnung zu weiteren Angaben im Verarbeitungsverzeichnis zu ermöglichen (z. B. konkrete Löschregeln).

Empfänger

Zu beschreiben sind die Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen. Es sind darunter auch „Zugriffsberechtigte“ zu verstehen, die

nicht namentlich anzuführen sind, aber über eine Rollen- oder Funktionsbeschreibung eindeutig bestimmbar sein müssen.

Hinsichtlich der Abrechnung der Bezüge von Bediensteten sind beispielsweise zu nennen:

- Banken
- Sozialversicherungsträger
- Finanzämter
- behördeninterne Datenempfänger
- Gläubiger

Übermittlung in Drittländer / an internationale Organisationen

Es ist das betroffene Drittland / die betroffene internationale Organisation anzugeben. Wenn keine Übermittlung stattfindet, ist das ebenfalls zu vermerken.

Empfänger in Drittländern und internationalen Organisationen sind gesondert konkret zu benennen.

Löschfrist

In dieser Rubrik sind die vorgesehenen Fristen für die Löschung der einzelnen Datenkategorien anzugeben.

Ausschlaggebend ist der Zweck der Datenerhebung und der Datennutzung. Zu löschen ist grundsätzlich unverzüglich nach Erfüllung des Zwecks, es sei denn es gibt gesetzliche Aufbewahrungspflichten oder vom Verantwortlichen entsprechend den Grundsätzen der DSGVO festgelegte Löschfristen.

Ein allgemeiner Hinweis auf Aufbewahrungspflichten genügt nicht, es sind präzise Angaben erforderlich.

Technische und organisatorische Maßnahmen

Angesprochen sind Maßnahmen, die hinsichtlich der Sicherheit der Verarbeitung getroffen werden ebenso wie Maßnahmen zur Gewährleistung von Betroffenenrechten.

Dazu zählen die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Gewährleistung der Integrität und Vertraulichkeit sowie der Verfügbarkeit und Belastbarkeit der Systeme und Dienste, die Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu ihnen nach einem physischen oder technischen Zwischenfall sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen.

In Bezug auf die Standardanwendungen erfolgt ein Verweis auf das allgemeine Sicherheitskonzept im BKA, sodass nur Abweichungen davon für die jeweilige Verarbeitungstätigkeit extra angeführt werden müssen. In diesem Fall ist eine allgemeine, einfach nachvollziehbare Beschreibung der getroffenen Maßnahmen aufzunehmen. Soweit innerhalb einer Verarbeitungstätigkeit hinsichtlich der Personen- bzw. Datenkategorien differenziert wird, sind auch die entsprechenden Maßnahmen differenziert darzustellen.

Ansprechpartner

In dieser Rubrik ist der Ansprechpartner in der jeweils zuständigen Organisationseinheit für die Verarbeitung anzuführen.

Rechtliche Grundlage

Gemeint ist die konkrete Rechtsgrundlage der Verarbeitung bezogen auf den festgelegten Zweck.

In Frage kommen eine gesetzliche Verpflichtung des Verantwortlichen, die Erforderlichkeit der Verarbeitung zur Vertragserfüllung, die Einwilligung der / des Betroffenen, ein öffentliches Interesse oder lebenswichtige Interessen.

allfälliger Auftragsverarbeiter

In dieser Rubrik sind vom BKA verschiedene Auftragsverarbeiter anzugeben, die im Auftrag des Verantwortlichen Verarbeitungen durchführen. Das kann ein anderes Ressort sein oder auch ein externer Dienstleister.

Die Befüllung durch die einzelnen Organisationseinheiten ist auch hier nur erforderlich, soweit es sich nicht um eine Standardanwendung handelt.

Was ist nach Fertigstellung des Verarbeitungsverzeichnisses zum Stichtag 25. Mai 2018 zu beachten?

Nachdem das Verarbeitungsverzeichnis zum Stichtag 25. Mai 2018 vollständig erstellt wurde, ist es nun wichtig, dieses laufend einem „Praxistest“ zu unterziehen.

Zunächst ist das Verarbeitungsverzeichnis ein Dokument, das regelmäßig zu ergänzen und zu adaptieren ist, wenn neue Verarbeitungstätigkeiten aufgenommen werden oder bestehende Verarbeitungstätigkeiten sich ändern.

Ob bei Änderungen von bestehenden Verarbeitungstätigkeiten Anpassungen der Einträge ausreichen oder neue Einträge erforderlich sind, hängt von der Intensität der Änderungen ab und muss im Einzelfall beurteilt werden.

Ändert sich der Zweck einer Verarbeitung, so handelt es sich dabei grundsätzlich um eine eigene Verarbeitungstätigkeit. Bei einer nur geringfügigen Änderung des Zwecks muss geprüft werden, ob eine bereits bestehende Beschreibung einer Verarbeitungstätigkeit lediglich anzupassen ist, oder ob eine vollständige neue Beschreibung anzufertigen ist. Neu hinzukommende Verarbeitungstätigkeiten und Änderungen bestehender Verarbeitungstätigkeiten wirken sich auf die Betroffenenrechte aus. Werden aufgrund der Änderung z. B. personenbezogene Daten nun an (ressortexterne) Stellen übermittelt, die bisher nicht eingebunden waren, müssen parallel zur Änderung des Verarbeitungsverzeichnisses auch die Betroffenen entsprechend informiert oder (wenn keine andere Rechtsgrundlage vorliegt) ihre Zustimmung eingeholt werden.

Die Einträge in das Verarbeitungsverzeichnis und die Dokumente, die zur Wahrung der Betroffenenrechte erstellt werden (Informationsschreiben oder Zustimmungserklärungen) müssen jedenfalls inhaltlich übereinstimmen. Wird z. B. im Verarbeitungsverzeichnis als rechtliche Grundlage der Verarbeitung das Bundesministeriengesetz angeführt,

soll nicht gleichzeitig in einem Formular die Einwilligung der Betroffenen eingeholt werden, da beide Rechtsgrundlagen grundsätzlich nicht gleichzeitig zutreffen können.

Es können sich in der Praxis diesbezügliche Probleme insbesondere dort ergeben, wo die Einträge im Verarbeitungsverzeichnis sehr allgemein gehalten wurden. Das betrifft vor allem die Rechtsgrundlage und die Löschfristen.

Beispiel:

Im Verarbeitungsverzeichnis wurde die Verarbeitungstätigkeit „E-Mail-Verteiler für Veranstaltungen, Konferenzen, Arbeitssitzungen“ aufgenommen. Als Rechtsgrundlage wird eine das Ressort betreffende Bestimmung des Bundesministerengesetzes angeführt, bezüglich der Löschung wird auf die ELAK-Skartierungsfrist hingewiesen.

Als später ein E-Mail-Verteiler für eine Veranstaltung erstellt wird, die sich an diverse Personen auch außerhalb des Bundesdienstes richtet, ist nach rechtlicher Überprüfung davon auszugehen, dass die aktive Zustimmung der Betroffenen zur Datenverarbeitung eingeholt werden muss.

Da der konkrete Einladungsvorgang nicht im ELAK veraktet wird, ist in den Zustimmungserklärungen ein Verweis auf die allgemeine Skartierungsfrist nicht zutreffend. Die Betroffenen sind daher in der Zustimmungserklärung auch über die konkreten Löschregeln zu informieren (z. B. „nach einer Nachbereitungszeit von...“ plus Hinweis auf die Möglichkeit, die Zustimmung zu widerrufen).

Parallel ist das Verarbeitungsverzeichnis zu korrigieren, indem je nach Thema der E-Mail-Verteiler im Bereich der Rechtsgrundlage und der Löschfristen differenziert wird (z. B. Rechtsgrundlage „BMG“ für Einladungen zu Treffen der Arbeitsgruppen X und Y; Rechtsgrundlage „Zustimmung“ bei Einladungen zu Veranstaltungen mit einem weit gefächerten TeilnehmerInnenkreis; differenzierte Darstellung, für welche Fälle welche Löschregeln gelten).

Bei Verwendung von DataReg können die nötigen Differenzierungen durch entsprechende Befüllung der freien Textfelder vorgenommen werden.

Wenn durch zu viele erforderliche Differenzierungen die Übersichtlichkeit verloren geht, ist es besser, gesonderte Verarbeitungstätigkeiten im Verarbeitungsverzeichnis anzulegen.

Da der Verantwortliche die Erfüllung seiner Dokumentationspflichten jederzeit der Datenschutzbehörde nachweisen können muss, ist der Fokus auf eine übersichtliche und rasch abrufbare Form der Darstellung zu legen.

10 Beispiele aus der Praxis

1. Sie verfügen über eine Datenbank, die Namen und E-Mail-Adressen von Personen enthält, die sich für den Bezug eines Newsletter Ihrer Abteilung angemeldet haben. Von diesen Personen wurde die Einwilligung zur Datenverarbeitung zu diesem Zweck eingeholt. Nun beabsichtigen Sie, die betroffenen Personen zu einer Veranstaltung einzuladen. Diese Verarbeitung ist ohne die ausdrückliche Einwilligung der BezieherInnen des Newsletter unzulässig, da der Zweck nicht mit dem ursprünglichen Zweck der Datenverarbeitung vereinbar ist. Um der DSGVO zu entsprechen, muss eine Einwilligung freiwillig erfolgen, in informierter Weise geschehen und für einen bestimmten Zweck gegeben werden, in der Erklärung muss auf alle Gründe für die Verarbeitung unmissverständlich hingewiesen werden, die Einwilligung muss ausdrücklich sein und durch eine bestätigende Handlung erfolgen (zum Beispiel ein elektronisches Kontrollkästchen, das die Person online ausdrücklich bestätigen muss, oder eine Unterschrift auf einem Formular), die Erklärung muss eine klare und einfache Sprache verwenden und eindeutig wahrnehmbar sein und es muss möglich sein, die Einwilligung zu widerrufen und der / dem Betroffenen diese Möglichkeit erklärt werden.
2. Um einen Newsletter versenden zu können, benötigen Sie Name und E-Mail-Adresse der BezieherInnen des Newsletter. Diese personenbezogenen Daten dürfen (bei Zustimmung der betroffenen Personen) erhoben, gespeichert und verwendet werden. Das Geburtsdatum darf aber nicht verarbeitet werden, da es sich dabei um keine Information handelt, die zum Versand des Newsletter benötigt wird. Wenn personenbezogene Daten erforderlich sind, sollten diese dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“). Es obliegt Ihrer Verantwortung, zu bewerten, wie viele Daten erforderlich sind, und zu gewährleisten, dass nicht relevante Daten nicht erhoben werden.
3. Sie verfügen über eine Datenbank, in der über mehrere Jahre Name, E-Mail-Adresse und Funktion im Unternehmen von VertreterInnen der Wirtschaft gesammelt werden, die bereits an Veranstaltungen Ihrer Abteilung teilgenommen haben. Zweck dieser Datensammlung ist der Versand von Einladungen für passende Veranstaltungen in der Zukunft. Auf Grund des Inkrafttretens der DSGVO müssen Sie von diesen Personen die nachweisliche Zustimmung zur weiteren Verwendung ihrer Daten für diesen Zweck einholen. Die Daten müssen regelmäßig aktualisiert werden und es muss eine Löschfrist festgelegt werden, die sachlich nachvollziehbar ist und die dem Betroffenen im Rahmen der Einwilligung auch mitgeteilt wird (z.B. Löschung, wenn die betroffene Person das verlangt). Daten müssen so kurz wie möglich gespeichert werden. Sie müssen zudem sicherstellen, dass die aufbewahrten Daten sachlich richtig und auf dem neuesten Stand sind.

4. Sie führen eine Datenbank, die erforderliche personenbezogene Daten der Mitglieder einer Kommission enthält. Diese Daten werden (wie die Mehrheit der von Behörden gespeicherten personenbezogenen Daten) auf der Grundlage einer rechtlichen Verpflichtung verarbeitet. Im Behördenbereich kommen als Handlungsgrundlagen auch die Wahrnehmung von Aufgaben, die im öffentlichen Interesse liegen, oder die Ausübung öffentlicher Gewalt, die der betreffenden Behörde übertragen wurde, in Frage. Bei der Verarbeitung personenbezogener Daten müssen Behörden wesentliche Grundsätze beachten, zum Beispiel faire und rechtmäßige Verarbeitung, Zweckbindung und Datenminimierung. Vor der Verarbeitung personenbezogener Daten müssen betroffene Personen über die Verarbeitung, ihre Zwecke, die Art der erhobenen Daten, die Empfänger und ihre Datenschutzrechte unterrichtet werden.

5. Ihr Diensthandy wird gestohlen. Aufgrund der dort gespeicherten personenbezogenen Daten und falls davon auszugehen ist, dass ein Unbefugter Zugriff darauf erhält, handelt es sich dabei um eine Verletzung des Schutzes personenbezogener Daten. Wenn aufbewahrte personenbezogene Daten unbeabsichtigt oder unrechtmäßig unbefugten Empfängern offengelegt werden, vorübergehend nicht verfügbar sind oder geändert werden, muss die Datenschutzbehörde unverzüglich und spätestens binnen 72 Stunden, nachdem Ihnen die Verletzung bekannt wurde, über diese Verletzung des Schutzes personenbezogener Daten unterrichtet werden. Die Behörden müssen gegebenenfalls auch betroffene Personen über die Verletzung informieren, insbesondere wenn sensible Daten betroffen sind. Wenden Sie sich im Falle eines derartigen Ereignisses unverzüglich an die Datenschutzbeauftragte.

6. Eine Person, deren personenbezogene Daten für eine behördliche Tätigkeit des BKA verarbeitet werden, legt Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten, die die Behörde im öffentlichen Interesse durchführt, ein. Die betroffene Person muss die Gründe, die sich aus ihrer besonderen Situation ergeben, nennen. Das BKA kann die Verarbeitung der Daten fortsetzen und den Antrag ablehnen, wenn zwingende berechnete Interessen für die Verarbeitung vorliegen, die die Rechte und Freiheiten der betroffenen Person überwiegen, oder wenn die Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden.

7. Das BKA schließt einen Vertrag mit einer Catering-Firma. Es dürfen daher personenbezogene Daten verarbeitet werden, die erforderlich sind, um vor Abschluss des Vertrags und zur Vertragsabwicklung die erforderlichen Maßnahmen zu ergreifen, so etwa die Namen und E-Mail-Adressen der Ansprechpersonen bei der Catering-Firma.

8. Sie stellen als MitarbeiterIn der Personalabteilung der Sozialversicherung personenbezogene Daten (zum Beispiel Informationen über das Entgelt der Bediensteten) zur Verfügung. Diese Übermittlung beruht auf einer gesetzlichen Verpflichtung und ist daher DSGVO-konform.
9. Sie haben für die Verarbeitung personenbezogener Daten im Rahmen des Versands von Informationsmaterial Einwilligungen der Betroffenen vor dem 25. Mai 2018 eingeholt. Sie stellen sicher, dass die Einwilligungen in schriftlicher Form erfolgt sind und auch sonst allen Anforderungen der Datenschutz-Grundverordnung entsprechen. Wenn dies der Fall ist, müssen Sie die Betroffenen nicht um erneute Einwilligung ersuchen.
10. Sie haben vor einigen Jahren die Einwilligung der BezieherInnen von Informationsmaterial erhalten und dafür ein Online-System mit bereits aktivierten Kontrollkästchen verwendet. Diese Art der Einwilligung ist ab dem 25. Mai 2018 ungültig, da sie nicht den Erfordernissen der DSGVO entspricht. Sie müssen diese Einwilligungen erneut einholen, wenn Sie die Daten weiterhin verarbeiten möchten.
11. Sie versenden einen Online-Newsletter. Der Betroffene erteilt seine Einwilligung zur Registrierung für den Online-Newsletter, der es Ihnen erlaubt, alle Daten zu seinen Interessen zu verarbeiten, um ein Profil darüber zu erstellen, an welchen Artikeln er Interesse zeigt. Ein Jahr später teilt er Ihnen mit, dass er den Online-Newsletter nicht mehr erhalten möchte. Sie müssen sämtliche personenbezogenen Daten über diese Person aus Ihrer Datenbank löschen, die im Zusammenhang mit der Registrierung für den Newsletter erhoben wurden, einschließlich der Profile zu dieser Person.
12. Die Personalabteilung erhebt bei den neu eintretenden Bediensteten das personenbezogene Datum der Religionszugehörigkeit. Hierbei handelt es sich um ein sensibles Datum. Die Verarbeitung dieser Daten durch die Personalabteilung ist im Rahmen der DSGVO erlaubt, da sie für die Erfüllung des Dienstvertrages (Feiertage) erforderlich ist und im Verantwortungsbereich der Behörde liegt, deren MitarbeiterInnen der Amtsverschwiegenheit unterliegen.
13. Das BKA beauftragte für dienstrechtliche Zwecke (Feststellung der Dienstfähigkeit) einen Sachverständigen mit der Erstellung eines Gutachtens über die Ursachen der Erkrankung eines Mitarbeiters. Das erstellte Gutachten liegt im BKA nur in Papierform vor und wird zum Personalakt genommen. Der Mitarbeiter stellt den Antrag auf Löschung wegen Mangelhaftigkeit des Gutachtens. Weder das Gutachten als solches noch der Akt, in den das Gutachten eingeordnet wurde, ist als „Dateisystem“ im Sinne der DSGVO einzustufen. Dem Lösungsbegehren muss nicht gefolgt werden.

14. Sie nutzen Ihr eigenes, privates Adressbuch, um Freunde per E-Mail zu Ihrer Geburtstagsparty einzuladen. Die DSGVO kommt nicht zur Anwendung, da es sich um eine Tätigkeit im persönlichen/familiären Bereich handelt.

11 Musterdokumente

Die Datenschutzbeauftragte hat für diverse Fachbereiche des Bundeskanzleramtes nach den jeweiligen Bedürfnissen und Erfordernissen Muster erstellt.

Einige grundlegenden Muster, die für viele Arbeitsbereiche im Bundeskanzleramt von Bedeutung sind, werden nachfolgend dargestellt.

Bitte beachten Sie, dass diese Muster beispielhaft zu verstehen sind. Falls Sie aufgrund spezieller Fragstellungen darüber hinaus Unterstützung bei der Erstellung von Dokumenten für Ihren Arbeitsbereich benötigen, wenden Sie sich bitte an die Datenschutzbeauftragte.

11.1 Newsletter-Versand

Zustimmung zur Datenverarbeitung zwecks Bezugs eines Newsletters des Bundeskanzleramtes Datenschutzrechtliche Informationen gemäß Art 13 DSGVO

Verantwortlicher

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Telefon: +43 1 531 15-0,
E-Mail: post@bka.gv.at.

Wir speichern und verarbeiten Daten ausschließlich im Sinne 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 (DSGVO) sowie des österreichischen Datenschutzgesetzes, BGBl. I Nr. 165/1999, idgF.

Sie haben die Möglichkeit, unseren Newsletter zu abonnieren. Hierfür benötigen wir Ihre E-Mail-Adresse und Ihre Erklärung, dass Sie mit dem Bezug des Newsletters und der Verarbeitung Ihrer personenbezogenen Daten (Name, E-Mail-Adresse) einverstanden sind. Sie können den Bezug des Newsletters jederzeit stornieren. Senden sie Ihre Stornierung bitte an folgende E-Mail-Adresse: ...@bka.gv.at. Wir werden anschließend umgehend Ihre Daten im Zusammenhang mit dem Newsletter-Versand löschen.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

11.2 Einladungen zu Veranstaltungen

Zustimmung zum Bezug von Einladungen

**Zustimmung zur Datenverarbeitung
zwecks Teilnahme an Veranstaltungen des Bundeskanzleramtes
Datenschutzrechtliche Informationen gemäß Art 13 DSGVO**

Verantwortlicher

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Tel.: +43 1 531 15-0,
E-Mail: post@bka.gv.at.

Wir speichern und verarbeiten Daten ausschließlich im Sinne 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 (DSGVO) sowie des österreichischen Datenschutzgesetzes, BGBl. I Nr. 165/1999, idgF.

Sie erteilen hiermit Ihre Zustimmung zur Verarbeitung folgender personenbezogener Daten zum Zweck Ihrer Einladung zur Veranstaltungen des Bundeskanzleramtes (Abteilung ...): (Name, E-Mail-Adresse, *bitte nach Bedarf ergänzen*). Die Bereitstellung der genannten Daten ist für eine Teilnahme an unseren Veranstaltungen erforderlich. Eine Nicht-Bereitstellung hätte für Sie die Konsequenz, dass wie Ihre Teilnahme ablehnen müssen.

Sie können den Bezug unserer Einladungen jederzeit stornieren. Senden sie Ihre Stornierung bitte an folgende E-Mail-Adresse: ...@bka.gv.at. Wir werden anschließend umgehend Ihre Daten im Zusammenhang mit der Einladung zu unseren Veranstaltungen löschen.

Im Zuge des Veranstaltungsmanagements werden fallweise sicherheitspolizeiliche Registerabfragen durch die zuständigen Sicherheitsbehörden durchgeführt. Zu diesem Zweck können Ihre personenbezogenen Daten an die genannten Empfänger weitergeleitet werden.

Für die Organisation der Veranstaltung werden relevante Auszüge Ihrer Daten (*bitte nach Bedarf ergänzen*) überdies an Dienststellen des Bundeskanzleramtes (*bitte nach Bedarf ergänzen*) und weitere Institutionen (*bitte nach Bedarf ergänzen*) weitergeleitet.

Eine Übermittlung an Drittstaaten oder internationale Organisationen erfolgt grundsätzlich nicht ohne Ihre Zustimmung. Ausgenommen sind Fälle, in denen die Übermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist und beim Drittstaat bzw. der internationalen Organisation ein angemessener Datenschutz vorliegt.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

Einladungen auf gesetzlicher Grundlage

Teilnahme an Veranstaltungen des Bundeskanzleramtes Datenschutzrechtliche Informationen gemäß Art 13 DSGVO

Verantwortlicher

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Tel.: +43 1 531 15-0,
E-Mail: post@bka.gv.at.

Wir speichern und verarbeiten Daten ausschließlich im Sinne 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 (DSGVO) sowie des österreichischen Datenschutzgesetzes, BGBl. I Nr. 165/1999, idgF.

Sie erhalten diese Information, weil das Bundeskanzleramt Ihre personenbezogenen Daten (Name, E-Mail-Adresse, *bitte nach Bedarf ergänzen*) zwecks Einladung zur Veranstaltungen verarbeitet. Die Bereitstellung der genannten Daten ist für eine Teilnahme an unseren Veranstaltungen erforderlich. Eine Nicht-Bereitstellung hätte für Sie die Konsequenz, dass wir Ihre Teilnahme ablehnen müssen.

Unsere Zusendungen erfolgen auf der Rechtsgrundlage des Bundesministerien-gesetzes 1986, BGBl. Nr. 76/1986 idgF, Teil 2 der Anlage zu § 2 (Informations-tätigkeit der Bundesregierung).

Sie können den Bezug unserer Aussendungen jederzeit stornieren. Senden sie Ihre Stornierung bitte an folgende E-Mail-Adresse: ...@bka.gv.at. Wir werden anschließend umgehend Ihre Daten im Zusammenhang mit der Einladung zu unseren Veranstaltungen löschen.

Im Zuge des Veranstaltungsmanagements werden fallweise sicherheitspolizeiliche Registerabfragen durch die zuständigen Sicherheitsbehörden durchgeführt. Zu diesem Zweck können Ihre personenbezogenen Daten an die genannten Emp-fänger weitergeleitet werden.

Für die Organisation der Veranstaltung werden relevante Auszüge Ihrer Daten (*bitte nach Bedarf ergänzen*) überdies an Dienststellen des Bundeskanzleramtes (*bitte nach Bedarf ergänzen*) und weitere Institutionen (*bitte nach Bedarf er-gänzen*) weitergeleitet.

Eine Übermittlung an Drittstaaten oder internationale Organisationen erfolgt grundsätzlich nicht ohne Ihre Zustimmung. Ausgenommen sind Fälle, in denen die Übermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist und beim Drittstaat bzw. der internationalen Organisation ein angemessener Datenschutz vorliegt.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutz-recht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Daten-schutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

11.3 Hinweistafeln bei Veranstaltungen

Sehr geehrte Besucherin, sehr geehrter Besucher,

Bei der heutigen Veranstaltung werden Fotos, Ton- und Filmaufnahmen gemacht.

Verantwortlicher für die Datenverarbeitung ist das Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Telefon: +43 1 531 15-0, E-Mail: post@bka.gv.at.

Wir speichern und verarbeiten Daten ausschließlich im Sinne der EU-Datenschutz-Grundverordnung (DSGVO) und des österreichischen Datenschutzgesetzes idgF.

Zweck der Aufnahmen ist die interne Dokumentation der Veranstaltung und gegebenenfalls auch ihre Veröffentlichung.

Rechtsgrundlage für die Speicherung und Verarbeitung der Aufnahmen ist das Vorliegen eines öffentlichen Interesses an der Dokumentation gemäß Artikel 6 Abs. 1 lit. e DSGVO.

Mit der Teilnahme an der Veranstaltung stimmen Sie der Veröffentlichung der Fotos, Ton- und Filmaufnahmen zu, die im Rahmen der Veranstaltung entstehen. Wenn Sie mit der Veröffentlichung dieser Aufnahmen nicht einverstanden sind, ist Ihre Teilnahme an der Veranstaltung leider nicht möglich.

Die heute aufgenommenen Fotos, Ton- und Filmaufnahmen werden an folgende Empfänger weitergeleitet: ...

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

11.4 Zustimmung zur Veröffentlichung von Fotos

Zustimmungserklärung für Personen über 14 Jahre

Zustimmungserklärung

für die Veröffentlichung von Foto- bzw. Videomaterial vom Tag der offenen Tür des Bundeskanzleramtes am ... Datenschutzrechtliche Informationen gemäß Art 13 DSGVO

Ich,, (Vor- und Zuname in Druckbuchstaben), geboren am (TT.MM.JJJJ), erteile hiermit meine Zustimmung zur Veröffentlichung der Foto- bzw. Videoaufnahmen, die beim heutigen Tag der offenen Tür von mir gemacht werden.

Verantwortlicher

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Telefon: +43 1 531 15-0,
E-Mail: post@bka.gv.at.

Eine Veröffentlichung ist auf der Website des Bundeskanzleramtes, seinen Social-Media-Kanälen sowie gegebenenfalls in Printmedien vorgesehen.

Das Bundeskanzleramt speichert und verarbeitet Daten ausschließlich im Sinne 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 (DSGVO) sowie des durch das Datenschutz-Anpassungsgesetz novellierten Datenschutzgesetzes in der geltenden Fassung.

Die heute aufgenommenen Fotos werden archiviert. Daher ist keine Löschung vorgesehen.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

Wien, ... 2020

Unterschrift

Zustimmungserklärung für Personen unter 14 Jahre

Zustimmungserklärung

für die Veröffentlichung von Foto- bzw. Videomaterial

vom Tag der offenen Tür des Bundeskanzleramtes am ...

Datenschutzrechtliche Informationen gemäß Art 13 DSGVO

Ich,, (Vor- und Zuname in Druckbuchstaben), erteile hiermit meine Zustimmung zur Veröffentlichung der Foto- bzw. Videoaufnahmen, die beim heutigen Tag der offenen Tür von meinem Kind (Ich bin erziehungsberechtigt), geboren am (TT.MM.JJJJ) gemacht werden.

Verantwortlicher

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Telefon: +43 1 531 15-0,
E-Mail: post@bka.gv.at.

Eine Veröffentlichung ist auf der Website des Bundeskanzleramtes, seinen Social-Media-Kanälen sowie gegebenenfalls in Printmedien vorgesehen.

Das Bundeskanzleramt speichert und verarbeitet Daten ausschließlich im Sinne 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 (DSGVO) sowie des durch das Datenschutz-Anpassungsgesetz novellierten Datenschutzgesetzes in der geltenden Fassung.

Die heute aufgenommenen Fotos werden archiviert. Daher ist keine Löschung vorgesehen.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

Wien, ... 2020

Unterschrift

11.5 Verwendung von Outlook-Verteilern

Datenverarbeitung im Rahmen eines E-Mail-Verteilers des Bundeskanzleramtes Datenschutzrechtliche Informationen gemäß Art 13 DSGVO

Verantwortlicher

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Telefon: +43 1 531 15-0,
E-Mail: post@bka.gv.at

Wir speichern und verarbeiten Daten ausschließlich im Sinne 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 (DSGVO) sowie des österreichischen Datenschutzgesetzes, BGBl. I Nr. 165/1999, idgF.

Die Verarbeitung Ihrer personenbezogenen Daten, konkret Ihrer E-Mail-Adresse, erfolgt zum Zweck ... auf folgender Rechtsgrundlage: Informations- und Koordinationstätigkeit der Bundesregierung gemäß Teil 2 der Anlage zu § 2 Bundesministeriengesetz 1986 (BMG), idgF.

Sie können den Bezug unserer Aussendungen jederzeit stornieren. Senden Sie Ihre Stornierung an folgende E-Mail-Adresse: ...@bka.gv.at. Wir löschen anschließend umgehend Ihre Daten im Zusammenhang mit dem angeführten Zweck.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

11.6 Beantwortung der Anfragen von BürgerInnen (Bürgerservice)

Anfrage an das Bundeskanzleramt

Datenschutzrechtliche Informationen gemäß Art 13 DSGVO

Verantwortlicher

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Telefon: +43 1 531 15-0,
E-Mail: post@bka.gv.at

Wir speichern und verarbeiten Daten ausschließlich im Sinne 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 (DSGVO) sowie des österreichischen Datenschutzgesetzes, BGBl. I Nr. 165/1999, idgF.

Unsere Zusendung erfolgt auf der Rechtsgrundlage des Bundesministerien-gesetzes 1986, BGBl. Nr. 76/1986 idgF, Teil 2 der Anlage zu § 2 (Informationstätigkeit der Bundesregierung). Hierfür speichern wir Ihren Vor- und Zunamen, Ihre E-Mail-Adresse und ggf. sonstige personenbezogene Daten, die Sie im Zuge Ihres Schreibens an das Bundeskanzleramt übermitteln. Ihre Daten werden nach der gesetzlichen Aufbewahrungsfrist für elektronische Akten im Bundeskanzleramt (Skartierungsfrist 10 Jahre) gelöscht.

Für die zutreffende Beantwortung Ihres Anliegens werden relevante Auszüge Ihrer Daten (insbesondere Vor- und Zuname, E-Mail-Adresse, Anschrift und ggf. Telefonnummern) – wenn organisationstechnisch erforderlich – an Dienststellen des Bundeskanzleramtes (die Kabinette und jeweiligen Fachabteilungen) weitergeleitet, sowie ggf. an andere Bundesministerien übermittelt.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

11.7 Musterdokument zur Beantwortung von Anträgen auf Löschung von digitalen Schriftstücke und Unterlagen bzw. personenbezogenen Daten im ELAK

Gemäß § 12 Bundesministeriengesetz BGBl. Nr. 76/1986 idgF ist die formale Behandlung der von den Bundesministerien zu besorgenden Geschäfte von der Bundesregierung in einer für alle Bundesministerien einheitlichen Kanzleiordnung (Büroordnung) festzulegen. Desgleichen sind die notwendigen Maßnahmen zum Schutz personenbezogener Daten anzuordnen. Aufgrund dieser Gesetzesbestimmung erging die Büroordnung 2004, die in § 25 festlegt, dass die Aufbewahrungsfrist des elektronischen Aktes grundsätzlich mit dem Ablauf des zehnten Kalenderjahres nach dem letzten Bearbeitungsvorgang festgesetzt wird. Gemäß § 26 Abs. 2 ist zudem das Österreichische Staatsarchiv vor einer beabsichtigten Vernichtung von Akten zu verständigen, um diesem die Gelegenheit zu geben, solche Akten zu sichten und bei Bedarf zu übernehmen.

Ihrem Antrag auf Löschung der digitalen Schriftstücke und Unterlagen, die im ELAK verarbeitet wurden, kann daher nicht entsprochen werden, weil die mindestens 10-jährige bzw. bei Archivzwecken darüber hinaus gehende Speicherung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der das Bundeskanzleramt aufgrund des Bundesministeriengesetzes und der Büroordnung unterliegt. Darüber hinaus widerspricht der Löschung, dass die Verarbeitung zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, erforderlich ist (Art 17 Abs.3 lit. b DSGVO).

Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Datenschutzbehörde beschweren. In Österreich ist die Datenschutzbehörde zuständig.

11.8 Beantwortung von Auskunftsbegehren

Wenn es nicht zutrifft, dass personenbezogene Daten der Antragstellerin / des Antragstellers verarbeitet werden:

Das Bundeskanzleramt hat Ihren Antrag auf Auskunft vom ... am ... erhalten und teilt Ihnen innerhalb der vorgesehenen Frist von einem Monat folgendes mit:
Das Bundeskanzleramt (*eventuell, je nach Anfrage: Sektion ..., Abteilung ...*) verarbeitet keine Sie betreffende personenbezogene Daten.

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren.

In Österreich ist dies die Österreichische Datenschutzbehörde, Barichgasse 40-42, 1030 Wien, Telefon: +43 1 52152-0, E-Mail: dsb@dsb.gv.at.

Sie erreichen uns unter folgenden Kontaktdaten:

Bundeskanzleramt, Abteilung ..., Ansprechperson ..., Telefon ..., E-Mail ...

Unsere Datenschutzbeauftragte erreichen Sie unter:

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at

Wenn es zutrifft, dass personenbezogene Daten der Antragstellerin / des Antragstellers verarbeitet werden, ist die Beantwortung folgendermaßen abzufassen und inhaltlich je nach dem vorliegenden Sachverhalt zu ergänzen:

Das Bundeskanzleramt hat Ihren Antrag auf Auskunft vom ... am ... erhalten und teilt Ihnen innerhalb der vorgesehenen Frist von einem Monat folgendes mit:

Das Bundeskanzleramt (*eventuell, je nach Anfrage: Sektion ..., Abteilung ...*) verarbeitet Sie betreffende personenbezogene Daten.

Zweck dieser Verarbeitung ist ... (*ergänzen*).

Es werden folgende Kategorien Sie betreffender personenbezogener Daten verarbeitet: (*ergänzen – konkrete Daten sind anzuführen, d. h. der konkrete Name, ...*).

Ausdrucke der relevanten Datenverarbeitungen finden Sie im Anhang. ODER Beiliegend werden Ihnen die relevanten Datenverarbeitungen elektronisch übermittelt.

(*Falls zutreffend:*) Ihre Daten wurden dem Bundeskanzleramt von ... (*ergänzen*) übermittelt.

(*Falls zutreffend:*) Die Sie betreffenden personenbezogenen Daten werden gegenüber folgenden Empfängern offengelegt: ... (*ergänzen*).

Die Sie betreffenden personenbezogenen Daten werden gespeichert und ... (*ergänzen – z. B. Verweis auf ELAK-Skartierungsfrist*) gelöscht. ODER Die Sie betreffenden personenbezogenen Daten werden gespeichert und nicht gelöscht, weil ... (*ergänzen – z. B. Verweis auf Archivwürdigkeit*).

(*Anmerkung: Bitte entsprechend dem Eintrag ins DataReg formulieren und gesetzliche Grundlage für die Löschfrist angeben, wenn eine solche besteht.*)

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Österreichische Datenschutzbehörde, Barichgasse 40-42, 1030 Wien, Telefon: +43 1 52152-0, E-Mail: dsb@dsb.gv.at.

Sie erreichen uns unter folgenden Kontaktdaten:

Bundeskanzleramt, Abteilung ..., Ansprechperson ..., Telefon ..., E-Mail ...

Unsere Datenschutzbeauftragte erreichen Sie unter:

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at

11.9 Durchführung einer Datenschutz-Folgenabschätzung

I. Bezeichnung der Verarbeitungstätigkeit:

Zuständige Abteilung:

Abteilungsleiter:

II. Beschreibung der Verarbeitungstätigkeit:

1. Grundlegende Informationen

| | |
|---|--------------------------------------|
| Welche personenbezogenen Daten werden verarbeitet? | Risikofaktor: Niedrig/Mittel/Hoch |
| <hr/> | |
| Für welchen Zweck werden die personenbezogenen Daten verarbeitet? | Risikofaktor: Niedrig/Mittel/Hoch |
| <hr/> | |
| Welche Kategorien von betroffenen Personen sind durch die Verarbeitung erfasst? | Risikofaktor: Niedrig/Mittel/Hoch |
| <hr/> | |
| Wie viele Personen sind von der Verarbeitung betroffen? | Risikofaktor: Niedrig/Mittel/Hoch |
| <hr/> | |
| Mit Hilfe welcher Technologie werden die Daten verarbeitet? Werden dabei auch neue Technologien genutzt? | Risikofaktor: Niedrig/Mittel/Hoch |
| <hr/> | |
| Wurden die betroffenen Personen über die Verarbeitung informiert? Und wenn ja, welche Informationen wurden ihnen dabei gegeben? | Risikofaktor: Niedrig/Mittel/Hoch |
| <hr/> | |
| Werden in der Verarbeitung automatisiert Entscheidungen über die betroffene Person getroffen? | Risikofaktor: Niedrig/Mittel/Hoch |
| <hr/> | |
| Wie viele Personen sind von der Verarbeitung betroffen? | Risikofaktor: Niedrig/Mittel/Hoch |
| <hr/> | |
| Mit Hilfe welcher Technologie werden die Daten verarbeitet? Werden dabei auch neue Technologien genutzt? | Risikofaktor: Niedrig/Mittel/Hoch |
| <hr/> | |

Wurden die betroffenen Personen über die Verarbeitung informiert? Und wenn ja, welche Informationen wurden ihnen dabei gegeben?

Risikofaktor:
Niedrig/Mittel/Hoch

Werden in der Verarbeitung automatisiert Entscheidungen über die betroffene Person getroffen?

Risikofaktor:
Niedrig/Mittel/Hoch

Werden die personenbezogenen Daten mit anderen Datensätzen kombiniert oder verglichen?

Risikofaktor:
Niedrig/Mittel/Hoch

Wie werden die Daten erfasst?

Risikofaktor:
Niedrig/Mittel/Hoch

Wird sichergestellt, dass nur für den angegebenen Zweck erforderliche Daten erfasst werden?

Risikofaktor:
Niedrig/Mittel/Hoch

In welchem Umfang werden die Daten verarbeitet?

Risikofaktor:
Niedrig/Mittel/Hoch

Wer hat Zugriff auf die personenbezogenen Daten? Haben Auftragsnehmer Zugriff auf diese Daten und geben diese wiederum an Subauftragsnehmer weiter?

Risikofaktor:
Niedrig/Mittel/Hoch

Werden die Daten an andere Organisationseinheiten weitergegeben oder an externe Dritte?

Risikofaktor:
Niedrig/Mittel/Hoch

Werden Daten auch außerhalb der EU/EWR weitergeleitet oder haben Personen daraus Zugriff?

Risikofaktor:
Niedrig/Mittel/Hoch

Wo werden die personenbezogenen Daten gespeichert?

Risikofaktor:
Niedrig/Mittel/Hoch

Wie lange werden die personenbezogenen Daten gespeichert?

Risikofaktor:
Niedrig/Mittel/Hoch

2. Rechtliche Beurteilung

(a) Schwellwertanalyse

Vorfrage: Ist die Verarbeitung in der Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV, BGBl. II Nr. 108/2018) oder in der Datenschutz-Folgenabschätzung-Verordnung (DSFA-V, BGBl. II Nr. 278/2018) gelistet?

Ist eine Datenschutzfolgenabschätzung jedenfalls erforderlich oder kann sie entfallen?

Datenschutz-Folgenabschätzung-Verordnung: Datenschutzfolgenabschätzung ist jedenfalls durchzuführen

Datenschutz-Folgenabschätzung-Ausnahmenverordnung: Keine Datenschutzfolgenabschätzung erforderlich, sondern lediglich zu dokumentieren, dass ein inhaltsgleicher Fall vorliegt.

Liegt eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche vor?

In diesem Fall ist jedenfalls eine Datenschutzfolgenabschätzung durchzuführen (Art 35 Abs. 3 lit. c DSGVO).

(b) Rechtliche Risikobewertung

Erfolgt die Verarbeitung zu festgelegten, eindeutigen und legitimen Zwecken?

Zweck und Umfang der Verarbeitungstätigkeit müssen im Vorfeld klar abgegrenzt und definiert sein.

Liegt ein Rechtfertigungsgrund des Art 6 DSGVO vor?

Es ist zu prüfen und zu beschreiben, auf welcher Rechtsgrundlage die Daten verarbeitet werden.

Werden nur die für den konkreten Zweck notwendigen Daten verarbeitet oder gibt es gelindere Mittel? Können statt personenbezogenen Daten auch anonyme Daten verwendet werden?

Die Datenverarbeitung darf – auch mit Blick auf Privacy by default – nur solche Daten enthalten, deren Verarbeitung für den Zweck angemessen und erheblich ist.

Werden die Daten nur solange (personenbezogen) aufbewahrt, als dies zur Erreichung des Zwecks absolut erforderlich ist?

Nach dem Ende gesetzlicher Aufbewahrungspflichten ist eine strenge Prüfung der Aufbewahrungsdauer abzubilden.

Haben nur die Personen Zugriff auf personenbezogene Daten, die diese tatsächlich im Rahmen der Zweckerfüllung benötigen?

Auch innerhalb des Unternehmens ist zu gewährleisten, dass der Datenzugriff auf das notwendige Ausmaß beschränkt ist.

Wurde der Betroffene ausreichend informiert?

Die nach Art 13 und 14 DSGVO erforderlichen Informationen müssen den Betroffenen rechtzeitig und vollständig zur Verfügung stehen.

Kann der Betroffene jederzeit Auskunft über seine Daten sowie eine maschinenlesbare Kopie erhalten?

Die nach Art 15 und 20 DSGVO zustehenden Rechte müssen auch technisch innerhalb der Frist umsetzbar sein.

Kann der Betroffene seine Daten berichtigen, löschen und deren Verarbeitung einschränken lassen?

Die nach Art 16, 17, 18, 19 und 21 DSGVO zustehenden Rechte müssen auch technisch innerhalb der Frist umsetzbar sein.

Welche Empfänger bekommen auf Basis welcher Rechtsgrundlage welche Daten? Sind die notwendigen vertraglichen Verpflichtungen eingehalten?

Neben Übermittlungsempfängern, die Daten zu eigenen Zwecken auf Basis einer gesonderten Rechtsgrundlage verarbeiten, sind insbesondere auch Auftragsverarbeiter und die zugrundeliegenden Verträge nach Art 28 DSGVO darzustellen.

Erfolgt eine Übermittlung an Empfänger außerhalb des EWR? Werden nachweisbare, geeignete Garantien eingehalten?

Sofern kein Angemessenheitsbeschluss der EU-Kommission vorliegt, müssen geeignete Garantien getroffen und nachgewiesen werden (z.B. Standarddatenschutzklauseln).

3. Technische Risikobewertung

Das technische Risiko wird als hoch/mittel/niedrig eingestuft, weil ...

4. Maßnahmen zur Risikobegrenzung

| Festgestelltes Risiko | Wahrscheinlichkeit eines Risikoeintritts, Auswirkung und Folgen für betroffene Personen | Maßnahmen zur Risikobegrenzung | Risikoeffekt |
|-----------------------|---|--|---------------------|
| hoch/mittel-niedrig | hoch/mittel/niedrig | z.B. 1. angemessene Datensicherheitsmaßnahmen 2. Informationstafeln 3. schriftliche Erklärungen der zuständigen Sachbearbeiter über ... | hoch/mittel/niedrig |

5. Implementierung

Wer ist für die Implementierung der getroffenen Maßnahmen zuständig?

| Getroffene Maßnahme | Datum der Fertigstellung |
|---|---|
| z.B. 1. angemessene Datensicherheitsmaßnahmen 2. Informationstafeln 3. schriftliche Erklärungen der zuständigen Sachbearbeiter über... | 1. umgesetzt durch Verwendung geeigneter Technologie 2. angebracht am ... 3. eingeholt am ... |

11.10 Datenschutzinformation für Förderverträge

Abschluss eines Fördervertrages mit dem Bundeskanzleramt Datenschutzrechtliche Informationen gemäß Art 13 DSGVO

Verantwortlicher

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Telefon: +43 1 531 15-0,

E-Mail: post@bka.gv.at

Wir speichern und verarbeiten Daten ausschließlich im Sinne 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 (DSGVO) sowie des österreichischen Datenschutzgesetzes, BGBl. I Nr. 165/1999, idgF.

Die Verarbeitung Ihrer personenbezogenen Daten erfolgt auf der Rechtsgrundlage von Artikel 6 Absatz 1 lit. b DSGVO zur Anbahnung und Erfüllung eines Fördervertrages, wozu auch die Überprüfung der Förderabrechnung zählt.

Konkret verarbeiten wir jene personenbezogenen Daten, die Sie bei der Antragstellung bekannt gegeben haben sowie jene Daten, die im Zuge der Vertragsabwicklung noch bekannt zu geben sind.

Ihre personenbezogenen Daten werden so lange verarbeitet, als die Geltendmachung von Rechtsansprüchen aus dem Fördervertrag möglich ist.

Eine Weiterleitung Ihrer personenbezogenen Daten kann gegebenenfalls an den Rechnungshof, die Europäische Kommission, die Transparenzdatenbank und das Bundesministerium für Finanzen erfolgen. Weiters können diese Daten an die Rechtsvertretung des Bundeskanzleramtes sowie an Gerichte und Verwaltungsbehörden zur Durchsetzung oder Abwehr von Rechtsansprüchen in Zusammenhang mit dem Förderungsvertrag oder dessen Anbahnung übermittelt werden. Darüber hinaus können andere förderungsgewährende Stellen, insbesondere jene, die im Förderungsansuchen genannt werden, diese Daten erhalten.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

Weitere Informationen

Sie erreichen uns für alle Anfragen im Zusammenhang mit der Förderung unter folgenden Kontaktdaten: Bundeskanzleramt, Abteilung ..., Ballhausplatz 2, 1010 Wien, Telefon: +43 1 53115-..., E-Mail: ...@bka.gv.at

Unsere Datenschutzbeauftragte erreichen Sie unter: Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010-Wien, E-Mail: sektion.praesidium@bka.gv.at.

11.11 Hinweistafeln bei Videoüberwachung

In den Eingangs- und Zugangsbereichen des Bundeskanzleramtes werden Videoaufnahmen gemacht.

Verantwortlicher

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien, Telefon: +43 1 531 15-0,
E-Mail: post@bka.gv.at.

Unsere Datenschutzbeauftragte erreichen Sie unter Bundeskanzleramt, Datenschutzbeauftragte, Ballhausplatz 2, 1010 Wien, E-Mail: sektion.praesidium@bka.gv.at.

Wir verarbeiten die genannten Aufnahmen ausschließlich im Sinne der EU-Datenschutz-Grundverordnung (DSGVO).

Zweck der Aufnahmen ist der Personen- und Objektschutz im Bundeskanzleramt.

Rechtsgrundlage für die Videoaufnahmen ist gemäß Art. 6 Abs. 1 lit. f DSGVO, dass die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist.

Die Aufnahmen werden nach 72 Stunden gelöscht.

Wenn es zur Aufklärung einer Straftat erforderlich ist, werden die Aufnahmen an die zuständigen Stellen weitergeleitet.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch zu. Wenn Sie der Meinung sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist dies die Datenschutzbehörde.

I

(Gesetzgebungsakte)

VERORDNUNGEN

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)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ⁽¹⁾,

nach Stellungnahme des Ausschusses der Regionen ⁽²⁾,

gemäß dem ordentlichen Gesetzgebungsverfahren ⁽³⁾,

in Erwägung nachstehender Gründe:

- (1) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
- (2) Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.
- (3) Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates ⁽⁴⁾ ist die Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.

⁽¹⁾ ABl. C 229 vom 31.7.2012, S. 90.

⁽²⁾ ABl. C 391 vom 18.12.2012, S. 127.

⁽³⁾ Standpunkt des Europäischen Parlaments vom 12. März 2014 (noch nicht im Amtsblatt veröffentlicht) und Standpunkt des Rates in erster Lesung vom 8. April 2016 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlaments vom 14. April 2016.

⁽⁴⁾ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

- (4) Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen. Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Diese Verordnung steht im Einklang mit allen Grundrechten und achtet alle Freiheiten und Grundsätze, die mit der Charta anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, Schutz personenbezogener Daten, Gedanken-, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung und Informationsfreiheit, unternehmerische Freiheit, Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren und Vielfalt der Kulturen, Religionen und Sprachen.
- (5) Die wirtschaftliche und soziale Integration als Folge eines funktionierenden Binnenmarkts hat zu einem deutlichen Anstieg des grenzüberschreitenden Verkehrs personenbezogener Daten geführt. Der unionsweite Austausch personenbezogener Daten zwischen öffentlichen und privaten Akteuren einschließlich natürlichen Personen, Vereinigungen und Unternehmen hat zugenommen. Das Unionsrecht verpflichtet die Verwaltungen der Mitgliedstaaten, zusammenzuarbeiten und personenbezogene Daten auszutauschen, damit sie ihren Pflichten nachkommen oder für eine Behörde eines anderen Mitgliedstaats Aufgaben durchführen können.
- (6) Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass private Unternehmen und Behörden im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen. Zunehmend machen auch natürliche Personen Informationen öffentlich weltweit zugänglich. Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert und dürfte den Verkehr personenbezogener Daten innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen noch weiter erleichtern, wobei ein hohes Datenschutzniveau zu gewährleisten ist.
- (7) Diese Entwicklungen erfordern einen soliden, kohärenteren und klar durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union, da es von großer Wichtigkeit ist, eine Vertrauensbasis zu schaffen, die die digitale Wirtschaft dringend benötigt, um im Binnenmarkt weiter wachsen zu können. Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen. Natürliche Personen, Wirtschaft und Staat sollten in rechtlicher und praktischer Hinsicht über mehr Sicherheit verfügen.
- (8) Wenn in dieser Verordnung Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind, können die Mitgliedstaaten Teile dieser Verordnung in ihr nationales Recht aufnehmen, soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen.
- (9) Die Ziele und Grundsätze der Richtlinie 95/46/EG besitzen nach wie vor Gültigkeit, doch hat die Richtlinie nicht verhindern können, dass der Datenschutz in der Union unterschiedlich gehandhabt wird, Rechtsunsicherheit besteht oder in der Öffentlichkeit die Meinung weit verbreitet ist, dass erhebliche Risiken für den Schutz natürlicher Personen bestehen, insbesondere im Zusammenhang mit der Benutzung des Internets. Unterschiede beim Schutzniveau für die Rechte und Freiheiten von natürlichen Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten in den Mitgliedstaaten, vor allem beim Recht auf Schutz dieser Daten, können den unionsweiten freien Verkehr solcher Daten behindern. Diese Unterschiede im Schutzniveau können daher ein Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten darstellen, den Wettbewerb verzerren und die Behörden an der Erfüllung der ihnen nach dem Unionsrecht obliegenden Pflichten hindern. Sie erklären sich aus den Unterschieden bei der Umsetzung und Anwendung der Richtlinie 95/46/EG.
- (10) Um ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden. Hinsichtlich der Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, sollten die Mitgliedstaaten die Möglichkeit haben, nationale Bestimmungen, mit denen die Anwendung der Vorschriften dieser Verordnung genauer festgelegt wird, beizubehalten oder einzuführen. In Verbindung mit den allgemeinen und horizontalen Rechtsvorschriften über den Datenschutz zur Umsetzung der Richtlinie 95/46/EG gibt es in den Mitgliedstaaten mehrere sektorspezifische Rechtsvorschriften in Bereichen, die spezifischere Bestimmungen erfordern. Diese Verordnung bietet den Mitgliedstaaten zudem einen Spielraum für die Spezifizierung ihrer Vorschriften, auch für die Verarbeitung besonderer Kategorien von personenbezogenen Daten (im Folgenden „sensible Daten“). Diesbezüglich schließt diese Verordnung nicht Rechtsvorschriften der Mitgliedstaaten aus, in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

- (11) Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert die Stärkung und präzise Festlegung der Rechte der betroffenen Personen sowie eine Verschärfung der Verpflichtungen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden, ebenso wie — in den Mitgliedstaaten — gleiche Befugnisse bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung.
- (12) Artikel 16 Absatz 2 AEUV ermächtigt das Europäische Parlament und den Rat, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten zu erlassen.
- (13) Damit in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, beseitigt werden, ist eine Verordnung erforderlich, die für die Wirtschaftsteilnehmer einschließlich Kleinunternehmen sowie kleiner und mittlerer Unternehmen Rechtssicherheit und Transparenz schafft, natürliche Personen in allen Mitgliedstaaten mit demselben Niveau an durchsetzbaren Rechten ausstattet, dieselben Pflichten und Zuständigkeiten für die Verantwortlichen und Auftragsverarbeiter vorsieht und eine gleichmäßige Kontrolle der Verarbeitung personenbezogener Daten und gleichwertige Sanktionen in allen Mitgliedstaaten sowie eine wirksame Zusammenarbeit zwischen den Aufsichtsbehörden der einzelnen Mitgliedstaaten gewährleistet. Das reibungslose Funktionieren des Binnenmarkts erfordert, dass der freie Verkehr personenbezogener Daten in der Union nicht aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten eingeschränkt oder verboten wird. Um der besonderen Situation der Kleinunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen, enthält diese Verordnung eine abweichende Regelung hinsichtlich des Führens eines Verzeichnisses für Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen. Außerdem werden die Organe und Einrichtungen der Union sowie die Mitgliedstaaten und deren Aufsichtsbehörden dazu angehalten, bei der Anwendung dieser Verordnung die besonderen Bedürfnisse von Kleinunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen. Für die Definition des Begriffs „Kleinunternehmen sowie kleine und mittlere Unternehmen“ sollte Artikel 2 des Anhangs zur Empfehlung 2003/361/EG der Kommission ⁽¹⁾ maßgebend sein.
- (14) Der durch diese Verordnung gewährte Schutz sollte für die Verarbeitung der personenbezogenen Daten natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gelten. Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person.
- (15) Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen. Der Schutz natürlicher Personen sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten nicht in den Anwendungsbereich dieser Verordnung fallen.
- (16) Diese Verordnung gilt nicht für Fragen des Schutzes von Grundrechten und Grundfreiheiten und des freien Verkehrs personenbezogener Daten im Zusammenhang mit Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, wie etwa die nationale Sicherheit betreffende Tätigkeiten. Diese Verordnung gilt nicht für die von den Mitgliedstaaten im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der Union durchgeführte Verarbeitung personenbezogener Daten.
- (17) Die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates ⁽²⁾ gilt für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, sollten an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst und im Lichte der vorliegenden Verordnung angewandt werden. Um einen soliden und kohärenten Rechtsrahmen im Bereich des Datenschutzes in der Union zu gewährleisten, sollten die erforderlichen Anpassungen der Verordnung (EG) Nr. 45/2001 im Anschluss an den Erlass der vorliegenden Verordnung vorgenommen werden, damit sie gleichzeitig mit der vorliegenden Verordnung angewandt werden können.
- (18) Diese Verordnung gilt nicht für die Verarbeitung von personenbezogenen Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen

⁽¹⁾ Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinunternehmen sowie der kleinen und mittleren Unternehmen (C(2003)1422) (Abl. L 124 vom 20.5.2003, S. 36).

⁽²⁾ Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (Abl. L 8 vom 12.1.2001, S. 1).

oder wirtschaftlichen Tätigkeit vorgenommen wird. Als persönliche oder familiäre Tätigkeiten könnte auch das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten gelten. Diese Verordnung gilt jedoch für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen.

- (19) Der 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie der freie Verkehr dieser Daten sind in einem eigenen Unionsrechtsakt geregelt. Deshalb sollte diese Verordnung auf Verarbeitungstätigkeiten dieser Art keine Anwendung finden. Personenbezogene Daten, die von Behörden nach dieser Verordnung verarbeitet werden, sollten jedoch, wenn sie zu den vorstehenden Zwecken verwendet werden, einem spezifischeren Unionsrechtsakt, nämlich der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates ⁽¹⁾ unterliegen. Die Mitgliedstaaten können die zuständigen Behörden im Sinne der Richtlinie (EU) 2016/680 mit Aufgaben betrauen, die nicht zwangsläufig für die 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, ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den Anwendungsbereich dieser Verordnung fällt,

als sie in den Anwendungsbereich des Unionsrechts fällt. In Bezug auf die Verarbeitung personenbezogener Daten durch diese Behörden für Zwecke, die in den Anwendungsbereich dieser Verordnung fallen, sollten die Mitgliedstaaten spezifischere Bestimmungen beibehalten oder einführen können, um die Anwendung der Vorschriften dieser Verordnung anzupassen. In den betreffenden Bestimmungen können die Auflagen für die Verarbeitung personenbezogener Daten durch diese zuständigen Behörden für jene anderen Zwecke präziser festgelegt werden, wobei der verfassungsmäßigen, organisatorischen und administrativen Struktur des betreffenden Mitgliedstaats Rechnung zu tragen ist. Soweit diese Verordnung für die Verarbeitung personenbezogener Daten durch private Stellen gilt, sollte sie vorsehen, dass die Mitgliedstaaten einige Pflichten und Rechte unter bestimmten Voraussetzungen mittels Rechtsvorschriften beschränken können, wenn diese Beschränkung in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz bestimmter wichtiger Interessen darstellt, wozu auch die öffentliche Sicherheit und die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung zählen, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Dies ist beispielsweise im Rahmen der Bekämpfung der Geldwäsche oder der Arbeit kriminaltechnischer Labors von Bedeutung.

- (20) Diese Verordnung gilt zwar unter anderem für die Tätigkeiten der Gerichte und anderer Justizbehörden, doch könnte im Unionsrecht oder im Recht der Mitgliedstaaten festgelegt werden, wie die Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung personenbezogener Daten durch Gerichte und andere Justizbehörden im Einzelnen auszusehen haben. Damit die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassung unangetastet bleibt, sollten die Aufsichtsbehörden nicht für die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein. Mit der Aufsicht über diese Datenverarbeitungsvorgänge sollten besondere Stellen im Justizsystem des Mitgliedstaats betraut werden können, die insbesondere die Einhaltung der Vorschriften dieser Verordnung sicherstellen, Richter und Staatsanwälte besser für ihre Pflichten aus dieser Verordnung sensibilisieren und Beschwerden in Bezug auf derartige Datenverarbeitungsvorgänge bearbeiten sollten.
- (21) Die vorliegende Verordnung berührt nicht die Anwendung der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates ⁽²⁾ und insbesondere die der Vorschriften der Artikel 12 bis 15 jener Richtlinie zur Verantwortlichkeit von Anbietern reiner Vermittlungsdienste. Die genannte Richtlinie soll dazu beitragen, dass der Binnenmarkt einwandfrei funktioniert, indem sie den freien Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten sicherstellt.
- (22) Jede Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union sollte gemäß dieser Verordnung erfolgen, gleich, ob die Verarbeitung in oder außerhalb der Union stattfindet. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei nicht ausschlaggebend.

⁽¹⁾ 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, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2000/383/JI des Rates (siehe Seite 89 dieses Amtsblatts).

⁽²⁾ Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) (ABl. L 178 vom 17.7.2000, S. 1).

- (23) Damit einer natürlichen Person der gemäß dieser Verordnung gewährleistete Schutz nicht vorenthalten wird, sollte die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter dieser Verordnung unterliegen, wenn die Verarbeitung dazu dient, diesen betroffenen Personen gegen Entgelt oder unentgeltlich Waren oder Dienstleistungen anzubieten. Um festzustellen, ob dieser Verantwortliche oder Auftragsverarbeiter betroffenen Personen, die sich in der Union befinden, Waren oder Dienstleistungen anbietet, sollte festgestellt werden, ob der Verantwortliche oder Auftragsverarbeiter offensichtlich beabsichtigt, betroffenen Personen in einem oder mehreren Mitgliedstaaten der Union Dienstleistungen anzubieten. Während die bloße Zugänglichkeit der Website des Verantwortlichen, des Auftragsverarbeiters oder eines Vermittlers in der Union, einer E-Mail-Adresse oder anderer Kontaktdaten oder die Verwendung einer Sprache, die in dem Drittland, in dem der Verantwortliche niedergelassen ist, allgemein gebräuchlich ist, hierfür kein ausreichender Anhaltspunkt ist, können andere Faktoren wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern, die sich in der Union befinden, darauf hindeuten, dass der Verantwortliche beabsichtigt, den Personen in der Union Waren oder Dienstleistungen anzubieten.
- (24) Die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter sollte auch dann dieser Verordnung unterliegen, wenn sie dazu dient, das Verhalten dieser betroffenen Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt. Ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von betroffenen Personen gilt, sollte daran festgemacht werden, ob ihre Internetaktivitäten nachvollzogen werden, einschließlich der möglichen nachfolgenden Verwendung von Techniken zur Verarbeitung personenbezogener Daten, durch die von einer natürlichen Person ein Profil erstellt wird, das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen.
- (25) Ist nach Völkerrecht das Recht eines Mitgliedstaats anwendbar, z. B. in einer diplomatischen oder konsularischen Vertretung eines Mitgliedstaats, so sollte die Verordnung auch auf einen nicht in der Union niedergelassenen Verantwortlichen Anwendung finden.
- (26) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.
- (27) Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.
- (28) Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen. Durch die ausdrückliche Einführung der „Pseudonymisierung“ in dieser Verordnung ist nicht beabsichtigt, andere Datenschutzmaßnahmen auszuschließen.
- (29) Um Anreize für die Anwendung der Pseudonymisierung bei der Verarbeitung personenbezogener Daten zu schaffen, sollten Pseudonymisierungsmaßnahmen, die jedoch eine allgemeine Analyse zulassen, bei demselben Verantwortlichen möglich sein, wenn dieser die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um — für die jeweilige Verarbeitung — die Umsetzung dieser Verordnung zu gewährleisten, wobei sicherzustellen ist, dass zusätzliche Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden. Der für die Verarbeitung der personenbezogenen Daten Verantwortliche, sollte die befugten Personen bei diesem Verantwortlichen angeben.

- (30) Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.
- (31) Behörden, gegenüber denen personenbezogene Daten aufgrund einer rechtlichen Verpflichtung für die Ausübung ihres offiziellen Auftrags offengelegt werden, wie Steuer- und Zollbehörden, Finanzermittlungsstellen, unabhängige Verwaltungsbehörden oder Finanzmarktbehörden, die für die Regulierung und Aufsicht von Wertpapiermärkten zuständig sind, sollten nicht als Empfänger gelten, wenn sie personenbezogene Daten erhalten, die für die Durchführung — gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten — eines einzelnen Untersuchungsauftrags im Interesse der Allgemeinheit erforderlich sind. Anträge auf Offenlegung, die von Behörden ausgehen, sollten immer schriftlich erfolgen, mit Gründen versehen sein und gelegentlichen Charakter haben, und sie sollten nicht vollständige Dateisysteme betreffen oder zur Verknüpfung von Dateisystemen führen. Die Verarbeitung personenbezogener Daten durch die genannten Behörden sollte den für die Zwecke der Verarbeitung geltenden Datenschutzvorschriften entsprechen.
- (32) Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen. Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen. Wenn die Verarbeitung mehreren Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden. Wird die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert, so muss die Aufforderung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen.
- (33) Oftmals kann der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimmte Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.
- (34) Genetische Daten sollten als personenbezogene Daten über die ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person definiert werden, die aus der Analyse einer biologischen Probe der betreffenden natürlichen Person, insbesondere durch eine Chromosomen, Desoxyribonukleinsäure (DNS)- oder Ribonukleinsäure (RNS)-Analyse oder der Analyse eines anderen Elements, durch die gleichwertige Informationen erlangt werden können, gewonnen werden.
- (35) Zu den personenbezogenen Gesundheitsdaten sollten alle Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen. Dazu gehören auch Informationen über die natürliche Person, die im Zuge der Anmeldung für sowie der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates ⁽¹⁾ für die natürliche Person erhoben werden, Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen.
- (36) Die Hauptniederlassung des Verantwortlichen in der Union sollte der Ort seiner Hauptverwaltung in der Union sein, es sei denn, dass Entscheidungen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten in einer anderen Niederlassung des Verantwortlichen in der Union getroffen werden; in diesem Fall sollte die

⁽¹⁾ Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45).

letztenannte als Hauptniederlassung gelten. Zur Bestimmung der Hauptniederlassung eines Verantwortlichen in der Union sollten objektive Kriterien herangezogen werden; ein Kriterium sollte dabei die effektive und tatsächliche Ausübung von Managementtätigkeiten durch eine feste Einrichtung sein, in deren Rahmen die Grundsatzentscheidungen zur Festlegung der Zwecke und Mittel der Verarbeitung getroffen werden. Dabei sollte nicht ausschlaggebend sein, ob die Verarbeitung der personenbezogenen Daten tatsächlich an diesem Ort ausgeführt wird. Das Vorhandensein und die Verwendung technischer Mittel und Verfahren zur Verarbeitung personenbezogener Daten oder Verarbeitungstätigkeiten begründen an sich noch keine Hauptniederlassung und sind daher kein ausschlaggebender Faktor für das Bestehen einer Hauptniederlassung. Die Hauptniederlassung des Auftragsverarbeiters sollte der Ort sein, an dem der Auftragsverarbeiter seine Hauptverwaltung in der Union hat, oder — wenn er keine Hauptverwaltung in der Union hat — der Ort, an dem die wesentlichen Verarbeitungstätigkeiten in der Union stattfinden. Sind sowohl der Verantwortliche als auch der Auftragsverarbeiter betroffen, so sollte die Aufsichtsbehörde des Mitgliedstaats, in dem der Verantwortliche seine Hauptniederlassung hat, die zuständige federführende Aufsichtsbehörde bleiben, doch sollte die Aufsichtsbehörde des Auftragsverarbeiters als betroffene Aufsichtsbehörde betrachtet werden und diese Aufsichtsbehörde sollte sich an dem in dieser Verordnung vorgesehenen Verfahren der Zusammenarbeit beteiligen. Auf jeden Fall sollten die Aufsichtsbehörden des Mitgliedstaats oder der Mitgliedstaaten, in dem bzw. denen der Auftragsverarbeiter eine oder mehrere Niederlassungen hat, nicht als betroffene Aufsichtsbehörden betrachtet werden, wenn sich der Beschlussentwurf nur auf den Verantwortlichen bezieht. Wird die Verarbeitung durch eine Unternehmensgruppe vorgenommen, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten, es sei denn, die Zwecke und Mittel der Verarbeitung werden von einem anderen Unternehmen festgelegt.

- (37) Eine Unternehmensgruppe sollte aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen bestehen, wobei das herrschende Unternehmen dasjenige sein sollte, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann. Ein Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, sollte zusammen mit diesen als eine „Unternehmensgruppe“ betrachtet werden.
- (38) Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen. Die Einwilligung des Trägers der elterlichen Verantwortung sollte im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein.
- (39) Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen. Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollten die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen. Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. Es sollten alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.
- (40) Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden, die sich aus dieser Verordnung oder —

wann immer in dieser Verordnung darauf Bezug genommen wird — aus dem sonstigen Unionsrecht oder dem Recht der Mitgliedstaaten ergibt, so unter anderem auf der Grundlage, dass sie zur Erfüllung der rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist.

- (41) Wenn in dieser Verordnung auf eine Rechtsgrundlage oder eine Gesetzgebungsmaßnahme Bezug genommen wird, erfordert dies nicht notwendigerweise einen von einem Parlament angenommenen Gesetzgebungsakt; davon unberührt bleiben Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats. Die entsprechende Rechtsgrundlage oder Gesetzgebungsmaßnahme sollte jedoch klar und präzise sein und ihre Anwendung sollte für die Rechtsunterworfenen gemäß der Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden „Gerichtshof“) und des Europäischen Gerichtshofs für Menschenrechte vorhersehbar sein.
- (42) Erfolgt die Verarbeitung mit Einwilligung der betroffenen Person, sollte der Verantwortliche nachweisen können, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat. Insbesondere bei Abgabe einer schriftlichen Erklärung in anderer Sache sollten Garantien sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt. Gemäß der Richtlinie 93/13/EWG des Rates ⁽¹⁾ sollte eine vom Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden, und sie sollte keine missbräuchlichen Klauseln beinhalten. Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen. Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.
- (43) Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.
- (44) Die Verarbeitung von Daten sollte als rechtmäßig gelten, wenn sie für die Erfüllung oder den geplanten Abschluss eines Vertrags erforderlich ist.
- (45) Erfolgt die Verarbeitung durch den Verantwortlichen aufgrund einer ihm obliegenden rechtlichen Verpflichtung oder ist die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich, muss hierfür eine Grundlage im Unionsrecht oder im Recht eines Mitgliedstaats bestehen. Mit dieser Verordnung wird nicht für jede einzelne Verarbeitung ein spezifisches Gesetz verlangt. Ein Gesetz als Grundlage für mehrere Verarbeitungsvorgänge kann ausreichend sein, wenn die Verarbeitung aufgrund einer dem Verantwortlichen obliegenden rechtlichen Verpflichtung erfolgt oder wenn die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich ist. Desgleichen sollte im Unionsrecht oder im Recht der Mitgliedstaaten geregelt werden, für welche Zwecke die Daten verarbeitet werden dürfen. Ferner könnten in diesem Recht die allgemeinen Bedingungen dieser Verordnung zur Regelung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten präzisiert und es könnte darin festgelegt werden, wie der Verantwortliche zu bestimmen ist, welche Art von personenbezogenen Daten verarbeitet werden, welche Personen betroffen sind, welchen Einrichtungen die personenbezogenen Daten offengelegt, für welche Zwecke und wie lange sie gespeichert werden dürfen und welche anderen Maßnahmen ergriffen werden, um zu gewährleisten, dass die Verarbeitung rechtmäßig und nach Treu und Glauben erfolgt. 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 öffentliche Recht fallende natürliche oder juristische Person oder, sofern dies durch das öffentliche Interesse einschließlich gesundheitlicher Zwecke, wie die öffentliche Gesundheit oder die soziale Sicherheit oder die Verwaltung von Leistungen der Gesundheitsfürsorge, gerechtfertigt ist, eine natürliche oder juristische Person des Privatrechts, wie beispielsweise eine Berufseinigung, handeln sollte.
- (46) Die Verarbeitung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein lebenswichtiges Interesse der betroffenen Person oder einer anderen natürlichen Person zu schützen. Personenbezogene Daten sollten grundsätzlich nur dann aufgrund eines lebenswichtigen Interesses einer anderen natürlichen Person verarbeitet werden, wenn die Verarbeitung offensichtlich nicht auf eine andere

⁽¹⁾ Richtlinie 93/13/EWG des Rates vom 5. April 1993 über missbräuchliche Klauseln in Verbraucherverträgen (ABl. L 95 vom 21.4.1993, S. 29).

Rechtsgrundlage gestützt werden kann. Einige Arten der Verarbeitung können sowohl wichtigen Gründen des öffentlichen Interesses als auch lebenswichtigen Interessen der betroffenen Person dienen; so kann beispielsweise die Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen erforderlich sein.

- (47) Die Rechtmäßigkeit der Verarbeitung kann durch die berechtigten Interessen eines Verantwortlichen, auch eines Verantwortlichen, dem die personenbezogenen Daten offengelegt werden dürfen, oder eines Dritten begründet sein, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen; dabei sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen. Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht. Auf jeden Fall wäre das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen. Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, sollte diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten, die diese in Erfüllung ihrer Aufgaben vornehmen. Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.
- (48) Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt.
- (49) Die Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams — CERT, beziehungsweise Computer Security Incident Response Teams — CSIRT), Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten stellt in dem Maße ein berechtigtes Interesse des jeweiligen Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service“-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.
- (50) Die Verarbeitung personenbezogener Daten für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden, sollte nur zulässig sein, wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten. Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, so können im Unionsrecht oder im Recht der Mitgliedstaaten die Aufgaben und Zwecke bestimmt und konkretisiert werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird. Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke sollte als vereinbar und rechtmäßiger Verarbeitungsvorgang gelten. Die im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehene Rechtsgrundlage für die Verarbeitung personenbezogener Daten kann auch als Rechtsgrundlage für eine Weiterverarbeitung dienen. Um festzustellen, ob ein Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, sollte der Verantwortliche nach Einhaltung aller Anforderungen für die Rechtmäßigkeit der ursprünglichen Verarbeitung unter anderem prüfen, ob ein Zusammenhang zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung besteht, in welchem Kontext die Daten erhoben wurden, insbesondere die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten, um welche Art von personenbezogenen Daten es sich handelt, welche Folgen die beabsichtigte Weiterverarbeitung für die betroffenen Personen

hat und ob sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang geeignete Garantien bestehen.

Hat die betroffene Person ihre Einwilligung erteilt oder beruht die Verarbeitung auf Unionsrecht oder dem Recht der Mitgliedstaaten, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt, so sollte der Verantwortliche die personenbezogenen Daten ungeachtet der Vereinbarkeit der Zwecke weiterverarbeiten dürfen. In jedem Fall sollte gewährleistet sein, dass die in dieser Verordnung niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über diese anderen Zwecke und über ihre Rechte einschließlich des Widerspruchsrechts unterrichtet wird. Der Hinweis des Verantwortlichen auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit und die Übermittlung der maßgeblichen personenbezogenen Daten in Einzelfällen oder in mehreren Fällen, die im Zusammenhang mit derselben Straftat oder derselben Bedrohung der öffentlichen Sicherheit stehen, an eine zuständige Behörde sollten als berechtigtes Interesse des Verantwortlichen gelten. Eine derartige Übermittlung personenbezogener Daten im berechtigten Interesse des Verantwortlichen oder deren Weiterverarbeitung sollte jedoch unzulässig sein, wenn die Verarbeitung mit einer rechtlichen, beruflichen oder sonstigen verbindlichen Pflicht zur Geheimhaltung unvereinbar ist.

- (51) Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können. Diese personenbezogenen Daten sollten personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft hervorgeht, wobei die Verwendung des Begriffs „rassische Herkunft“ in dieser Verordnung nicht bedeutet, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt. Die Verarbeitung von Lichtbildern sollte nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs „biometrische Daten“ erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Derartige personenbezogene Daten sollten nicht verarbeitet werden, es sei denn, die Verarbeitung ist in den in dieser Verordnung dargelegten besonderen Fällen zulässig, wobei zu berücksichtigen ist, dass im Recht der Mitgliedstaaten besondere Datenschutzbestimmungen festgelegt sein können, um die Anwendung der Bestimmungen dieser Verordnung anzupassen, damit die Einhaltung einer rechtlichen Verpflichtung oder die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, möglich ist. Zusätzlich zu den speziellen Anforderungen an eine derartige Verarbeitung sollten die allgemeinen Grundsätze und andere Bestimmungen dieser Verordnung, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung, gelten. Ausnahmen von dem allgemeinen Verbot der Verarbeitung dieser besonderen Kategorien personenbezogener Daten sollten ausdrücklich vorgesehen werden, unter anderem bei ausdrücklicher Einwilligung der betroffenen Person oder bei bestimmten Notwendigkeiten, insbesondere wenn die Verarbeitung im Rahmen rechtmäßiger Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, die sich für die Ausübung von Grundfreiheiten einsetzen.
- (52) Ausnahmen vom Verbot der Verarbeitung besonderer Kategorien von personenbezogenen Daten sollten auch erlaubt sein, wenn sie im Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen sind, und — vorbehaltlich angemessener Garantien zum Schutz der personenbezogenen Daten und anderer Grundrechte — wenn dies durch das öffentliche Interesse gerechtfertigt ist, insbesondere für die Verarbeitung von personenbezogenen Daten auf dem Gebiet des Arbeitsrechts und des Rechts der sozialen Sicherheit einschließlich Renten und zwecks Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen, Prävention oder Kontrolle ansteckender Krankheiten und anderer schwerwiegender Gesundheitsgefahren. Eine solche Ausnahme kann zu gesundheitlichen Zwecken gemacht werden, wie der Gewährleistung der öffentlichen Gesundheit und der Verwaltung von Leistungen der Gesundheitsversorgung, insbesondere wenn dadurch die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen sichergestellt werden soll, oder wenn die Verarbeitung im öffentlichen Interesse liegenden Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken dient. Die Verarbeitung solcher personenbezogener Daten sollte zudem ausnahmsweise erlaubt sein, wenn sie erforderlich ist, um rechtliche Ansprüche, sei es in einem Gerichtsverfahren oder in einem Verwaltungsverfahren oder einem außergerichtlichen Verfahren, geltend zu machen, auszuüben oder zu verteidigen.
- (53) Besondere Kategorien personenbezogener Daten, die eines höheren Schutzes verdienen, sollten nur dann für gesundheitsbezogene Zwecke verarbeitet werden, wenn dies für das Erreichen dieser Zwecke im Interesse einzelner natürlicher Personen und der Gesellschaft insgesamt erforderlich ist, insbesondere im Zusammenhang mit der Verwaltung der Dienste und Systeme des Gesundheits- oder Sozialbereichs, einschließlich der Verarbeitung dieser Daten durch die Verwaltung und die zentralen nationalen Gesundheitsbehörden zwecks Qualitätskontrolle, Verwaltungsinformationen und der allgemeinen nationalen und lokalen Überwachung des Gesundheitssystems oder des Sozialsystems und zwecks Gewährleistung der Kontinuität der Gesundheits- und Sozialfürsorge und der grenzüberschreitenden Gesundheitsversorgung oder Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen oder für im öffentlichen Interesse liegende Archive, zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken, die auf Rechtsvorschriften

der Union oder der Mitgliedstaaten beruhen, die einem im öffentlichen Interesse liegenden Ziel dienen müssen, sowie für Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Diese Verordnung sollte daher harmonisierte Bedingungen für die Verarbeitung besonderer Kategorien personenbezogener Gesundheitsdaten im Hinblick auf bestimmte Erfordernisse harmonisieren, insbesondere wenn die Verarbeitung dieser Daten für gesundheitsbezogene Zwecke von Personen durchgeführt wird, die gemäß einer rechtlichen Verpflichtung dem Berufsgeheimnis unterliegen. Im Recht der Union oder der Mitgliedstaaten sollten besondere und angemessene Maßnahmen zum Schutz der Grundrechte und der personenbezogenen Daten natürlicher Personen vorgesehen werden. Den Mitgliedstaaten sollte gestattet werden, weitere Bedingungen — einschließlich Beschränkungen — in Bezug auf die Verarbeitung von genetischen Daten, biometrischen Daten oder Gesundheitsdaten beizubehalten oder einzuführen. Dies sollte jedoch den freien Verkehr personenbezogener Daten innerhalb der Union nicht beeinträchtigen, falls die betreffenden Bedingungen für die grenzüberschreitende Verarbeitung solcher Daten gelten.

- (54) Aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit kann es notwendig sein, besondere Kategorien personenbezogener Daten auch ohne Einwilligung der betroffenen Person zu verarbeiten. Diese Verarbeitung sollte angemessenen und besonderen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen unterliegen. In diesem Zusammenhang sollte der Begriff „öffentliche Gesundheit“ im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates⁽¹⁾ ausgelegt werden und alle Elemente im Zusammenhang mit der Gesundheit wie den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von Gesundheitsversorgungsleistungen und den allgemeinen Zugang zu diesen Leistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen. Eine solche Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber oder Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten.
- (55) Auch die Verarbeitung personenbezogener Daten durch staatliche Stellen zu verfassungsrechtlich oder völkerrechtlich verankerten Zielen von staatlich anerkannten Religionsgemeinschaften erfolgt aus Gründen des öffentlichen Interesses.
- (56) Wenn es in einem Mitgliedstaat das Funktionieren des demokratischen Systems erfordert, dass die politischen Parteien im Zusammenhang mit Wahlen personenbezogene Daten über die politische Einstellung von Personen sammeln, kann die Verarbeitung derartiger Daten aus Gründen des öffentlichen Interesses zugelassen werden, sofern geeignete Garantien vorgesehen werden.
- (57) Kann der Verantwortliche anhand der von ihm verarbeiteten personenbezogenen Daten eine natürliche Person nicht identifizieren, so sollte er nicht verpflichtet sein, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu identifizieren. Allerdings sollte er sich nicht weigern, zusätzliche Informationen entgegenzunehmen, die von der betroffenen Person beigebracht werden, um ihre Rechte geltend zu machen. Die Identifizierung sollte die digitale Identifizierung einer betroffenen Person — beispielsweise durch Authentifizierungsverfahren etwa mit denselben Berechtigungsnachweisen, wie sie die betroffene Person verwendet, um sich bei dem von dem Verantwortlichen bereitgestellten Online-Dienst anzumelden — einschließen.
- (58) Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden. Diese Information könnte in elektronischer Form bereitgestellt werden, beispielsweise auf einer Website, wenn sie für die Öffentlichkeit bestimmt ist. Dies gilt insbesondere für Situationen, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik es der betroffenen Person schwer machen, zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden, wie etwa bei der Werbung im Internet. Wenn sich die Verarbeitung an Kinder richtet, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann.
- (59) Es sollten Modalitäten festgelegt werden, die einer betroffenen Person die Ausübung der Rechte, die ihr nach dieser Verordnung zustehen, erleichtern, darunter auch Mechanismen, die dafür sorgen, dass sie unentgeltlich insbesondere Zugang zu personenbezogenen Daten und deren Berichtigung oder Löschung beantragen und gegebenenfalls erhalten oder von ihrem Widerspruchsrecht Gebrauch machen kann. So sollte der Verantwortliche auch dafür sorgen, dass Anträge elektronisch gestellt werden können, insbesondere wenn die personenbezogenen Daten elektronisch verarbeitet werden. Der Verantwortliche sollte verpflichtet werden, den Antrag der betroffenen Person unverzüglich, spätestens aber innerhalb eines Monats zu beantworten und gegebenenfalls zu begründen, warum er den Antrag ablehnt.

⁽¹⁾ Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 zu Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz (ABl. L 354 vom 31.12.2008, S. 70).

- (60) Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird. Der Verantwortliche sollte der betroffenen Person alle weiteren Informationen zur Verfügung stellen, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten. Darüber hinaus sollte er die betroffene Person darauf hinweisen, dass Profiling stattfindet und welche Folgen dies hat. Werden die personenbezogenen Daten bei der betroffenen Person erhoben, so sollte dieser darüber hinaus mitgeteilt werden, ob sie verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche Folgen eine Zurückhaltung der Daten nach sich ziehen würde. Die betreffenden Informationen können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, so sollten sie maschinenlesbar sein.
- (61) Dass sie betreffende personenbezogene Daten verarbeitet werden, sollte der betroffenen Person zum Zeitpunkt der Erhebung mitgeteilt werden oder, falls die Daten nicht von ihr, sondern aus einer anderen Quelle erlangt werden, innerhalb einer angemessenen Frist, die sich nach dem konkreten Einzelfall richtet. Wenn die personenbezogenen Daten rechtmäßig einem anderen Empfänger offengelegt werden dürfen, sollte die betroffene Person bei der erstmaligen Offenlegung der personenbezogenen Daten für diesen Empfänger darüber aufgeklärt werden. Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck zu verarbeiten als den, für den die Daten erhoben wurden, so sollte er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und andere erforderliche Informationen zur Verfügung stellen. Konnte der betroffenen Person nicht mitgeteilt werden, woher die personenbezogenen Daten stammen, weil verschiedene Quellen benutzt wurden, so sollte die Unterrichtung allgemein gehalten werden.
- (62) Die Pflicht, Informationen zur Verfügung zu stellen, erübrigt sich jedoch, wenn die betroffene Person die Information bereits hat, wenn die Speicherung oder Offenlegung der personenbezogenen Daten ausdrücklich durch Rechtsvorschriften geregelt ist oder wenn sich die Unterrichtung der betroffenen Person als unmöglich erweist oder mit unverhältnismäßig hohem Aufwand verbunden ist. Letzteres könnte insbesondere bei Verarbeitungen für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken der Fall sein. Als Anhaltspunkte sollten dabei die Zahl der betroffenen Personen, das Alter der Daten oder etwaige geeignete Garantien in Betracht gezogen werden.
- (63) Eine betroffene Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Dies schließt das Recht betroffene Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten. Jede betroffene Person sollte daher ein Anrecht darauf haben zu wissen und zu erfahren, insbesondere zu welchen Zwecken die personenbezogenen Daten verarbeitet werden und, wenn möglich, wie lange sie gespeichert werden, wer die Empfänger der personenbezogenen Daten sind, nach welcher Logik die automatische Verarbeitung personenbezogener Daten erfolgt und welche Folgen eine solche Verarbeitung haben kann, zumindest in Fällen, in denen die Verarbeitung auf Profiling beruht. Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde. Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird. Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt.
- (64) Der Verantwortliche sollte alle vertretbaren Mittel nutzen, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen, insbesondere im Rahmen von Online-Diensten und im Fall von Online-Kennungen. Ein Verantwortlicher sollte personenbezogene Daten nicht allein zu dem Zweck speichern, auf mögliche Auskunftsersuchen reagieren zu können.
- (65) Eine betroffene Person sollte ein Recht auf Berichtigung der sie betreffenden personenbezogenen Daten besitzen sowie ein „Recht auf Vergessenwerden“, wenn die Speicherung ihrer Daten gegen diese Verordnung oder gegen das Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, verstößt. Insbesondere sollten betroffene Personen Anspruch darauf haben, dass ihre personenbezogenen Daten gelöscht und nicht mehr verarbeitet werden, wenn die personenbezogenen Daten hinsichtlich der Zwecke, für die sie erhoben bzw. anderweitig verarbeitet wurden, nicht mehr benötigt werden, wenn die betroffenen Personen ihre Einwilligung in die Verarbeitung widerrufen oder Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten eingelegt haben oder wenn die Verarbeitung ihrer personenbezogenen Daten aus anderen Gründen gegen diese Verordnung verstößt. Dieses Recht ist insbesondere wichtig in Fällen, in denen die betroffene Person ihre Einwilligung noch im Kindesalter gegeben hat und insofern die mit der Verarbeitung verbundenen Gefahren nicht

in vollem Umfang absehen konnte und die personenbezogenen Daten — insbesondere die im Internet gespeicherten — später löschen möchte. Die betroffene Person sollte dieses Recht auch dann ausüben können, wenn sie kein Kind mehr ist. Die weitere Speicherung der personenbezogenen Daten sollte jedoch rechtmäßig sein, wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

- (66) Um dem „Recht auf Vergessenwerden“ im Netz mehr Geltung zu verschaffen, sollte das Recht auf Löschung ausgeweitet werden, indem ein Verantwortlicher, der die personenbezogenen Daten öffentlich gemacht hat, verpflichtet wird, den Verantwortlichen, die diese personenbezogenen Daten verarbeiten, mitzuteilen, alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen der personenbezogenen Daten zu löschen. Dabei sollte der Verantwortliche, unter Berücksichtigung der verfügbaren Technologien und der ihm zur Verfügung stehenden Mittel, angemessene Maßnahmen — auch technischer Art — treffen, um die Verantwortlichen, die diese personenbezogenen Daten verarbeiten, über den Antrag der betroffenen Person zu informieren.
- (67) Methoden zur Beschränkung der Verarbeitung personenbezogener Daten könnten unter anderem darin bestehen, dass ausgewählte personenbezogenen Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzer gesperrt werden oder dass veröffentlichte Daten vorübergehend von einer Website entfernt werden. In automatisierten Dateisystemen sollte die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel so erfolgen, dass die personenbezogenen Daten in keiner Weise weiterverarbeitet werden und nicht verändert werden können. Auf die Tatsache, dass die Verarbeitung der personenbezogenen Daten beschränkt wurde, sollte in dem System unmissverständlich hingewiesen werden.
- (68) Um im Fall der Verarbeitung personenbezogener Daten mit automatischen Mitteln eine bessere Kontrolle über die eigenen Daten zu haben, sollte die betroffene Person außerdem berechtigt sein, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten und sie einem anderen Verantwortlichen zu übermitteln. Die Verantwortlichen sollten dazu aufgefordert werden, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen. Dieses Recht sollte dann gelten, wenn die betroffene Person die personenbezogenen Daten mit ihrer Einwilligung zur Verfügung gestellt hat oder die Verarbeitung zur Erfüllung eines Vertrags erforderlich ist. Es sollte nicht gelten, wenn die Verarbeitung auf einer anderen Rechtsgrundlage als ihrer Einwilligung oder eines Vertrags erfolgt. Dieses Recht sollte naturgemäß nicht gegen Verantwortliche ausgeübt werden, die personenbezogenen Daten in Erfüllung ihrer öffentlichen Aufgaben verarbeiten. Es sollte daher nicht gelten, wenn die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder für die Wahrnehmung einer ihm übertragenen Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung einer ihm übertragenen öffentlichen Gewalt erfolgt, erforderlich ist. Das Recht der betroffenen Person, sie betreffende personenbezogene Daten zu übermitteln oder zu empfangen, sollte für den Verantwortlichen nicht die Pflicht begründen, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten. Ist im Fall eines bestimmten Satzes personenbezogener Daten mehr als eine betroffene Person tangiert, so sollte das Recht auf Empfang der Daten die Grundrechte und Grundfreiheiten anderer betroffener Personen nach dieser Verordnung unberührt lassen. Dieses Recht sollte zudem das Recht der betroffenen Person auf Löschung ihrer personenbezogenen Daten und die Beschränkungen dieses Rechts gemäß dieser Verordnung nicht berühren und insbesondere nicht bedeuten, dass die Daten, die sich auf die betroffene Person beziehen und von ihr zur Erfüllung eines Vertrags zur Verfügung gestellt worden sind, gelöscht werden, soweit und solange diese personenbezogenen Daten für die Erfüllung des Vertrags notwendig sind. Soweit technisch machbar, sollte die betroffene Person das Recht haben, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden.
- (69) Dürfen die personenbezogenen Daten möglicherweise rechtmäßig verarbeitet werden, weil die Verarbeitung für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt — die dem Verantwortlichen übertragen wurde, — oder aufgrund des berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist, sollte jede betroffene Person trotzdem das Recht haben, Widerspruch gegen die Verarbeitung der sich aus ihrer besonderen Situation ergebenden personenbezogenen Daten einzulegen. Der für die Verarbeitung Verantwortliche sollte darlegen müssen, dass seine zwingenden berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben.
- (70) Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so sollte die betroffene Person jederzeit unentgeltlich insoweit Widerspruch gegen eine solche — ursprüngliche oder spätere — Verarbeitung einschließlich des Profiling einlegen können, als sie mit dieser Direktwerbung zusammenhängt. Die betroffene Person sollte ausdrücklich auf dieses Recht hingewiesen werden; dieser Hinweis sollte in einer verständlichen und von anderen Informationen getrennten Form erfolgen.

- (71) Die betroffene Person sollte das Recht haben, keiner Entscheidung — was eine Maßnahme einschließen kann — zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie die automatische Ablehnung eines Online-Kreditanspruchs oder Online-Einstellungsverfahrens ohne jegliches menschliche Eingreifen. Zu einer derartigen Verarbeitung zählt auch das „Profiling“, das in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person besteht, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Eine auf einer derartigen Verarbeitung, einschließlich des Profilings, beruhende Entscheidungsfindung sollte allerdings erlaubt sein, wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der für die Verarbeitung Verantwortliche unterliegt, ausdrücklich zulässig ist, auch um im Einklang mit den Vorschriften, Standards und Empfehlungen der Institutionen der Union oder der nationalen Aufsichtsgremien Betrug und Steuerhinterziehung zu überwachen und zu verhindern und die Sicherheit und Zuverlässigkeit eines von dem Verantwortlichen bereitgestellten Dienstes zu gewährleisten, oder wenn dies für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und einem Verantwortlichen erforderlich ist oder wenn die betroffene Person ihre ausdrückliche Einwilligung hierzu erteilt hat. In jedem Fall sollte eine solche Verarbeitung mit angemessenen Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person und des Anspruchs auf direktes Eingreifen einer Person, auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf Anfechtung der Entscheidung. Diese Maßnahme sollte kein Kind betreffen.

Um unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten, sollte der für die Verarbeitung Verantwortliche geeignete mathematische oder statistische Verfahren für das Profiling verwenden, technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird, und personenbezogene Daten in einer Weise sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird und mit denen verhindert wird, dass es gegenüber natürlichen Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung zu diskriminierenden Wirkungen oder zu Maßnahmen kommt, die eine solche Wirkung haben. Automatisierte Entscheidungsfindung und Profiling auf der Grundlage besonderer Kategorien von personenbezogenen Daten sollten nur unter bestimmten Bedingungen erlaubt sein.

- (72) Das Profiling unterliegt den Vorschriften dieser Verordnung für die Verarbeitung personenbezogener Daten, wie etwa die Rechtsgrundlage für die Verarbeitung oder die Datenschutzgrundsätze. Der durch diese Verordnung eingerichtete Europäische Datenschutzausschuss (im Folgenden „Ausschuss“) sollte, diesbezüglich Leitlinien herausgeben können.
- (73) Im Recht der Union oder der Mitgliedstaaten können Beschränkungen hinsichtlich bestimmter Grundsätze und hinsichtlich des Rechts auf Unterrichtung, Auskunft zu und Berichtigung oder Löschung personenbezogener Daten, des Rechts auf Datenübertragbarkeit und Widerspruch, Entscheidungen, die auf der Erstellung von Profilen beruhen, sowie Mitteilungen über eine Verletzung des Schutzes personenbezogener Daten an eine betroffene Person und bestimmten damit zusammenhängenden Pflichten der Verantwortlichen vorgesehen werden, soweit dies in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um die öffentliche Sicherheit aufrechtzuerhalten, wozu unter anderem der Schutz von Menschenleben insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen, die Verhütung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung — was auch den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt — oder die Verhütung, Aufdeckung und Verfolgung von Verstößen gegen Berufsstandsregeln bei reglementierten Berufen, das Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen Interesses sowie die Weiterverarbeitung von archivierten personenbezogenen Daten zur Bereitstellung spezifischer Informationen im Zusammenhang mit dem politischen Verhalten unter ehemaligen totalitären Regimen gehört, und zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, etwa wichtige wirtschaftliche oder finanzielle Interessen, oder die betroffene Person und die Rechte und Freiheiten anderer Personen, einschließlich in den Bereichen soziale Sicherheit, öffentliche Gesundheit und humanitäre Hilfe, zu schützen. Diese Beschränkungen sollten mit der Charta und mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten im Einklang stehen.
- (74) Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind. Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen.

- (75) Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.
- (76) Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.
- (77) Anleitungen, wie der Verantwortliche oder Auftragsverarbeiter geeignete Maßnahmen durchzuführen hat und wie die Einhaltung der Anforderungen nachzuweisen ist, insbesondere was die Ermittlung des mit der Verarbeitung verbundenen Risikos, dessen Abschätzung in Bezug auf Ursache, Art, Eintrittswahrscheinlichkeit und Schwere und die Festlegung bewährter Verfahren für dessen Eindämmung betrifft, könnten insbesondere in Form von genehmigten Verhaltensregeln, genehmigten Zertifizierungsverfahren, Leitlinien des Ausschusses oder Hinweisen eines Datenschutzbeauftragten gegeben werden. Der Ausschuss kann ferner Leitlinien für Verarbeitungsvorgänge ausgeben, bei denen davon auszugehen ist, dass sie kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, und angeben, welche Abhilfemaßnahmen in diesen Fällen ausreichend sein können.
- (78) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.
- (79) Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter bedarf es — auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden — einer klaren Zuteilung der Verantwortlichkeiten durch diese Verordnung, einschließlich der Fälle, in denen ein Verantwortlicher die Verarbeitungszwecke und -mittel gemeinsam mit anderen Verantwortlichen festlegt oder ein Verarbeitungsvorgang im Auftrag eines Verantwortlichen durchgeführt wird.
- (80) Jeder Verantwortliche oder Auftragsverarbeiter ohne Niederlassung in der Union, dessen Verarbeitungstätigkeiten sich auf betroffene Personen beziehen, die sich in der Union aufhalten, und dazu dienen, diesen Personen in der Union Waren oder Dienstleistungen anzubieten — unabhängig davon, ob von der betroffenen Person eine Zahlung verlangt wird — oder deren Verhalten, soweit dieses innerhalb der Union erfolgt, zu beobachten, sollte einen Vertreter benennen müssen, es sei denn, die Verarbeitung erfolgt gelegentlich, schließt nicht die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten oder die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten ein und bringt unter Berücksichtigung ihrer

Art, ihrer Umstände, ihres Umfangs und ihrer Zwecke wahrscheinlich kein Risiko für die Rechte und Freiheiten natürlicher Personen mit sich oder bei dem Verantwortlichen handelt es sich um eine Behörde oder öffentliche Stelle. Der Vertreter sollte im Namen des Verantwortlichen oder des Auftragsverarbeiters tätig werden und den Aufsichtsbehörden als Anlaufstelle dienen. Der Verantwortliche oder der Auftragsverarbeiter sollte den Vertreter ausdrücklich bestellen und schriftlich beauftragen, in Bezug auf die ihm nach dieser Verordnung obliegenden Verpflichtungen an seiner Stelle zu handeln. Die Benennung eines solchen Vertreters berührt nicht die Verantwortung oder Haftung des Verantwortlichen oder des Auftragsverarbeiters nach Maßgabe dieser Verordnung. Ein solcher Vertreter sollte seine Aufgaben entsprechend dem Mandat des Verantwortlichen oder Auftragsverarbeiters ausführen und insbesondere mit den zuständigen Aufsichtsbehörden in Bezug auf Maßnahmen, die die Einhaltung dieser Verordnung sicherstellen sollen, zusammenarbeiten. Bei Verstößen des Verantwortlichen oder Auftragsverarbeiters sollte der bestellte Vertreter Durchsetzungsverfahren unterworfen werden.

- (81) Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des Verantwortlichen vorzunehmende Verarbeitung eingehalten werden, sollte ein Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, nur Auftragsverarbeiter heranziehen, die — insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen — hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen — auch für die Sicherheit der Verarbeitung — getroffen werden, die den Anforderungen dieser Verordnung genügen. Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Union oder der Mitgliedstaaten erfolgen, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind, wobei die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind. Der Verantwortliche und der Auftragsverarbeiter können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden, die entweder unmittelbar von der Kommission erlassen oder aber nach dem Kohärenzverfahren von einer Aufsichtsbehörde angenommen und dann von der Kommission erlassen wurden. Nach Beendigung der Verarbeitung im Namen des Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten nach Wahl des Verantwortlichen entweder zurückgeben oder löschen, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
- (82) Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.
- (83) Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau — auch hinsichtlich der Vertraulichkeit — gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden, wie etwa — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte.
- (84) Damit diese Verordnung in Fällen, in denen die Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, besser eingehalten wird, sollte der Verantwortliche für die Durchführung einer Datenschutz-Folgenabschätzung, mit der insbesondere die Ursache, Art, Besonderheit und Schwere dieses Risikos evaluiert werden, verantwortlich sein. Die Ergebnisse der Abschätzung sollten berücksichtigt werden, wenn darüber entschieden wird, welche geeigneten Maßnahmen ergriffen werden müssen, um nachzuweisen, dass die Verarbeitung der personenbezogenen Daten mit dieser Verordnung in Einklang steht. Geht aus einer Datenschutz-Folgenabschätzung hervor, dass Verarbeitungsvorgänge ein hohes Risiko bergen, das der Verantwortliche nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten eindämmen kann, so sollte die Aufsichtsbehörde vor der Verarbeitung konsultiert werden.
- (85) Eine Verletzung des Schutzes personenbezogener Daten kann — wenn nicht rechtzeitig und angemessen reagiert wird — einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte,

Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person. Deshalb sollte der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, unterrichten, es sei denn, der Verantwortliche kann im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Falls diese Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen, und die Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.

- (86) Der für die Verarbeitung Verantwortliche sollte die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten benachrichtigen, wenn diese Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt, damit diese die erforderlichen Vorkehrungen treffen können. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene natürliche Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Solche Benachrichtigungen der betroffenen Person sollten stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden wie beispielsweise Strafverfolgungsbehörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müssten betroffene Personen sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen.
- (87) Es sollte festgestellt werden, ob alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können. Bei der Feststellung, ob die Meldung unverzüglich erfolgt ist, sollten die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren Folgen und nachteilige Auswirkungen für die betroffene Person berücksichtigt werden. Die entsprechende Meldung kann zu einem Tätigwerden der Aufsichtsbehörde im Einklang mit ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen führen.
- (88) Bei der detaillierten Regelung des Formats und der Verfahren für die Meldung von Verletzungen des Schutzes personenbezogener Daten sollten die Umstände der Verletzung hinreichend berücksichtigt werden, beispielsweise ob personenbezogene Daten durch geeignete technische Sicherheitsvorkehrungen geschützt waren, die die Wahrscheinlichkeit eines Identitätsbetrugs oder anderer Formen des Datenmissbrauchs wirksam verringern. Überdies sollten solche Regeln und Verfahren den berechtigten Interessen der Strafverfolgungsbehörden in Fällen Rechnung tragen, in denen die Untersuchung der Umstände einer Verletzung des Schutzes personenbezogener Daten durch eine frühzeitige Offenlegung in unnötiger Weise behindert würde.
- (89) Gemäß der Richtlinie 95/46/EG waren Verarbeitungen personenbezogener Daten bei den Aufsichtsbehörden generell meldepflichtig. Diese Meldepflicht ist mit einem bürokratischen und finanziellen Aufwand verbunden und hat dennoch nicht in allen Fällen zu einem besseren Schutz personenbezogener Daten geführt. Diese unterschiedslosen allgemeinen Meldepflichten sollten daher abgeschafft und durch wirksame Verfahren und Mechanismen ersetzt werden, die sich stattdessen vorrangig mit denjenigen Arten von Verarbeitungsvorgängen befassen, die aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen. Zu solchen Arten von Verarbeitungsvorgängen gehören insbesondere solche, bei denen neue Technologien eingesetzt werden oder die neuartig sind und bei denen der Verantwortliche noch keine Datenschutz-Folgenabschätzung durchgeführt hat bzw. bei denen aufgrund der seit der ursprünglichen Verarbeitung vergangenen Zeit eine Datenschutz-Folgenabschätzung notwendig geworden ist.
- (90) In derartigen Fällen sollte der Verantwortliche vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchführen, mit der die spezifische Eintrittswahrscheinlichkeit und die Schwere dieses hohen Risikos unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Ursachen des Risikos bewertet werden. Diese Folgenabschätzung sollte sich insbesondere mit den Maßnahmen, Garantien und Verfahren befassen, durch die dieses Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden soll.
- (91) Dies sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und — beispielsweise aufgrund ihrer Sensibilität — wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird, sowie für andere Verarbeitungsvorgänge, die ein hohes Risiko für die

Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren. Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, wenn die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßnahmen verarbeitet werden. Gleichermaßen erforderlich ist eine Datenschutz-Folgenabschätzung für die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen, oder für alle anderen Vorgänge, bei denen nach Auffassung der zuständigen Aufsichtsbehörde die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, insbesondere weil sie die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern oder weil sie systematisch in großem Umfang erfolgen. Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogener Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.

- (92) Unter bestimmten Umständen kann es vernünftig und unter ökonomischen Gesichtspunkten zweckmäßig sein, eine Datenschutz-Folgenabschätzung nicht lediglich auf ein bestimmtes Projekt zu beziehen, sondern sie thematisch breiter anzulegen — beispielsweise wenn Behörden oder öffentliche Stellen eine gemeinsame Anwendung oder Verarbeitungsplattform schaffen möchten oder wenn mehrere Verantwortliche eine gemeinsame Anwendung oder Verarbeitungsumgebung für einen gesamten Wirtschaftssektor, für ein bestimmtes Marktsegment oder für eine weit verbreitete horizontale Tätigkeit einführen möchten.
- (93) Anlässlich des Erlasses des Gesetzes des Mitgliedstaats, auf dessen Grundlage die Behörde oder öffentliche Stelle ihre Aufgaben wahrnimmt und das den fraglichen Verarbeitungsvorgang oder die fraglichen Arten von Verarbeitungsvorgängen regelt, können die Mitgliedstaaten es für erforderlich erachten, solche Folgeabschätzungen vor den Verarbeitungsvorgängen durchzuführen.
- (94) Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung bei Fehlen von Garantien, Sicherheitsvorkehrungen und Mechanismen zur Minderung des Risikos ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen würde, und ist der Verantwortliche der Auffassung, dass das Risiko nicht durch in Bezug auf verfügbare Technologien und Implementierungskosten vertretbare Mittel eingedämmt werden kann, so sollte die Aufsichtsbehörde vor Beginn der Verarbeitungstätigkeiten konsultiert werden. Ein solches hohes Risiko ist wahrscheinlich mit bestimmten Arten der Verarbeitung und dem Umfang und der Häufigkeit der Verarbeitung verbunden, die für natürliche Personen auch eine Schädigung oder eine Beeinträchtigung der persönlichen Rechte und Freiheiten mit sich bringen können. Die Aufsichtsbehörde sollte das Beratungsersuchen innerhalb einer bestimmten Frist beantworten. Allerdings kann sie, auch wenn sie nicht innerhalb dieser Frist reagiert hat, entsprechend ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen eingreifen, was die Befugnis einschließt, Verarbeitungsvorgänge zu untersagen. Im Rahmen dieses Konsultationsprozesses kann das Ergebnis einer im Hinblick auf die betreffende Verarbeitung personenbezogener Daten durchgeführten Datenschutz-Folgenabschätzung der Aufsichtsbehörde unterbreitet werden; dies gilt insbesondere für die zur Eindämmung des Risikos für die Rechte und Freiheiten natürlicher Personen geplanten Maßnahmen.
- (95) Der Auftragsverarbeiter sollte erforderlichenfalls den Verantwortlichen auf Anfrage bei der Gewährleistung der Einhaltung der sich aus der Durchführung der Datenschutz-Folgenabschätzung und der vorherigen Konsultation der Aufsichtsbehörde ergebenden Auflagen unterstützen.
- (96) Eine Konsultation der Aufsichtsbehörde sollte auch während der Ausarbeitung von Gesetzes- oder Regelungsvorschriften, in denen eine Verarbeitung personenbezogener Daten vorgesehen ist, erfolgen, um die Vereinbarkeit der geplanten Verarbeitung mit dieser Verordnung sicherzustellen und insbesondere das mit ihr für die betroffene Person verbundene Risiko einzudämmen.
- (97) In Fällen, in denen die Verarbeitung durch eine Behörde — mit Ausnahmen von Gerichten oder unabhängigen Justizbehörden, die im Rahmen ihrer justiziellen Tätigkeit handeln —, im privaten Sektor durch einen Verantwortlichen erfolgt, dessen Kerntätigkeit in Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfordern, oder wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht, sollte der Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der internen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person, die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt, unterstützt werden. Im privaten Sektor bezieht sich die Kerntätigkeit eines Verantwortlichen auf seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als

Nebentätigkeit. Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die von dem Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich bei ihnen um Beschäftigte des Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.

- (98) Verbände oder andere Vereinigungen, die bestimmte Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, sollten ermutigt werden, in den Grenzen dieser Verordnung Verhaltensregeln auszuarbeiten, um eine wirksame Anwendung dieser Verordnung zu erleichtern, wobei den Besonderheiten der in bestimmten Sektoren erfolgenden Verarbeitungen und den besonderen Bedürfnissen der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen ist. Insbesondere könnten in diesen Verhaltensregeln — unter Berücksichtigung des mit der Verarbeitung wahrscheinlich einhergehenden Risikos für die Rechte und Freiheiten natürlicher Personen — die Pflichten der Verantwortlichen und der Auftragsverarbeiter bestimmt werden.
- (99) Bei der Ausarbeitung oder bei der Änderung oder Erweiterung solcher Verhaltensregeln sollten Verbände und oder andere Vereinigungen, die bestimmte Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, die maßgeblichen Interessenträger, möglichst auch die betroffenen Personen, konsultieren und die Eingaben und Stellungnahmen, die sie dabei erhalten, berücksichtigen.
- (100) Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.
- (101) Der Fluss personenbezogener Daten aus Drittländern und internationalen Organisationen und in Drittländer und internationale Organisationen ist für die Ausweitung des internationalen Handels und der internationalen Zusammenarbeit notwendig. Durch die Zunahme dieser Datenströme sind neue Herausforderungen und Anforderungen in Bezug auf den Schutz personenbezogener Daten entstanden. Das durch diese Verordnung unionsweit gewährleistete Schutzniveau für natürliche Personen sollte jedoch bei der Übermittlung personenbezogener Daten aus der Union an Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht untergraben werden, und zwar auch dann nicht, wenn aus einem Drittland oder von einer internationalen Organisation personenbezogene Daten an Verantwortliche oder Auftragsverarbeiter in demselben oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weiterübermittelt werden. In jedem Fall sind derartige Datenübermittlungen an Drittländer und internationale Organisationen nur unter strikter Einhaltung dieser Verordnung zulässig. Eine Datenübermittlung könnte nur stattfinden, wenn die in dieser Verordnung festgelegten Bedingungen zur Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vorbehaltlich der übrigen Bestimmungen dieser Verordnung von dem Verantwortlichen oder dem Auftragsverarbeiter erfüllt werden.
- (102) Internationale Abkommen zwischen der Union und Drittländern über die Übermittlung von personenbezogenen Daten einschließlich geeigneter Garantien für die betroffenen Personen werden von dieser Verordnung nicht berührt. Die Mitgliedstaaten können völkerrechtliche Übereinkünfte schließen, die die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen beinhalten, sofern sich diese Übereinkünfte weder auf diese Verordnung noch auf andere Bestimmungen des Unionsrechts auswirken und ein angemessenes Schutzniveau für die Grundrechte der betroffenen Personen umfassen.
- (103) Die Kommission darf mit Wirkung für die gesamte Union beschließen, dass ein bestimmtes Drittland, ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation ein angemessenes Datenschutzniveau bietet, und auf diese Weise in Bezug auf das Drittland oder die internationale Organisation, das bzw. die für fähig gehalten wird, ein solches Schutzniveau zu bieten, in der gesamten Union Rechtssicherheit schaffen und eine einheitliche Rechtsanwendung sicherstellen. In derartigen Fällen dürfen personenbezogene Daten ohne weitere Genehmigung an dieses Land oder diese internationale Organisation übermittelt werden. Die Kommission kann, nach Abgabe einer ausführlichen Erklärung, in der dem Drittland oder der internationalen Organisation eine Begründung gegeben wird, auch entscheiden, eine solche Feststellung zu widerrufen.
- (104) In Übereinstimmung mit den Grundwerten der Union, zu denen insbesondere der Schutz der Menschenrechte zählt, sollte die Kommission bei der Bewertung des Drittlands oder eines Gebiets oder eines bestimmten Sektors eines Drittlands berücksichtigen, inwieweit dort die Rechtsstaatlichkeit gewahrt ist, der Rechtsweg gewährleistet ist und die internationalen Menschenrechtsnormen und -standards eingehalten werden und welche allgemeinen und sektorspezifischen Vorschriften, wozu auch die Vorschriften über die öffentliche Sicherheit, die Landesverteidigung und die nationale Sicherheit sowie die öffentliche Ordnung und das Strafrecht zählen, dort gelten. Die Annahme eines Angemessenheitsbeschlusses in Bezug auf ein Gebiet oder einen bestimmten Sektor eines Drittlands sollte unter Berücksichtigung eindeutiger und objektiver Kriterien wie bestimmter Verarbeitungsvorgänge und des Anwendungsbereichs anwendbarer Rechtsnormen und geltender Rechtsvorschriften in dem Drittland erfolgen. Das Drittland sollte Garantien für ein angemessenes Schutzniveau bieten, das dem innerhalb

der Union gewährleisteten Schutzniveau der Sache nach gleichwertig ist, insbesondere in Fällen, in denen personenbezogene Daten in einem oder mehreren spezifischen Sektoren verarbeitet werden. Das Drittland sollte insbesondere eine wirksame unabhängige Überwachung des Datenschutzes gewährleisten und Mechanismen für eine Zusammenarbeit mit den Datenschutzbehörden der Mitgliedstaaten vorsehen, und den betroffenen Personen sollten wirksame und durchsetzbare Rechte sowie wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe eingeräumt werden.

- (105) Die Kommission sollte neben den internationalen Verpflichtungen, die das Drittland oder die internationale Organisation eingegangen ist, die Verpflichtungen, die sich aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere im Hinblick auf den Schutz personenbezogener Daten ergeben, sowie die Umsetzung dieser Verpflichtungen berücksichtigen. Insbesondere sollte der Beitritt des Drittlands zum Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dem dazugehörigen Zusatzprotokoll berücksichtigt werden. Die Kommission sollte den Ausschuss konsultieren, wenn sie das Schutzniveau in Drittländern oder internationalen Organisationen bewertet.
- (106) Die Kommission sollte die Wirkungsweise von Feststellungen zum Schutzniveau in einem Drittland, einem Gebiet oder einem bestimmten Sektor eines Drittlands oder einer internationalen Organisation überwachen; sie sollte auch die Wirkungsweise der Feststellungen, die auf der Grundlage des Artikels 25 Absatz 6 oder des Artikels 26 Absatz 4 der Richtlinie 95/46/EG erlassen werden, überwachen. In ihren Angemessenheitsbeschlüssen sollte die Kommission einen Mechanismus für die regelmäßige Überprüfung von deren Wirkungsweise vorsehen. Diese regelmäßige Überprüfung sollte in Konsultation mit dem betreffenden Drittland oder der betreffenden internationalen Organisation erfolgen und allen maßgeblichen Entwicklungen in dem Drittland oder der internationalen Organisation Rechnung tragen. Für die Zwecke der Überwachung und der Durchführung der regelmäßigen Überprüfungen sollte die Kommission die Standpunkte und Feststellungen des Europäischen Parlaments und des Rates sowie der anderen einschlägigen Stellen und Quellen berücksichtigen. Die Kommission sollte innerhalb einer angemessenen Frist die Wirkungsweise der letztgenannten Beschlüsse bewerten und dem durch diese Verordnung eingesetzten Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates⁽¹⁾ sowie dem Europäischen Parlament und dem Rat über alle maßgeblichen Feststellungen Bericht erstatten.
- (107) Die Kommission kann feststellen, dass ein Drittland, ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation kein angemessenes Datenschutzniveau mehr bietet. Die Übermittlung personenbezogener Daten an dieses Drittland oder an diese internationale Organisation sollte daraufhin verboten werden, es sei denn, die Anforderungen dieser Verordnung in Bezug auf die Datenübermittlung vorbehaltlich geeigneter Garantien, einschließlich verbindlicher interner Datenschutzvorschriften und auf Ausnahmen für bestimmte Fälle werden erfüllt. In diesem Falle sollten Konsultationen zwischen der Kommission und den betreffenden Drittländern oder internationalen Organisationen vorgesehen werden. Die Kommission sollte dem Drittland oder der internationalen Organisation frühzeitig die Gründe mitteilen und Konsultationen aufnehmen, um Abhilfe für die Situation zu schaffen.
- (108) Bei Fehlen eines Angemessenheitsbeschlusses sollte der Verantwortliche oder der Auftragsverarbeiter als Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorsehen. Diese geeigneten Garantien können darin bestehen, dass auf verbindliche interne Datenschutzvorschriften, von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln oder von einer Aufsichtsbehörde genehmigte Vertragsklauseln zurückgegriffen wird. Diese Garantien sollten sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden; dies gilt auch hinsichtlich der Verfügbarkeit von durchsetzbaren Rechten der betroffenen Person und von wirksamen Rechtsbehelfen einschließlich des Rechts auf wirksame verwaltungsrechtliche oder gerichtliche Rechtsbehelfe sowie des Rechts auf Geltendmachung von Schadenersatzansprüchen in der Union oder in einem Drittland. Sie sollten sich insbesondere auf die Einhaltung der allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten, die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen beziehen. Datenübermittlungen dürfen auch von Behörden oder öffentlichen Stellen an Behörden oder öffentliche Stellen in Drittländern oder an internationale Organisationen mit entsprechenden Pflichten oder Aufgaben vorgenommen werden, auch auf der Grundlage von Bestimmungen, die in Verwaltungsvereinbarungen — wie beispielsweise einer gemeinsamen Absichtserklärung —, mit denen den betroffenen Personen durchsetzbare und wirksame Rechte eingeräumt werden, aufzunehmen sind. Die Genehmigung der zuständigen Aufsichtsbehörde sollte erlangt werden, wenn die Garantien in nicht rechtsverbindlichen Verwaltungsvereinbarungen vorgesehen sind.
- (109) Die dem Verantwortlichen oder dem Auftragsverarbeiter offenstehende Möglichkeit, auf die von der Kommission oder einer Aufsichtsbehörde festgelegten Standard-Datenschutzklauseln zurückzugreifen, sollte den

⁽¹⁾ Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

Verantwortlichen oder den Auftragsverarbeiter weder daran hindern, die Standard-Datenschutzklauseln auch in umfangreicheren Verträgen, wie zum Beispiel Verträgen zwischen dem Auftragsverarbeiter und einem anderen Auftragsverarbeiter, zu verwenden, noch ihn daran hindern, ihnen weitere Klauseln oder zusätzliche Garantien hinzuzufügen, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln stehen oder die Grundrechte und Grundfreiheiten der betroffenen Personen beschneiden. Die Verantwortlichen und die Auftragsverarbeiter sollten ermutigt werden, mit vertraglichen Verpflichtungen, die die Standard-Schutzklauseln ergänzen, zusätzliche Garantien zu bieten.

- (110) Jede Unternehmensgruppe oder jede Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, sollte für ihre internationalen Datenübermittlungen aus der Union an Organisationen derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, genehmigte verbindliche interne Datenschutzvorschriften anwenden dürfen, sofern diese sämtliche Grundprinzipien und durchsetzbaren Rechte enthalten, die geeignete Garantien für die Übermittlungen beziehungsweise Kategorien von Übermittlungen personenbezogener Daten bieten.
- (111) Datenübermittlungen sollten unter bestimmten Voraussetzungen zulässig sein, nämlich wenn die betroffene Person ihre ausdrückliche Einwilligung erteilt hat, wenn die Übermittlung gelegentlich erfolgt und im Rahmen eines Vertrags oder zur Geltendmachung von Rechtsansprüchen, sei es vor Gericht oder auf dem Verwaltungswege oder in außergerichtlichen Verfahren, wozu auch Verfahren vor Regulierungsbehörden zählen, erforderlich ist. Die Übermittlung sollte zudem möglich sein, wenn sie zur Wahrung eines im Unionsrecht oder im Recht eines Mitgliedstaats festgelegten wichtigen öffentlichen Interesses erforderlich ist oder wenn sie aus einem durch Rechtsvorschriften vorgesehenen Register erfolgt, das von der Öffentlichkeit oder Personen mit berechtigtem Interesse eingesehen werden kann. In letzterem Fall sollte sich eine solche Übermittlung nicht auf die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten erstrecken dürfen. Ist das betreffende Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, sollte die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind, wobei den Interessen und Grundrechten der betroffenen Person in vollem Umfang Rechnung zu tragen ist.
- (112) Diese Ausnahmen sollten insbesondere für Datenübermittlungen gelten, die aus wichtigen Gründen des öffentlichen Interesses erforderlich sind, beispielsweise für den internationalen Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten, beispielsweise im Falle der Umgebungsuntersuchung bei ansteckenden Krankheiten oder zur Verringerung und/oder Beseitigung des Dopings im Sport. Die Übermittlung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein Interesse, das für die lebenswichtigen Interessen — einschließlich der körperlichen Unversehrtheit oder des Lebens — der betroffenen Person oder einer anderen Person wesentlich ist, zu schützen und die betroffene Person außerstande ist, ihre Einwilligung zu geben. Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im Recht der Mitgliedstaaten aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten sollten solche Bestimmungen der Kommission mitteilen. Jede Übermittlung personenbezogener Daten einer betroffenen Person, die aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu erteilen, an eine internationale humanitäre Organisation, die erfolgt, um eine nach den Genfer Konventionen obliegende Aufgabe auszuführen oder um dem in bewaffneten Konflikten anwendbaren humanitären Völkerrecht nachzukommen, könnte als aus einem wichtigen Grund im öffentlichen Interesse notwendig oder als im lebenswichtigen Interesse der betroffenen Person liegend erachtet werden.
- (113) Übermittlungen, die als nicht wiederholt erfolgend gelten können und nur eine begrenzte Zahl von betroffenen Personen betreffen, könnten auch zur Wahrung der zwingenden berechtigten Interessen des Verantwortlichen möglich sein, sofern die Interessen oder Rechte und Freiheiten der betroffenen Person nicht überwiegen und der Verantwortliche sämtliche Umstände der Datenübermittlung geprüft hat. Der Verantwortliche sollte insbesondere die Art der personenbezogenen Daten, den Zweck und die Dauer der vorgesehenen Verarbeitung, die Situation im Herkunftsland, in dem betreffenden Drittland und im Endbestimmungsland berücksichtigen und angemessene Garantien zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten vorsehen. Diese Übermittlungen sollten nur in den verbleibenden Fällen möglich sein, in denen keiner der anderen Gründe für die Übermittlung anwendbar ist. Bei wissenschaftlichen oder historischen Forschungszwecken oder bei statistischen Zwecken sollten die legitimen gesellschaftlichen Erwartungen in Bezug auf einen Wissenszuwachs berücksichtigt werden. Der Verantwortliche sollte die Aufsichtsbehörde und die betroffene Person von der Übermittlung in Kenntnis setzen.
- (114) In allen Fällen, in denen kein Kommissionsbeschluss zur Angemessenheit des in einem Drittland bestehenden Datenschutzniveaus vorliegt, sollte der Verantwortliche oder der Auftragsverarbeiter auf Lösungen zurückgreifen, mit denen den betroffenen Personen durchsetzbare und wirksame Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten in der Union nach der Übermittlung dieser Daten eingeräumt werden, damit sie weiterhin die Grundrechte und Garantien genießen können.

- (115) Manche Drittländer erlassen Gesetze, Vorschriften und sonstige Rechtsakte, die vorgeben, die Verarbeitungstätigkeiten natürlicher und juristischer Personen, die der Rechtsprechung der Mitgliedstaaten unterliegen, unmittelbar zu regeln. Dies kann Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden in Drittländern umfassen, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird und die nicht auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind. Die Anwendung dieser Gesetze, Verordnungen und sonstigen Rechtsakte außerhalb des Hoheitsgebiets der betreffenden Drittländer kann gegen internationales Recht verstoßen und dem durch diese Verordnung in der Union gewährleisteten Schutz natürlicher Personen zuwiderlaufen. Datenübermittlungen sollten daher nur zulässig sein, wenn die Bedingungen dieser Verordnung für Datenübermittlungen an Drittländer eingehalten werden. Dies kann unter anderem der Fall sein, wenn die Offenlegung aus einem wichtigen öffentlichen Interesse erforderlich ist, das im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt ist.
- (116) Wenn personenbezogene Daten in ein anderes Land außerhalb der Union übermittelt werden, besteht eine erhöhte Gefahr, dass natürliche Personen ihre Datenschutzrechte nicht wahrnehmen können und sich insbesondere gegen die unrechtmäßige Nutzung oder Offenlegung dieser Informationen zu schützen. Ebenso kann es vorkommen, dass Aufsichtsbehörden Beschwerden nicht nachgehen oder Untersuchungen nicht durchführen können, die einen Bezug zu Tätigkeiten außerhalb der Grenzen ihres Mitgliedstaats haben. Ihre Bemühungen um grenzüberschreitende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse, widersprüchliche Rechtsordnungen und praktische Hindernisse wie Ressourcenknappheit behindert werden. Die Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden muss daher gefördert werden, damit sie Informationen austauschen und mit den Aufsichtsbehörden in anderen Ländern Untersuchungen durchführen können. Um Mechanismen der internationalen Zusammenarbeit zu entwickeln, die die internationale Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtern und sicherstellen, sollten die Kommission und die Aufsichtsbehörden Informationen austauschen und bei Tätigkeiten, die mit der Ausübung ihrer Befugnisse in Zusammenhang stehen, mit den zuständigen Behörden der Drittländer nach dem Grundsatz der Gegenseitigkeit und gemäß dieser Verordnung zusammenarbeiten.
- (117) Die Errichtung von Aufsichtsbehörden in den Mitgliedstaaten, die befugt sind, ihre Aufgaben und Befugnisse völlig unabhängig wahrzunehmen, ist ein wesentlicher Bestandteil des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die Mitgliedstaaten sollten mehr als eine Aufsichtsbehörde errichten können, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht.
- (118) Die Tatsache, dass die Aufsichtsbehörden unabhängig sind, sollte nicht bedeuten, dass sie hinsichtlich ihrer Ausgaben keinem Kontroll- oder Überwachungsmechanismus unterworfen werden bzw. sie keiner gerichtlichen Überprüfung unterzogen werden können.
- (119) Errichtet ein Mitgliedstaat mehrere Aufsichtsbehörden, so sollte er mittels Rechtsvorschriften sicherstellen, dass diese Aufsichtsbehörden am Kohärenzverfahren wirksam beteiligt werden. Insbesondere sollte dieser Mitgliedstaat eine Aufsichtsbehörde bestimmen, die als zentrale Anlaufstelle für eine wirksame Beteiligung dieser Behörden an dem Verfahren fungiert und eine rasche und reibungslose Zusammenarbeit mit anderen Aufsichtsbehörden, dem Ausschuss und der Kommission gewährleistet.
- (120) Jede Aufsichtsbehörde sollte mit Finanzmitteln, Personal, Räumlichkeiten und einer Infrastruktur ausgestattet werden, wie sie für die wirksame Wahrnehmung ihrer Aufgaben, einschließlich derer im Zusammenhang mit der Amtshilfe und Zusammenarbeit mit anderen Aufsichtsbehörden in der gesamten Union, notwendig sind. Jede Aufsichtsbehörde sollte über einen eigenen, öffentlichen, jährlichen Haushaltsplan verfügen, der Teil des gesamten Staatshaushalts oder nationalen Haushalts sein kann.
- (121) Die allgemeinen Anforderungen an das Mitglied oder die Mitglieder der Aufsichtsbehörde sollten durch Rechtsvorschriften von jedem Mitgliedstaat geregelt werden und insbesondere vorsehen, dass diese Mitglieder im Wege eines transparenten Verfahrens entweder — auf Vorschlag der Regierung, eines Mitglieds der Regierung, des Parlaments oder einer Parlamentskammer — vom Parlament, der Regierung oder dem Staatsoberhaupt des Mitgliedstaats oder von einer unabhängigen Stelle ernannt werden, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird. Um die Unabhängigkeit der Aufsichtsbehörde zu gewährleisten, sollten ihre Mitglieder ihr Amt integer ausüben, von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen absehen und während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit ausüben. Die Aufsichtsbehörde sollte über eigenes Personal verfügen, das sie selbst oder eine nach dem Recht des Mitgliedstaats eingerichtete unabhängige Stelle auswählt und das ausschließlich der Leitung des Mitglieds oder der Mitglieder der Aufsichtsbehörde unterstehen sollte.
- (122) Jede Aufsichtsbehörde sollte dafür zuständig sein, im Hoheitsgebiet ihres Mitgliedstaats die Befugnisse auszuüben und die Aufgaben zu erfüllen, die ihr mit dieser Verordnung übertragen wurden. Dies sollte insbesondere für

Folgendes gelten: die Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung des Verantwortlichen oder Auftragsverarbeiters im Hoheitsgebiet ihres Mitgliedstaats, die Verarbeitung personenbezogener Daten durch Behörden oder private Stellen, die im öffentlichen Interesse handeln, Verarbeitungstätigkeiten, die Auswirkungen auf betroffene Personen in ihrem Hoheitsgebiet haben, oder Verarbeitungstätigkeiten eines Verantwortlichen oder Auftragsverarbeiters ohne Niederlassung in der Union, sofern sie auf betroffene Personen mit Wohnsitz in ihrem Hoheitsgebiet ausgerichtet sind. Dies sollte auch die Bearbeitung von Beschwerden einer betroffenen Person, die Durchführung von Untersuchungen über die Anwendung dieser Verordnung sowie die Förderung der Information der Öffentlichkeit über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten einschließen.

- (123) Die Aufsichtsbehörden sollten die Anwendung der Bestimmungen dieser Verordnung überwachen und zu ihrer einheitlichen Anwendung in der gesamten Union beitragen, um natürliche Personen im Hinblick auf die Verarbeitung ihrer Daten zu schützen und den freien Verkehr personenbezogener Daten im Binnenmarkt zu erleichtern. Zu diesem Zweck sollten die Aufsichtsbehörden untereinander und mit der Kommission zusammenarbeiten, ohne dass eine Vereinbarung zwischen den Mitgliedstaaten über die Leistung von Amtshilfe oder über eine derartige Zusammenarbeit erforderlich wäre.
- (124) Findet die Verarbeitung personenbezogener Daten im Zusammenhang mit der Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union statt und hat der Verantwortliche oder der Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat oder hat die Verarbeitungstätigkeit im Zusammenhang mit der Tätigkeit einer einzigen Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat bzw. wird sie voraussichtlich solche Auswirkungen haben, so sollte die Aufsichtsbehörde für die Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters oder für die einzige Niederlassung des Verantwortlichen oder Auftragsverarbeiters als federführende Behörde fungieren. Sie sollte mit den anderen Behörden zusammenarbeiten, die betroffen sind, weil der Verantwortliche oder Auftragsverarbeiter eine Niederlassung im Hoheitsgebiet ihres Mitgliedstaats hat, weil die Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz in ihrem Hoheitsgebiet hat oder weil bei ihnen eine Beschwerde eingelegt wurde. Auch wenn eine betroffene Person ohne Wohnsitz in dem betreffenden Mitgliedstaat eine Beschwerde eingelegt hat, sollte die Aufsichtsbehörde, bei der Beschwerde eingelegt wurde, auch eine betroffene Aufsichtsbehörde sein. Der Ausschuss sollte — im Rahmen seiner Aufgaben in Bezug auf die Herausgabe von Leitlinien zu allen Fragen im Zusammenhang mit der Anwendung dieser Verordnung — insbesondere Leitlinien zu den Kriterien ausgeben können, die bei der Feststellung zu berücksichtigen sind, ob die fragliche Verarbeitung erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat und was einen maßgeblichen und begründeten Einspruch darstellt.
- (125) Die federführende Behörde sollte berechtigt sein, verbindliche Beschlüsse über Maßnahmen zu erlassen, mit denen die ihr gemäß dieser Verordnung übertragenen Befugnisse ausgeübt werden. In ihrer Eigenschaft als federführende Behörde sollte diese Aufsichtsbehörde für die enge Einbindung und Koordinierung der betroffenen Aufsichtsbehörden im Entscheidungsprozess sorgen. Wird beschlossen, die Beschwerde der betroffenen Person vollständig oder teilweise abzuweisen, so sollte dieser Beschluss von der Aufsichtsbehörde angenommen werden, bei der die Beschwerde eingelegt wurde.
- (126) Der Beschluss sollte von der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden gemeinsam vereinbart werden und an die Hauptniederlassung oder die einzige Niederlassung des Verantwortlichen oder Auftragsverarbeiters gerichtet sein und für den Verantwortlichen und den Auftragsverarbeiter verbindlich sein. Der Verantwortliche oder Auftragsverarbeiter sollte die erforderlichen Maßnahmen treffen, um die Einhaltung dieser Verordnung und die Umsetzung des Beschlusses zu gewährleisten, der der Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters im Hinblick auf die Verarbeitungstätigkeiten in der Union von der federführenden Aufsichtsbehörde mitgeteilt wurde.
- (127) Jede Aufsichtsbehörde, die nicht als federführende Aufsichtsbehörde fungiert, sollte in örtlichen Fällen zuständig sein, wenn der Verantwortliche oder Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat hat, der Gegenstand der spezifischen Verarbeitung aber nur die Verarbeitungstätigkeiten in einem einzigen Mitgliedstaat und nur betroffene Personen in diesem einen Mitgliedstaat betrifft, beispielsweise wenn es um die Verarbeitung von personenbezogenen Daten von Arbeitnehmern im spezifischen Beschäftigungskontext eines Mitgliedstaats geht. In solchen Fällen sollte die Aufsichtsbehörde unverzüglich die federführende Aufsichtsbehörde über diese Angelegenheit unterrichten. Nach ihrer Unterrichtung sollte die federführende Aufsichtsbehörde entscheiden, ob sie den Fall nach den Bestimmungen zur Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden gemäß der Vorschrift zur Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden (im Folgenden „Verfahren der Zusammenarbeit und Kohärenz“) regelt oder ob die Aufsichtsbehörde, die sie unterrichtet hat, den Fall auf örtlicher Ebene regeln sollte. Dabei sollte die federführende Aufsichtsbehörde berücksichtigen, ob der Verantwortliche oder der Auftragsverarbeiter in dem Mitgliedstaat, dessen Aufsichtsbehörde sie unterrichtet hat, eine Niederlassung hat, damit Beschlüsse gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter wirksam durchgesetzt werden. Entscheidet die federführende Aufsichtsbehörde, den Fall selbst zu regeln, sollte die Aufsichtsbehörde, die sie

unterrichtet hat, die Möglichkeit haben, einen Beschlussentwurf vorzulegen, dem die federführende Aufsichtsbehörde bei der Ausarbeitung ihres Beschlussentwurfs im Rahmen dieses Verfahrens der Zusammenarbeit und Kohärenz weitestgehend Rechnung tragen sollte.

- (128) Die Vorschriften über die federführende Behörde und das Verfahren der Zusammenarbeit und Kohärenz sollten keine Anwendung finden, wenn die Verarbeitung durch Behörden oder private Stellen im öffentlichen Interesse erfolgt. In diesen Fällen sollte die Aufsichtsbehörde des Mitgliedstaats, in dem die Behörde oder private Einrichtung ihren Sitz hat, die einzige Aufsichtsbehörde sein, die dafür zuständig ist, die Befugnisse auszuüben, die ihr mit dieser Verordnung übertragen wurden.
- (129) Um die einheitliche Überwachung und Durchsetzung dieser Verordnung in der gesamten Union sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und wirksamen Befugnisse haben, darunter, insbesondere im Fall von Beschwerden natürlicher Personen, Untersuchungsbefugnisse, Abhilfebefugnisse und Sanktionsbefugnisse und Genehmigungsbefugnisse und beratende Befugnisse, sowie — unbeschadet der Befugnisse der Strafverfolgungsbehörden nach dem Recht der Mitgliedstaaten — die Befugnis, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und Gerichtsverfahren anzustrengen. Dazu sollte auch die Befugnis zählen, eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen. Die Mitgliedstaaten können andere Aufgaben im Zusammenhang mit dem Schutz personenbezogener Daten im Rahmen dieser Verordnung festlegen. Die Befugnisse der Aufsichtsbehörden sollten in Übereinstimmung mit den geeigneten Verfahrensgarantien nach dem Unionsrecht und dem Recht der Mitgliedstaaten unparteiisch, gerecht und innerhalb einer angemessenen Frist ausgeübt werden. Insbesondere sollte jede Maßnahme im Hinblick auf die Gewährleistung der Einhaltung dieser Verordnung geeignet, erforderlich und verhältnismäßig sein, wobei die Umstände des jeweiligen Einzelfalls zu berücksichtigen sind, das Recht einer jeden Person, gehört zu werden, bevor eine individuelle Maßnahme getroffen wird, die nachteilige Auswirkungen auf diese Person hätte, zu achten ist und überflüssige Kosten und übermäßige Unannehmlichkeiten für die Betroffenen zu vermeiden sind. Untersuchungsbefugnisse im Hinblick auf den Zugang zu Räumlichkeiten sollten im Einklang mit besonderen Anforderungen im Verfahrensrecht der Mitgliedstaaten ausgeübt werden, wie etwa dem Erfordernis einer vorherigen richterlichen Genehmigung. Jede rechtsverbindliche Maßnahme der Aufsichtsbehörde sollte schriftlich erlassen werden und sie sollte klar und eindeutig sein; die Aufsichtsbehörde, die die Maßnahme erlassen hat, und das Datum, an dem die Maßnahme erlassen wurde, sollten angegeben werden und die Maßnahme sollte vom Leiter oder von einem von ihm bevollmächtigten Mitglied der Aufsichtsbehörde unterschrieben sein und eine Begründung für die Maßnahme sowie einen Hinweis auf das Recht auf einen wirksamen Rechtsbehelf enthalten. Dies sollte zusätzliche Anforderungen nach dem Verfahrensrecht der Mitgliedstaaten nicht ausschließen. Der Erlass eines rechtsverbindlichen Beschlusses setzt voraus, dass er in dem Mitgliedstaat der Aufsichtsbehörde, die den Beschluss erlassen hat, gerichtlich überprüft werden kann.
- (130) Ist die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, nicht die federführende Aufsichtsbehörde, so sollte die federführende Aufsichtsbehörde gemäß den Bestimmungen dieser Verordnung über Zusammenarbeit und Kohärenz eng mit der Aufsichtsbehörde zusammenarbeiten, bei der die Beschwerde eingereicht wurde. In solchen Fällen sollte die federführende Aufsichtsbehörde bei Maßnahmen, die rechtliche Wirkungen entfalten sollen, unter anderem bei der Verhängung von Geldbußen, den Standpunkt der Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde und die weiterhin befugt sein sollte, in Abstimmung mit der zuständigen Aufsichtsbehörde Untersuchungen im Hoheitsgebiet ihres eigenen Mitgliedstaats durchzuführen, weitestgehend berücksichtigen.
- (131) Wenn eine andere Aufsichtsbehörde als federführende Aufsichtsbehörde für die Verarbeitungstätigkeiten des Verantwortlichen oder des Auftragsverarbeiters fungieren sollte, der konkrete Gegenstand einer Beschwerde oder der mögliche Verstoß jedoch nur die Verarbeitungstätigkeiten des Verantwortlichen oder des Auftragsverarbeiters in dem Mitgliedstaat betrifft, in dem die Beschwerde eingereicht wurde oder der mögliche Verstoß aufgedeckt wurde, und die Angelegenheit keine erheblichen Auswirkungen auf betroffene Personen in anderen Mitgliedstaaten hat oder haben dürfte, sollte die Aufsichtsbehörde, bei der eine Beschwerde eingereicht wurde oder die Situationen, die mögliche Verstöße gegen diese Verordnung darstellen, aufgedeckt hat bzw. auf andere Weise darüber informiert wurde, versuchen, eine gütliche Einigung mit dem Verantwortlichen zu erzielen; falls sich dies als nicht erfolgreich erweist, sollte sie die gesamte Bandbreite ihrer Befugnisse wahrnehmen. Dies sollte auch Folgendes umfassen: die spezifische Verarbeitung im Hoheitsgebiet des Mitgliedstaats der Aufsichtsbehörde oder im Hinblick auf betroffene Personen im Hoheitsgebiet dieses Mitgliedstaats; die Verarbeitung im Rahmen eines Angebots von Waren oder Dienstleistungen, das speziell auf betroffene Personen im Hoheitsgebiet des Mitgliedstaats der Aufsichtsbehörde ausgerichtet ist; oder eine Verarbeitung, die unter Berücksichtigung der einschlägigen rechtlichen Verpflichtungen nach dem Recht der Mitgliedstaaten bewertet werden muss.
- (132) Auf die Öffentlichkeit ausgerichtete Sensibilisierungsmaßnahmen der Aufsichtsbehörden sollten spezifische Maßnahmen einschließen, die sich an die Verantwortlichen und die Auftragsverarbeiter, einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen, und an natürliche Personen, insbesondere im Bildungsbereich, richten.

- (133) Die Aufsichtsbehörden sollten sich gegenseitig bei der Erfüllung ihrer Aufgaben unterstützen und Amtshilfe leisten, damit eine einheitliche Anwendung und Durchsetzung dieser Verordnung im Binnenmarkt gewährleistet ist. Eine Aufsichtsbehörde, die um Amtshilfe ersucht hat, kann eine einstweilige Maßnahme erlassen, wenn sie nicht binnen eines Monats nach Eingang des Amtshilfeersuchens bei der ersuchten Aufsichtsbehörde eine Antwort von dieser erhalten hat.
- (134) Jede Aufsichtsbehörde sollte gegebenenfalls an gemeinsamen Maßnahmen von anderen Aufsichtsbehörden teilnehmen. Die ersuchte Aufsichtsbehörde sollte auf das Ersuchen binnen einer bestimmten Frist antworten müssen.
- (135) Um die einheitliche Anwendung dieser Verordnung in der gesamten Union sicherzustellen, sollte ein Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung (Kohärenzverfahren) für die Zusammenarbeit zwischen den Aufsichtsbehörden eingeführt werden. Dieses Verfahren sollte insbesondere dann angewendet werden, wenn eine Aufsichtsbehörde beabsichtigt, eine Maßnahme zu erlassen, die rechtliche Wirkungen in Bezug auf Verarbeitungsvorgänge entfalten soll, die für eine bedeutende Zahl betroffener Personen in mehreren Mitgliedstaaten erhebliche Auswirkungen haben. Ferner sollte es zur Anwendung kommen, wenn eine betroffene Aufsichtsbehörde oder die Kommission beantragt, dass die Angelegenheit im Rahmen des Kohärenzverfahrens behandelt wird. Dieses Verfahren sollte andere Maßnahmen, die die Kommission möglicherweise in Ausübung ihrer Befugnisse nach den Verträgen trifft, unberührt lassen.
- (136) Bei Anwendung des Kohärenzverfahrens sollte der Ausschuss, falls von der Mehrheit seiner Mitglieder so entschieden wird oder falls eine andere betroffene Aufsichtsbehörde oder die Kommission darum ersuchen, binnen einer festgelegten Frist eine Stellungnahme abgeben. Dem Ausschuss sollte auch die Befugnis übertragen werden, bei Streitigkeiten zwischen Aufsichtsbehörden rechtsverbindliche Beschlüsse zu erlassen. Zu diesem Zweck sollte er in klar bestimmten Fällen, in denen die Aufsichtsbehörden insbesondere im Rahmen des Verfahrens der Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden widersprüchliche Standpunkte zu dem Sachverhalt, vor allem in der Frage, ob ein Verstoß gegen diese Verordnung vorliegt, vertreten, grundsätzlich mit einer Mehrheit von zwei Dritteln seiner Mitglieder rechtsverbindliche Beschlüsse erlassen.
- (137) Es kann dringender Handlungsbedarf zum Schutz der Rechte und Freiheiten von betroffenen Personen bestehen, insbesondere wenn eine erhebliche Behinderung der Durchsetzung des Rechts einer betroffenen Person droht. Eine Aufsichtsbehörde sollte daher hinreichend begründete einstweilige Maßnahmen in ihrem Hoheitsgebiet mit einer festgelegten Geltungsdauer von höchstens drei Monaten erlassen können.
- (138) Die Anwendung dieses Verfahrens sollte in den Fällen, in denen sie verbindlich vorgeschrieben ist, eine Bedingung für die Rechtmäßigkeit einer Maßnahme einer Aufsichtsbehörde sein, die rechtliche Wirkungen entfalten soll. In anderen Fällen von grenzüberschreitender Relevanz sollte das Verfahren der Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden zur Anwendung gelangen, und die betroffenen Aufsichtsbehörden können auf bilateraler oder multilateraler Ebene Amtshilfe leisten und gemeinsame Maßnahmen durchführen, ohne auf das Kohärenzverfahren zurückzugreifen.
- (139) Zur Förderung der einheitlichen Anwendung dieser Verordnung sollte der Ausschuss als unabhängige Einrichtung der Union eingesetzt werden. Damit der Ausschuss seine Ziele erreichen kann, sollte er Rechtspersönlichkeit besitzen. Der Ausschuss sollte von seinem Vorsitz vertreten werden. Er sollte die mit der Richtlinie 95/46/EG eingesetzte Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten ersetzen. Er sollte aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder deren jeweiligen Vertretern gebildet werden. An den Beratungen des Ausschusses sollte die Kommission ohne Stimmrecht teilnehmen und der Europäische Datenschutzbeauftragte sollte spezifische Stimmrechte haben. Der Ausschuss sollte zur einheitlichen Anwendung der Verordnung in der gesamten Union beitragen, die Kommission insbesondere im Hinblick auf das Schutzniveau in Drittländern oder internationalen Organisationen beraten und die Zusammenarbeit der Aufsichtsbehörden in der Union fördern. Der Ausschuss sollte bei der Erfüllung seiner Aufgaben unabhängig handeln.
- (140) Der Ausschuss sollte von einem Sekretariat unterstützt werden, das von dem Europäischen Datenschutzbeauftragten bereitgestellt wird. Das Personal des Europäischen Datenschutzbeauftragten, das an der Wahrnehmung der dem Ausschuss gemäß dieser Verordnung übertragenen Aufgaben beteiligt ist, sollte diese Aufgaben ausschließlich gemäß den Anweisungen des Vorsitzes des Ausschusses durchführen und diesem Bericht erstatten.
- (141) Jede betroffene Person sollte das Recht haben, bei einer einzigen Aufsichtsbehörde insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts eine Beschwerde einzureichen und gemäß Artikel 47 der Charta einen wirksamen gerichtlichen Rechtsbehelf einzulegen, wenn sie sich in ihren Rechten gemäß dieser Verordnung

verletzt sieht oder wenn die Aufsichtsbehörde auf eine Beschwerde hin nicht tätig wird, eine Beschwerde teilweise oder ganz abweist oder ablehnt oder nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist. Die auf eine Beschwerde folgende Untersuchung sollte vorbehaltlich gerichtlicher Überprüfung so weit gehen, wie dies im Einzelfall angemessen ist. Die Aufsichtsbehörde sollte die betroffene Person innerhalb eines angemessenen Zeitraums über den Fortgang und die Ergebnisse der Beschwerde unterrichten. Sollten weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde erforderlich sein, sollte die betroffene Person über den Zwischenstand informiert werden. Jede Aufsichtsbehörde sollte Maßnahmen zur Erleichterung der Einreichung von Beschwerden treffen, wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

- (142) Betroffene Personen, die sich in ihren Rechten gemäß dieser Verordnung verletzt sehen, sollten das Recht haben, nach dem Recht eines Mitgliedstaats gegründete Einrichtungen, Organisationen oder Verbände ohne Gewinnerzielungsabsicht, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes personenbezogener Daten tätig sind, zu beauftragen, in ihrem Namen Beschwerde bei einer Aufsichtsbehörde oder einen gerichtlichen Rechtsbehelf einzulegen oder das Recht auf Schadensersatz in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist. Die Mitgliedstaaten können vorsehen, dass diese Einrichtungen, Organisationen oder Verbände das Recht haben, unabhängig vom Auftrag einer betroffenen Person in dem betreffenden Mitgliedstaat eine eigene Beschwerde einzulegen, und das Recht auf einen wirksamen gerichtlichen Rechtsbehelf haben sollten, wenn sie Grund zu der Annahme haben, dass die Rechte der betroffenen Person infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung verletzt worden sind. Diesen Einrichtungen, Organisationen oder Verbänden kann unabhängig vom Auftrag einer betroffenen Person nicht gestattet werden, im Namen einer betroffenen Person Schadensersatz zu verlangen.
- (143) Jede natürliche oder juristische Person hat das Recht, unter den in Artikel 263 AEUV genannten Voraussetzungen beim Gerichtshof eine Klage auf Nichtigkeitserklärung eines Beschlusses des Ausschusses zu erheben. Als Adressaten solcher Beschlüsse müssen die betroffenen Aufsichtsbehörden, die diese Beschlüsse anfechten möchten, binnen zwei Monaten nach deren Übermittlung gemäß Artikel 263 AEUV Klage erheben. Sofern Beschlüsse des Ausschusses einen Verantwortlichen, einen Auftragsverarbeiter oder den Beschwerdeführer unmittelbar und individuell betreffen, so können diese Personen binnen zwei Monaten nach Veröffentlichung der betreffenden Beschlüsse auf der Website des Ausschusses im Einklang mit Artikel 263 AEUV eine Klage auf Nichtigkeitserklärung erheben. Unbeschadet dieses Rechts nach Artikel 263 AEUV sollte jede natürliche oder juristische Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf bei dem zuständigen einzelstaatlichen Gericht gegen einen Beschluss einer Aufsichtsbehörde haben, der gegenüber dieser Person Rechtswirkungen entfaltet. Ein derartiger Beschluss betrifft insbesondere die Ausübung von Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen durch die Aufsichtsbehörde oder die Ablehnung oder Abweisung von Beschwerden. Das Recht auf einen wirksamen gerichtlichen Rechtsbehelf umfasst jedoch nicht rechtlich nicht bindende Maßnahmen der Aufsichtsbehörden wie von ihr abgegebene Stellungnahmen oder Empfehlungen. Verfahren gegen eine Aufsichtsbehörde sollten bei den Gerichten des Mitgliedstaats angestrengt werden, in dem die Aufsichtsbehörde ihren Sitz hat, und sollten im Einklang mit dem Verfahrensrecht dieses Mitgliedstaats durchgeführt werden. Diese Gerichte sollten eine uneingeschränkte Zuständigkeit besitzen, was die Zuständigkeit, sämtliche für den bei ihnen anhängigen Rechtsstreit maßgebliche Sach- und Rechtsfragen zu prüfen, einschließt. Wurde eine Beschwerde von einer Aufsichtsbehörde abgelehnt oder abgewiesen, kann der Beschwerdeführer Klage bei den Gerichten desselben Mitgliedstaats erheben.

Im Zusammenhang mit gerichtlichen Rechtsbehelfen in Bezug auf die Anwendung dieser Verordnung können einzelstaatliche Gerichte, die eine Entscheidung über diese Frage für erforderlich halten, um ihr Urteil erlassen zu können, bzw. müssen einzelstaatliche Gerichte in den Fällen nach Artikel 267 AEUV den Gerichtshof um eine Vorabentscheidung zur Auslegung des Unionsrechts — das auch diese Verordnung einschließt — ersuchen. Wird darüber hinaus der Beschluss einer Aufsichtsbehörde zur Umsetzung eines Beschlusses des Ausschusses vor einem einzelstaatlichen Gericht angefochten und wird die Gültigkeit des Beschlusses des Ausschusses in Frage gestellt, so hat dieses einzelstaatliche Gericht nicht die Befugnis, den Beschluss des Ausschusses für nichtig zu erklären, sondern es muss im Einklang mit Artikel 267 AEUV in der Auslegung des Gerichtshofs den Gerichtshof mit der Frage der Gültigkeit befassen, wenn es den Beschluss für nichtig hält. Allerdings darf ein einzelstaatliches Gericht den Gerichtshof nicht auf Anfrage einer natürlichen oder juristischen Person mit Fragen der Gültigkeit des Beschlusses des Ausschusses befassen, wenn diese Person Gelegenheit hatte, eine Klage auf Nichtigkeitserklärung dieses Beschlusses zu erheben — insbesondere wenn sie unmittelbar und individuell von dem Beschluss betroffen war —, diese Gelegenheit jedoch nicht innerhalb der Frist gemäß Artikel 263 AEUV genutzt hat.

- (144) Hat ein mit einem Verfahren gegen die Entscheidung einer Aufsichtsbehörde befasstes Gericht Anlass zu der Vermutung, dass ein dieselbe Verarbeitung betreffendes Verfahren — etwa zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter oder wegen desselben Anspruchs — vor einem zuständigen Gericht in einem anderen Mitgliedstaat anhängig ist, so sollte es mit diesem Gericht Kontakt aufnehmen, um sich zu vergewissern, dass ein solches verwandtes Verfahren existiert. Sind verwandte Verfahren vor einem Gericht in einem anderen Mitgliedstaat anhängig, so kann jedes später angerufene Gericht das Verfahren aussetzen oder sich auf Anfrage einer Partei auch zugunsten des zuerst angerufenen Gerichts für

unzuständig erklären, wenn dieses später angerufene Gericht für die betreffenden Verfahren zuständig ist und die Verbindung von solchen verwandten Verfahren nach seinem Recht zulässig ist. Verfahren gelten als miteinander verwandt, wenn zwischen ihnen eine so enge Beziehung gegeben ist, dass eine gemeinsame Verhandlung und Entscheidung geboten erscheint, um zu vermeiden, dass in getrennten Verfahren einander widersprechende Entscheidungen ergehen.

- (145) Bei Verfahren gegen Verantwortliche oder Auftragsverarbeiter sollte es dem Kläger überlassen bleiben, ob er die Gerichte des Mitgliedstaats anruft, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat, oder des Mitgliedstaats, in dem die betroffene Person ihren Aufenthaltsort hat; dies gilt nicht, wenn es sich bei dem Verantwortlichen um eine Behörde eines Mitgliedstaats handelt, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.
- (146) Der Verantwortliche oder der Auftragsverarbeiter sollte Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen. Der Verantwortliche oder der Auftragsverarbeiter sollte von seiner Haftung befreit werden, wenn er nachweist, dass er in keiner Weise für den Schaden verantwortlich ist. Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht. Dies gilt unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten. Zu einer Verarbeitung, die mit der vorliegenden Verordnung nicht im Einklang steht, zählt auch eine Verarbeitung, die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten und Durchführungsrechtsakten und Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang steht. Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten. Sind Verantwortliche oder Auftragsverarbeiter an derselben Verarbeitung beteiligt, so sollte jeder Verantwortliche oder Auftragsverarbeiter für den gesamten Schaden haftbar gemacht werden. Werden sie jedoch nach Maßgabe des Rechts der Mitgliedstaaten zu demselben Verfahren hinzugezogen, so können sie im Verhältnis zu der Verantwortung anteilmäßig haftbar gemacht werden, die jeder Verantwortliche oder Auftragsverarbeiter für den durch die Verarbeitung entstandenen Schaden zu tragen hat, sofern sichergestellt ist, dass die betroffene Person einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhält. Jeder Verantwortliche oder Auftragsverarbeiter, der den vollen Schadenersatz geleistet hat, kann anschließend ein Rückgriffsverfahren gegen andere an derselben Verarbeitung beteiligte Verantwortliche oder Auftragsverarbeiter anstrengen.
- (147) Soweit in dieser Verordnung spezifische Vorschriften über die Gerichtsbarkeit — insbesondere in Bezug auf Verfahren im Hinblick auf einen gerichtlichen Rechtsbehelf einschließlich Schadenersatz gegen einen Verantwortlichen oder Auftragsverarbeiter — enthalten sind, sollten die allgemeinen Vorschriften über die Gerichtsbarkeit, wie sie etwa in der Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates ⁽¹⁾ enthalten sind, der Anwendung dieser spezifischen Vorschriften nicht entgegenstehen.
- (148) Im Interesse einer konsequenteren Durchsetzung der Vorschriften dieser Verordnung sollten bei Verstößen gegen diese Verordnung zusätzlich zu den geeigneten Maßnahmen, die die Aufsichtsbehörde gemäß dieser Verordnung verhängt, oder an Stelle solcher Maßnahmen Sanktionen einschließlich Geldbußen verhängt werden. Im Falle eines geringfügigeren Verstoßes oder falls voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, kann anstelle einer Geldbuße eine Verwarnung erteilt werden. Folgendem sollte jedoch gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes, dem vorsätzlichen Charakter des Verstoßes, den Maßnahmen zur Minderung des entstandenen Schadens, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, der Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, der Einhaltung der gegen den Verantwortlichen oder Auftragsverarbeiter angeordneten Maßnahmen, der Einhaltung von Verhaltensregeln und jedem anderen erschwerenden oder mildernden Umstand. Für die Verhängung von Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.
- (149) Die Mitgliedstaaten sollten die strafrechtlichen Sanktionen für Verstöße gegen diese Verordnung, auch für Verstöße gegen auf der Grundlage und in den Grenzen dieser Verordnung erlassene nationale Vorschriften, festlegen können. Diese strafrechtlichen Sanktionen können auch die Einziehung der durch die Verstöße gegen diese Verordnung erzielten Gewinne ermöglichen. Die Verhängung von strafrechtlichen Sanktionen für Verstöße gegen solche nationalen Vorschriften und von verwaltungsrechtlichen Sanktionen sollte jedoch nicht zu einer Verletzung des Grundsatzes „ne bis in idem“, wie er vom Gerichtshof ausgelegt worden ist, führen.
- (150) Um die verwaltungsrechtlichen Sanktionen bei Verstößen gegen diese Verordnung zu vereinheitlichen und ihnen mehr Wirkung zu verleihen, sollte jede Aufsichtsbehörde befugt sein, Geldbußen zu verhängen. In dieser

⁽¹⁾ Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates vom 12. Dezember 2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (ABl. L 351 vom 20.12.2012, S. 1).

Verordnung sollten die Verstöße sowie die Obergrenze der entsprechenden Geldbußen und die Kriterien für ihre Festsetzung genannt werden, wobei diese Geldbußen von der zuständigen Aufsichtsbehörde in jedem Einzelfall unter Berücksichtigung aller besonderen Umstände und insbesondere der Art, Schwere und Dauer des Verstoßes und seiner Folgen sowie der Maßnahmen, die ergriffen worden sind, um die Einhaltung der aus dieser Verordnung erwachsenden Verpflichtungen zu gewährleisten und die Folgen des Verstoßes abzuwenden oder abzumildern, festzusetzen sind. Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102 AEUV verstanden werden. Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der Erwägung des angemessenen Betrags für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen. Das Kohärenzverfahren kann auch genutzt werden, um eine kohärente Anwendung von Geldbußen zu fördern. Die Mitgliedstaaten sollten bestimmen können, ob und inwieweit gegen Behörden Geldbußen verhängt werden können. Auch wenn die Aufsichtsbehörden bereits Geldbußen verhängt oder eine Verwarnung erteilt haben, können sie ihre anderen Befugnisse ausüben oder andere Sanktionen nach Maßgabe dieser Verordnung verhängen.

- (151) Nach den Rechtsordnungen Dänemarks und Estlands sind die in dieser Verordnung vorgesehenen Geldbußen nicht zulässig. Die Vorschriften über die Geldbußen können so angewandt werden, dass die Geldbuße in Dänemark durch die zuständigen nationalen Gerichte als Strafe und in Estland durch die Aufsichtsbehörde im Rahmen eines Verfahrens bei Vergehen verhängt wird, sofern eine solche Anwendung der Vorschriften in diesen Mitgliedstaaten die gleiche Wirkung wie die von den Aufsichtsbehörden verhängten Geldbußen hat. Daher sollten die zuständigen nationalen Gerichte die Empfehlung der Aufsichtsbehörde, die die Geldbuße in die Wege geleitet hat, berücksichtigen. In jeden Fall sollten die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein.
- (152) Soweit diese Verordnung verwaltungsrechtliche Sanktionen nicht harmonisiert oder wenn es in anderen Fällen — beispielsweise bei schweren Verstößen gegen diese Verordnung — erforderlich ist, sollten die Mitgliedstaaten eine Regelung anwenden, die wirksame, verhältnismäßige und abschreckende Sanktionen vorsieht. Es sollte im Recht der Mitgliedstaaten geregelt werden, ob diese Sanktionen strafrechtlicher oder verwaltungsrechtlicher Art sind.
- (153) Im Recht der Mitgliedstaaten sollten die Vorschriften über die freie Meinungsäußerung und Informationsfreiheit, auch von Journalisten, Wissenschaftlern, Künstlern und/oder Schriftstellern, mit dem Recht auf Schutz der personenbezogenen Daten gemäß dieser Verordnung in Einklang gebracht werden. Für die Verarbeitung personenbezogener Daten ausschließlich zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken sollten Abweichungen und Ausnahmen von bestimmten Vorschriften dieser Verordnung gelten, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit dem Recht auf Freiheit der Meinungsäußerung und Informationsfreiheit, wie es in Artikel 11 der Charta garantiert ist, in Einklang zu bringen. Dies sollte insbesondere für die Verarbeitung personenbezogener Daten im audiovisuellen Bereich sowie in Nachrichten- und Pressearchiven gelten. Die Mitgliedstaaten sollten daher Gesetzgebungsmaßnahmen zur Regelung der Abweichungen und Ausnahmen erlassen, die zum Zwecke der Abwägung zwischen diesen Grundrechten notwendig sind. Die Mitgliedstaaten sollten solche Abweichungen und Ausnahmen in Bezug auf die allgemeinen Grundsätze, die Rechte der betroffenen Person, den Verantwortlichen und den Auftragsverarbeiter, die Übermittlung von personenbezogenen Daten an Drittländer oder an internationale Organisationen, die unabhängigen Aufsichtsbehörden, die Zusammenarbeit und Kohärenz und besondere Datenverarbeitungssituationen erlassen. Sollten diese Abweichungen oder Ausnahmen von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein, sollte das Recht des Mitgliedstaats angewendet werden, dem der Verantwortliche unterliegt. Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, müssen Begriffe wie Journalismus, die sich auf diese Freiheit beziehen, weit ausgelegt werden.
- (154) Diese Verordnung ermöglicht es, dass bei ihrer Anwendung der Grundsatz des Zugangs der Öffentlichkeit zu amtlichen Dokumenten berücksichtigt wird. Der Zugang der Öffentlichkeit zu amtlichen Dokumenten kann als öffentliches Interesse betrachtet werden. Personenbezogene Daten in Dokumenten, die sich im Besitz einer Behörde oder einer öffentlichen Stelle befinden, sollten von dieser Behörde oder Stelle öffentlich offengelegt werden können, sofern dies im Unionsrecht oder im Recht der Mitgliedstaaten, denen sie unterliegt, vorgesehen ist. Diese Rechtsvorschriften sollten den Zugang der Öffentlichkeit zu amtlichen Dokumenten und die Weiterverwendung von Informationen des öffentlichen Sektors mit dem Recht auf Schutz personenbezogener Daten in Einklang bringen und können daher die notwendige Übereinstimmung mit dem Recht auf Schutz personenbezogener Daten gemäß dieser Verordnung regeln. Die Bezugnahme auf Behörden und öffentliche Stellen sollte in diesem Kontext sämtliche Behörden oder sonstigen Stellen beinhalten, die vom Recht des jeweiligen Mitgliedstaats über den Zugang der Öffentlichkeit zu Dokumenten erfasst werden. Die Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates⁽¹⁾ lässt das Schutzniveau für natürliche Personen in Bezug auf die Verarbeitung personenbezogener Daten gemäß den Bestimmungen des Unionsrechts und des

(¹) Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 345 vom 31.12.2003, S. 90).

Rechts der Mitgliedstaaten unberührt und beeinträchtigt diesen in keiner Weise, und sie bewirkt insbesondere keine Änderung der in dieser Verordnung dargelegten Rechte und Pflichten. Insbesondere sollte die genannte Richtlinie nicht für Dokumente gelten, die nach den Zugangsregelungen der Mitgliedstaaten aus Gründen des Schutzes personenbezogener Daten nicht oder nur eingeschränkt zugänglich sind, oder für Teile von Dokumenten, die nach diesen Regelungen zugänglich sind, wenn sie personenbezogene Daten enthalten, bei denen Rechtsvorschriften vorsehen, dass ihre Weiterverwendung nicht mit dem Recht über den Schutz natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten vereinbar ist.

- (155) Im Recht der Mitgliedstaaten oder in Kollektivvereinbarungen (einschließlich 'Betriebsvereinbarungen') können spezifische Vorschriften für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorgesehen werden, und zwar insbesondere Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen, über die Verarbeitung dieser Daten für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses.
- (156) Die Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken sollte geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung unterliegen. Mit diesen Garantien sollte sichergestellt werden, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere der Grundsatz der Datenminimierung gewährleistet wird. Die Weiterverarbeitung personenbezogener Daten zu im öffentlichen Interesse liegende Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken erfolgt erst dann, wenn der Verantwortliche geprüft hat, ob es möglich ist, diese Zwecke durch die Verarbeitung von personenbezogenen Daten, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, zu erfüllen, sofern geeignete Garantien bestehen (wie z. B. die Pseudonymisierung von personenbezogenen Daten). Die Mitgliedstaaten sollten geeignete Garantien in Bezug auf die Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken vorsehen. Es sollte den Mitgliedstaaten erlaubt sein, unter bestimmten Bedingungen und vorbehaltlich geeigneter Garantien für die betroffenen Personen Präzisierungen und Ausnahmen in Bezug auf die Informationsanforderungen sowie der Rechte auf Berichtigung, Löschung, Vergessenwerden, zur Einschränkung der Verarbeitung, auf Datenübertragbarkeit sowie auf Widerspruch bei der Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegende Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken vorzusehen. Im Rahmen der betreffenden Bedingungen und Garantien können spezifische Verfahren für die Ausübung dieser Rechte durch die betroffenen Personen vorgesehen sein — sofern dies angesichts der mit der spezifischen Verarbeitung verfolgten Zwecke angemessen ist — sowie technische und organisatorische Maßnahmen zur Minimierung der Verarbeitung personenbezogener Daten im Hinblick auf die Grundsätze der Verhältnismäßigkeit und der Notwendigkeit. Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken sollte auch anderen einschlägigen Rechtsvorschriften, beispielsweise für klinische Prüfungen, genügen.
- (157) Durch die Verknüpfung von Informationen aus Registern können Forscher neue Erkenntnisse von großem Wert in Bezug auf weit verbreiteten Krankheiten wie Herz-Kreislauferkrankungen, Krebs und Depression erhalten. Durch die Verwendung von Registern können bessere Forschungsergebnisse erzielt werden, da sie auf einen größeren Bevölkerungsanteil gestützt sind. Im Bereich der Sozialwissenschaften ermöglicht die Forschung anhand von Registern es den Forschern, entscheidende Erkenntnisse über den langfristigen Zusammenhang einer Reihe sozialer Umstände zu erlangen, wie Arbeitslosigkeit und Bildung mit anderen Lebensumständen. Durch Register erhaltene Forschungsergebnisse bieten solide, hochwertige Erkenntnisse, die die Basis für die Erarbeitung und Umsetzung wissenschaftlich gestützter politischer Maßnahmen darstellen, die Lebensqualität zahlreicher Menschen verbessern und die Effizienz der Sozialdienste verbessern können. Zur Erleichterung der wissenschaftlichen Forschung können daher personenbezogene Daten zu wissenschaftlichen Forschungszwecken verarbeitet werden, wobei sie angemessenen Bedingungen und Garantien unterliegen, die im Unionsrecht oder im Recht der Mitgliedstaaten festgelegt sind.
- (158) Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu Archivzwecken gelten, wobei darauf hinzuweisen ist, dass die Verordnung nicht für verstorbene Personen gelten sollte. Behörden oder öffentliche oder private Stellen, die Aufzeichnungen von öffentlichem Interesse führen, sollten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten rechtlich verpflichtet sein, Aufzeichnungen von bleibendem Wert für das allgemeine öffentliche Interesse zu erwerben, zu erhalten, zu bewerten, aufzubereiten, zu beschreiben, mitzuteilen, zu fördern, zu verbreiten sowie Zugang dazu bereitzustellen. Es sollte den Mitgliedstaaten ferner erlaubt sein vorzusehen, dass personenbezogene Daten zu Archivzwecken weiterverarbeitet werden, beispielsweise im Hinblick auf die Bereitstellung spezifischer Informationen im Zusammenhang mit dem politischen Verhalten unter ehemaligen totalitären Regimen, Völkermord, Verbrechen gegen die Menschlichkeit, insbesondere dem Holocaust, und Kriegsverbrechen.

- (159) Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken gelten. Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken im Sinne dieser Verordnung sollte weit ausgelegt werden und die Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen. Darüber hinaus sollte sie dem in Artikel 179 Absatz 1 AEUV festgeschriebenen Ziel, einen europäischen Raum der Forschung zu schaffen, Rechnung tragen. Die wissenschaftlichen Forschungszwecke sollten auch Studien umfassen, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Um den Besonderheiten der Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken zu genügen, sollten spezifische Bedingungen insbesondere hinsichtlich der Veröffentlichung oder sonstigen Offenlegung personenbezogener Daten im Kontext wissenschaftlicher Zwecke gelten. Geben die Ergebnisse wissenschaftlicher Forschung insbesondere im Gesundheitsbereich Anlass zu weiteren Maßnahmen im Interesse der betroffenen Person, sollten die allgemeinen Vorschriften dieser Verordnung für diese Maßnahmen gelten.
- (160) Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu historischen Forschungszwecken gelten. Dazu sollte auch historische Forschung und Forschung im Bereich der Genealogie zählen, wobei darauf hinzuweisen ist, dass diese Verordnung nicht für verstorbene Personen gelten sollte.
- (161) Für die Zwecke der Einwilligung in die Teilnahme an wissenschaftlichen Forschungstätigkeiten im Rahmen klinischer Prüfungen sollten die einschlägigen Bestimmungen der Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates ⁽¹⁾ gelten.
- (162) Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu statistischen Zwecken gelten. Das Unionsrecht oder das Recht der Mitgliedstaaten sollte in den Grenzen dieser Verordnung den statistischen Inhalt, die Zugangskontrolle, die Spezifikationen für die Verarbeitung personenbezogener Daten zu statistischen Zwecken und geeignete Maßnahmen zur Sicherung der Rechte und Freiheiten der betroffenen Personen und zur Sicherstellung der statistischen Geheimhaltung bestimmen. Unter dem Begriff „statistische Zwecke“ ist jeder für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche Vorgang der Erhebung und Verarbeitung personenbezogener Daten zu verstehen. Diese statistischen Ergebnisse können für verschiedene Zwecke, so auch für wissenschaftliche Forschungszwecke, weiterverwendet werden. Im Zusammenhang mit den statistischen Zwecken wird vorausgesetzt, dass die Ergebnisse der Verarbeitung zu statistischen Zwecken keine personenbezogenen Daten, sondern aggregierte Daten sind und diese Ergebnisse oder personenbezogenen Daten nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden.
- (163) Die vertraulichen Informationen, die die statistischen Behörden der Union und der Mitgliedstaaten zur Erstellung der amtlichen europäischen und der amtlichen nationalen Statistiken erheben, sollten geschützt werden. Die europäischen Statistiken sollten im Einklang mit den in Artikel 338 Absatz 2 AEUV dargelegten statistischen Grundsätzen entwickelt, erstellt und verbreitet werden, wobei die nationalen Statistiken auch mit dem Recht der Mitgliedstaaten übereinstimmen müssen. Die Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates ⁽²⁾ enthält genauere Bestimmungen zur Vertraulichkeit europäischer Statistiken.
- (164) Hinsichtlich der Befugnisse der Aufsichtsbehörden, von dem Verantwortlichen oder vom Auftragsverarbeiter Zugang zu personenbezogenen Daten oder zu seinen Räumlichkeiten zu erlangen, können die Mitgliedstaaten in den Grenzen dieser Verordnung den Schutz des Berufsgeheimnisses oder anderer gleichwertiger Geheimhaltungspflichten durch Rechtsvorschriften regeln, soweit dies notwendig ist, um das Recht auf Schutz der personenbezogenen Daten mit einer Pflicht zur Wahrung des Berufsgeheimnisses in Einklang zu bringen. Dies berührt nicht die bestehenden Verpflichtungen der Mitgliedstaaten zum Erlass von Vorschriften über das Berufsgeheimnis, wenn dies aufgrund des Unionsrechts erforderlich ist.
- (165) Im Einklang mit Artikel 17 AEUV achtet diese Verordnung den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren bestehenden verfassungsrechtlichen Vorschriften genießen, und beeinträchtigt ihn nicht.
- (166) Um die Zielvorgaben dieser Verordnung zu erfüllen, d. h. die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz ihrer personenbezogenen Daten zu schützen und den freien

⁽¹⁾ Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG Text von Bedeutung für den EWR (ABl. L 158 vom 27.5.2014, S. 1).

⁽²⁾ Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates vom 11. März 2009 über europäische Statistiken und zur Aufhebung der Verordnung (EG, Euratom) Nr. 1101/2008 des Europäischen Parlaments und des Rates über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften, der Verordnung (EG) Nr. 322/97 des Rates über die Gemeinschaftsstatistiken und des Beschlusses 89/382/EWG, Euratom des Rates zur Einsetzung eines Ausschusses für das Statistische Programm der Europäischen Gemeinschaften (ABl. L 87 vom 31.3.2009, S. 164).

Verkehr personenbezogener Daten innerhalb der Union zu gewährleisten, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen. Delegierte Rechtsakte sollten insbesondere in Bezug auf die für Zertifizierungsverfahren geltenden Kriterien und Anforderungen, die durch standardisierte Bildsymbole darzustellenden Informationen und die Verfahren für die Bereitstellung dieser Bildsymbole erlassen werden. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt. Bei der Vorbereitung und Ausarbeitung delegierter Rechtsakte sollte die Kommission gewährleisten, dass die einschlägigen Dokumente dem Europäischen Parlament und dem Rat gleichzeitig, rechtzeitig und auf angemessene Weise übermittelt werden.

- (167) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden, wenn dies in dieser Verordnung vorgesehen ist. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ausgeübt werden. In diesem Zusammenhang sollte die Kommission besondere Maßnahmen für Kleinunternehmen sowie kleine und mittlere Unternehmen erwägen.
- (168) Für den Erlass von Durchführungsrechtsakten bezüglich Standardvertragsklauseln für Verträge zwischen Verantwortlichen und Auftragsverarbeitern sowie zwischen Auftragsverarbeitern; Verhaltensregeln; technische Standards und Verfahren für die Zertifizierung; Anforderungen an die Angemessenheit des Datenschutzniveaus in einem Drittland, einem Gebiet oder bestimmten Sektor dieses Drittlands oder in einer internationalen Organisation; Standardschutzklauseln; Formate und Verfahren für den Informationsaustausch zwischen Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden im Hinblick auf verbindliche interne Datenschutzvorschriften; Amtshilfe; sowie Vorkehrungen für den elektronischen Informationsaustausch zwischen Aufsichtsbehörden und zwischen Aufsichtsbehörden und dem Ausschuss sollte das Prüfverfahren angewandt werden.
- (169) Die Kommission sollte sofort geltende Durchführungsrechtsakte erlassen, wenn anhand vorliegender Beweise festgestellt wird, dass ein Drittland, ein Gebiet oder ein bestimmter Sektor in diesem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau gewährleistet, und dies aus Gründen äußerster Dringlichkeit erforderlich ist.
- (170) Da das Ziel dieser Verordnung, nämlich die Gewährleistung eines gleichwertigen Datenschutzniveaus für natürliche Personen und des freien Verkehrs personenbezogener Daten in der Union, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen des Umfangs oder der Wirkungen der Maßnahme auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union (EUV) verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.
- (171) Die Richtlinie 95/46/EG sollte durch diese Verordnung aufgehoben werden. Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden. Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann. Auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.
- (172) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 konsultiert und hat am 7. März 2012 ⁽¹⁾ eine Stellungnahme abgegeben.
- (173) Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ⁽²⁾ bestimmte Pflichten, die dasselbe Ziel verfolgen, unterliegen, einschließlich der Pflichten des Verantwortlichen und der Rechte natürlicher Personen. Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden. Sobald diese Verordnung angenommen ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit dieser Verordnung zu gewährleisten —

⁽¹⁾ ABl. C 192 vom 30.6.2012, S. 7.

⁽²⁾ Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand und Ziele

- (1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
- (2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
- (3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

Artikel 2

Sachlicher Anwendungsbereich

- (1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.
- (2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten
 - a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,
 - b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,
 - c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,
 - d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.
- (3) Für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union gilt die Verordnung (EG) Nr. 45/2001. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, werden im Einklang mit Artikel 98 an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst.
- (4) Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit der Vermittler unberührt.

Artikel 3

Räumlicher Anwendungsbereich

- (1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.

(2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

- a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
- b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

(3) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

Artikel 4

Begriffsbestimmungen

Im Sinne dieser Verordnung 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung 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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;
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 dem Recht der Mitgliedstaaten

möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

10. „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;
11. „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;
12. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;
13. „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;
14. „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;
15. „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;
16. „Hauptniederlassung“
 - a) im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;
 - b) im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;
17. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;
18. „Unternehmen“ eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;
19. „Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;
20. „verbindliche interne Datenschutzvorschriften“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern;
21. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle;

22. „betroffene Aufsichtsbehörde“ eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil
- a) der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,
 - b) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder
 - c) eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;
23. „grenzüberschreitende Verarbeitung“ entweder
- a) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder
 - b) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann;
24. „maßgeblicher und begründeter Einspruch“ einen Einspruch gegen einen Beschlussentwurf im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder ob beabsichtigte Maßnahmen gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen;
25. „Dienst der Informationsgesellschaft“ eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates ⁽¹⁾;
26. „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 II

Grundsätze

Artikel 5

Grundsätze für die Verarbeitung personenbezogener Daten

- (1) Personenbezogene Daten müssen
- a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
 - b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
 - c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
 - d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

⁽¹⁾ Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

- e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
 - f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);
- (2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Artikel 6

Rechtmäßigkeit der Verarbeitung

- (1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
- a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
 - b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
 - c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
 - d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
 - e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
 - f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

- (3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch
- a) Unionsrecht oder
 - b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben

erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche — um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist — unter anderem

- a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
- b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
- c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,
- d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Artikel 7

Bedingungen für die Einwilligung

(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so 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. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

Artikel 8

Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

(1) Gilt Artikel 6 Absatz 1 Buchstabe a bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.

Die Mitgliedstaaten können durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.

(2) Der Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.

(3) Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, unberührt.

Artikel 9

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

- a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,
- b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,
- c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,
- d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,
- e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,
- f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,
- g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das 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, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,
- h) die Verarbeitung ist für Zwecke 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- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,
- i) die Verarbeitung ist 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, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

- j) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das 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, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.
- (3) Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.
- (4) Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

Artikel 10

Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

Artikel 11

Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

- (1) Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.
- (2) Kann der Verantwortliche in Fällen gemäß Absatz 1 des vorliegenden Artikels nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet er die betroffene Person hierüber, sofern möglich. In diesen Fällen finden die Artikel 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

KAPITEL III

Rechte der betroffenen Person

Abschnitt 1

Transparenz und Modalitäten

Artikel 12

Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

- (1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

(2) Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22. In den in Artikel 11 Absatz 2 genannten Fällen darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 22 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

(3) Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(4) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) Informationen gemäß den Artikeln 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 und Artikel 34 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder

- a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder
- b) sich weigern, aufgrund des Antrags tätig zu werden.

Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(6) Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den Artikeln 15 bis 21 stellt, so kann er unbeschadet des Artikels 11 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

(7) Die Informationen, die den betroffenen Personen gemäß den Artikeln 13 und 14 bereitzustellen sind, können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, müssen sie maschinenlesbar sein.

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen.

Abschnitt 2

Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten

Artikel 13

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

- a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
- c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

- d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
 - e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
 - f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.
- (2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:
- a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
 - b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
 - c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
 - d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
 - e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
 - f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.
- (3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.
- (4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

Artikel 14

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

- (1) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:
- a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
 - b) zusätzlich die Kontaktdaten des Datenschutzbeauftragten;
 - c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
 - d) die Kategorien personenbezogener Daten, die verarbeitet werden;
 - e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:

- a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- c) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- e) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- f) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;
- g) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Der Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2

- a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,
- b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,
- c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

(4) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(5) Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit

- a) die betroffene Person bereits über die Informationen verfügt,
- b) die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien oder soweit die in Absatz 1 des vorliegenden Artikels genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit,
- c) die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder
- d) die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

*Artikel 15***Auskunftsrecht der betroffenen Person**

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

- a) die Verarbeitungszwecke;
- b) die Kategorien personenbezogener Daten, die verarbeitet werden;
- c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 1b darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

*Abschnitt 3***Berichtigung und Löschung***Artikel 16***Recht auf Berichtigung**

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

*Artikel 17***Recht auf Löschung („Recht auf Vergessenwerden“)**

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

- a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

- b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.
- d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
- f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist

- a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;
- d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Artikel 18

Recht auf Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

- a) die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,
- b) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;
- c) der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
- d) die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

(2) Wurde die Verarbeitung gemäß Absatz 1 eingeschränkt, so dürfen diese personenbezogenen Daten — von ihrer Speicherung abgesehen — nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.

(3) Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Absatz 1 erwirkt hat, wird von dem Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird.

Artikel 19

Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

Der Verantwortliche teilt allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Artikel 16, Artikel 17 Absatz 1 und Artikel 18 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

Artikel 20

Recht auf Datenübertragbarkeit

(1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

- a) die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und
- b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

(2) Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

(3) Die Ausübung des Rechts nach Absatz 1 des vorliegenden Artikels lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

(4) Das Recht gemäß Absatz 2 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Abschnitt 4

Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall

Artikel 21

Widerspruchsrecht

(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(2) Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

(3) Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

(4) Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das in den Absätzen 1 und 2 genannte Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

(5) Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.

(6) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 89 Absatz 1 erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

Artikel 22

Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(2) Absatz 1 gilt nicht, wenn die Entscheidung

- a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
- b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
- c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

Abschnitt 5

Beschränkungen

Artikel 23

Beschränkungen

(1) Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

- a) die nationale Sicherheit;
- b) die Landesverteidigung;
- c) die öffentliche Sicherheit;

- d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;
- e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;
- f) den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;
- g) die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;
- h) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind;
- i) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;
- j) die Durchsetzung zivilrechtlicher Ansprüche.

(2) Jede Gesetzgebungsmaßnahme im Sinne des Absatzes 1 muss insbesondere gegebenenfalls spezifische Vorschriften enthalten zumindest in Bezug auf

- a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien,
- b) die Kategorien personenbezogener Daten,
- c) den Umfang der vorgenommenen Beschränkungen,
- d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung;
- e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen,
- f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,
- g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und
- h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist.

KAPITEL IV

Verantwortlicher und Auftragsverarbeiter

Abschnitt 1

Allgemeine Pflichten

Artikel 24

Verantwortung des für die Verarbeitung Verantwortlichen

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

(3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

*Artikel 25***Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**

(1) 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 trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(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.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

*Artikel 26***Gemeinsam für die Verarbeitung Verantwortliche**

(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

*Artikel 27***Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern**

(1) In den Fällen gemäß Artikel 3 Absatz 2 benennt der Verantwortliche oder der Auftragsverarbeiter schriftlich einen Vertreter in der Union.

(2) Die Pflicht gemäß Absatz 1 des vorliegenden Artikels gilt nicht für

a) eine Verarbeitung, die gelegentlich erfolgt, nicht die umfangreiche Verarbeitung besonderer Datenkategorien im Sinne des Artikels 9 Absatz 1 oder die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt und unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, oder

b) Behörden oder öffentliche Stellen.

- (3) Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die betroffenen Personen, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird, sich befinden.
- (4) Der Vertreter wird durch den Verantwortlichen oder den Auftragsverarbeiter beauftragt, zusätzlich zu diesem oder an seiner Stelle insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung zur Gewährleistung der Einhaltung dieser Verordnung als Anlaufstelle zu dienen.
- (5) Die Benennung eines Vertreters durch den Verantwortlichen oder den Auftragsverarbeiter erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den Verantwortlichen oder den Auftragsverarbeiter selbst.

Artikel 28

Auftragsverarbeiter

- (1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
- (2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer 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.
- (3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem 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 festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter
- die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
 - gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
 - alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;
 - die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
 - angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;
 - unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;
 - nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
 - dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen — einschließlich Inspektionen —, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) 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 nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung 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) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

Artikel 29

Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Artikel 30

Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

- a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- b) die Zwecke der Verarbeitung;
- c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

- d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
 - e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
 - f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
 - g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.
- (2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:
- a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
 - b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
 - c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
 - d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.
- (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 oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.
- (5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.

Artikel 31

Zusammenarbeit mit der Aufsichtsbehörde

Der Verantwortliche und der Auftragsverarbeiter und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Abschnitt 2

Sicherheit personenbezogener Daten

Artikel 32

Sicherheit der Verarbeitung

- (1) 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 des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:
- a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

- b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
 - c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
 - d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
- (2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.
- (3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
- (4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Artikel 33

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

- (1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.
- (2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.
- (3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:
- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- (4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.
- (5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

Artikel 34

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

- (1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

- a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, 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;
- b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;
- c) 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 die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

Abschnitt 3

Datenschutz-Folgenabschätzung und vorherige Konsultation

Artikel 35

Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

- a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
- b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
- c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

- (7) Die Folgenabschätzung enthält zumindest Folgendes:
- a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
 - b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
 - c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
 - d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.
- (8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.
- (9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.
- (10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.
- (11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Artikel 36

Vorherige Konsultation

- (1) Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.
- (2) Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 1 nicht im Einklang mit dieser Verordnung stünde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, unterbreitet sie dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu acht Wochen nach Erhalt des Ersuchens um Konsultation entsprechende schriftliche Empfehlungen und kann ihre in Artikel 58 genannten Befugnisse ausüben. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um sechs Wochen verlängert werden. Die Aufsichtsbehörde unterrichtet den Verantwortlichen oder gegebenenfalls den Auftragsverarbeiter über eine solche Fristverlängerung innerhalb eines Monats nach Eingang des Antrags auf Konsultation zusammen mit den Gründen für die Verzögerung. Diese Fristen können ausgesetzt werden, bis die Aufsichtsbehörde die für die Zwecke der Konsultation angeforderten Informationen erhalten hat.
- (3) Der Verantwortliche stellt der Aufsichtsbehörde bei einer Konsultation gemäß Absatz 1 folgende Informationen zur Verfügung:
- a) gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;
 - b) die Zwecke und die Mittel der beabsichtigten Verarbeitung;
 - c) die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen Maßnahmen und Garantien;
 - d) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

- e) die Datenschutz-Folgenabschätzung gemäß Artikel 35 und
- f) alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.

(4) Die Mitgliedstaaten konsultieren die Aufsichtsbehörde bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen, die die Verarbeitung betreffen.

(5) Ungeachtet des Absatzes 1 können Verantwortliche durch das Recht der Mitgliedstaaten verpflichtet werden, bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung zu Zwecken der sozialen Sicherheit und der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren und deren vorherige Genehmigung einzuholen.

Abschnitt 4

Datenschutzbeauftragter

Artikel 37

Benennung eines Datenschutzbeauftragten

- (1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn
 - a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,
 - b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
 - c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.
- (2) Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.
- (3) Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.
- (4) In anderen als den in Absatz 1 genannten Fällen können der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen. Der Datenschutzbeauftragte kann für derartige Verbände und andere Vereinigungen, die Verantwortliche oder Auftragsverarbeiter vertreten, handeln.
- (5) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.
- (6) Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.
- (7) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

Artikel 38

Stellung des Datenschutzbeauftragten

- (1) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Der Verantwortliche und der Auftragsverarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen.

(3) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters.

(4) Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.

(5) Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.

(6) Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Artikel 39

Aufgaben des Datenschutzbeauftragten

(1) Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

- a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;
- b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- c) Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;
- 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, und gegebenenfalls Beratung zu allen sonstigen Fragen.

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

Abschnitt 5

Verhaltensregeln und Zertifizierung

Artikel 40

Verhaltensregeln

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen.

(2) Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, können Verhaltensregeln ausarbeiten oder ändern oder erweitern, mit denen die Anwendung dieser Verordnung beispielsweise zu dem Folgenden präzisiert wird:

- a) faire und transparente Verarbeitung;

- b) die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen;
- c) Erhebung personenbezogener Daten;
- d) Pseudonymisierung personenbezogener Daten;
- e) Unterrichtung der Öffentlichkeit und der betroffenen Personen;
- f) Ausübung der Rechte betroffener Personen;
- g) Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist;
- h) die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 32;
- i) die Meldung von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden und die Benachrichtigung der betroffenen Person von solchen Verletzungen des Schutzes personenbezogener Daten;
- j) die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen oder
- k) außergerichtliche Verfahren und sonstige Streitbelegungsverfahren zur Beilegung von Streitigkeiten zwischen Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung, unbeschadet der Rechte betroffener Personen gemäß den Artikeln 77 und 79.

(3) Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden Verantwortlichen oder Auftragsverarbeiter können Verhaltensregeln, die gemäß Absatz 5 des vorliegenden Artikels genehmigt wurden und gemäß Absatz 9 des vorliegenden Artikels allgemeine Gültigkeit besitzen, können auch von Verantwortlichen oder Auftragsverarbeitern, die gemäß Artikel 3 nicht unter diese Verordnung fallen, eingehalten werden, um geeignete Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe des Artikels 46 Absatz 2 Buchstabe e zu bieten. Diese Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung ein, die geeigneten Garantien anzuwenden, auch im Hinblick auf die Rechte der betroffenen Personen.

(4) Die Verhaltensregeln gemäß Absatz 2 des vorliegenden Artikels müssen Verfahren vorsehen, die es der in Artikel 41 Absatz 1 genannten Stelle ermöglichen, die obligatorische Überwachung der Einhaltung ihrer Bestimmungen durch die Verantwortlichen oder die Auftragsverarbeiter, die sich zur Anwendung der Verhaltensregeln verpflichten, vorzunehmen, unbeschadet der Aufgaben und Befugnisse der Aufsichtsbehörde, die nach Artikel 55 oder 56 zuständig ist.

(5) Verbände und andere Vereinigungen gemäß Absatz 2 des vorliegenden Artikels, die beabsichtigen, Verhaltensregeln auszuarbeiten oder bestehende Verhaltensregeln zu ändern oder zu erweitern, legen den Entwurf der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung der Aufsichtsbehörde vor, die nach Artikel 55 zuständig ist. Die Aufsichtsbehörde gibt eine Stellungnahme darüber ab, ob der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung mit dieser Verordnung vereinbar ist und genehmigt diesen Entwurf der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung, wenn sie der Auffassung ist, dass er ausreichende geeignete Garantien bietet.

(6) Wird durch die Stellungnahme nach Absatz 5 der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung genehmigt und beziehen sich die betreffenden Verhaltensregeln nicht auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so nimmt die Aufsichtsbehörde die Verhaltensregeln in ein Verzeichnis auf und veröffentlicht sie.

(7) Bezieht sich der Entwurf der Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so legt die nach Artikel 55 zuständige Aufsichtsbehörde — bevor sie den Entwurf der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung genehmigt — ihn nach dem Verfahren gemäß Artikel 63 dem Ausschuss vor, der zu der Frage Stellung nimmt, ob der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung mit dieser Verordnung vereinbar ist oder — im Fall nach Absatz 3 dieses Artikels — geeignete Garantien vorsieht.

(8) Wird durch die Stellungnahme nach Absatz 7 bestätigt, dass der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung mit dieser Verordnung vereinbar ist oder — im Fall nach Absatz 3 — geeignete Garantien vorsieht, so übermittelt der Ausschuss seine Stellungnahme der Kommission.

(9) Die Kommission kann im Wege von Durchführungsrechtsakten beschließen, dass die ihr gemäß Absatz 8 übermittelten genehmigten Verhaltensregeln bzw. deren genehmigte Änderung oder Erweiterung allgemeine Gültigkeit in der Union besitzen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.

(10) Die Kommission trägt dafür Sorge, dass die genehmigten Verhaltensregeln, denen gemäß Absatz 9 allgemeine Gültigkeit zuerkannt wurde, in geeigneter Weise veröffentlicht werden.

(11) Der Ausschuss nimmt alle genehmigten Verhaltensregeln bzw. deren genehmigte Änderungen oder Erweiterungen in ein Register auf und veröffentlicht sie in geeigneter Weise.

Artikel 41

Überwachung der genehmigten Verhaltensregeln

(1) Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 57 und 58 kann die Überwachung der Einhaltung von Verhaltensregeln gemäß Artikel 40 von einer Stelle durchgeführt werden, die über das geeignete Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln verfügt und die von der zuständigen Aufsichtsbehörde zu diesem Zweck akkreditiert wurde.

(2) Eine Stelle gemäß Absatz 1 kann zum Zwecke der Überwachung der Einhaltung von Verhaltensregeln akkreditiert werden, wenn sie

- a) ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat;
- b) Verfahren festgelegt hat, die es ihr ermöglichen, zu bewerten, ob Verantwortliche und Auftragsverarbeiter die Verhaltensregeln anwenden können, die Einhaltung der Verhaltensregeln durch die Verantwortlichen und Auftragsverarbeiter zu überwachen und die Anwendung der Verhaltensregeln regelmäßig zu überprüfen;
- c) Verfahren und Strukturen festgelegt hat, mit denen sie Beschwerden über Verletzungen der Verhaltensregeln oder über die Art und Weise, in der die Verhaltensregeln von dem Verantwortlichen oder dem Auftragsverarbeiter angewendet werden oder wurden, nachgeht und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent macht, und
- d) zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

(3) Die zuständige Aufsichtsbehörde übermittelt den Entwurf der Kriterien für die Akkreditierung einer Stelle nach Absatz 1 gemäß dem Kohärenzverfahren nach Artikel 63 an den Ausschuss.

(4) Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde und der Bestimmungen des Kapitels VIII ergreift eine Stelle gemäß Absatz 1 vorbehaltlich geeigneter Garantien im Falle einer Verletzung der Verhaltensregeln durch einen Verantwortlichen oder einen Auftragsverarbeiter geeignete Maßnahmen, einschließlich eines vorläufigen oder endgültigen Ausschlusses des Verantwortlichen oder Auftragsverarbeiters von den Verhaltensregeln. Sie unterrichtet die zuständige Aufsichtsbehörde über solche Maßnahmen und deren Begründung.

(5) Die zuständige Aufsichtsbehörde widerruft die Akkreditierung einer Stelle gemäß Absatz 1, wenn die Voraussetzungen für ihre Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn die Stelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

(6) Dieser Artikel gilt nicht für die Verarbeitung durch Behörden oder öffentliche Stellen.

Artikel 42

Zertifizierung

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.

- (2) Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden Verantwortlichen oder Auftragsverarbeiter können auch datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen, die gemäß Absatz 5 des vorliegenden Artikels genehmigt worden sind, vorgesehen werden, um nachzuweisen, dass die Verantwortlichen oder Auftragsverarbeiter, die gemäß Artikel 3 nicht unter diese Verordnung fallen, im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe von Artikel 46 Absatz 2 Buchstabe f geeignete Garantien bieten. Diese Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung ein, diese geeigneten Garantien anzuwenden, auch im Hinblick auf die Rechte der betroffenen Personen.
- (3) Die Zertifizierung muss freiwillig und über ein transparentes Verfahren zugänglich sein.
- (4) Eine Zertifizierung gemäß diesem Artikel mindert nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörden, die gemäß Artikel 55 oder 56 zuständig sind.
- (5) Eine Zertifizierung nach diesem Artikel wird durch die Zertifizierungsstellen nach Artikel 43 oder durch die zuständige Aufsichtsbehörde anhand der von dieser zuständigen Aufsichtsbehörde gemäß Artikel 58 Absatz 3 oder — gemäß Artikel 63 — durch den Ausschuss genehmigten Kriterien erteilt. Werden die Kriterien vom Ausschuss genehmigt, kann dies zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen.
- (6) Der Verantwortliche oder der Auftragsverarbeiter, der die von ihm durchgeführte Verarbeitung dem Zertifizierungsverfahren unterwirft, stellt der Zertifizierungsstelle nach Artikel 43 oder gegebenenfalls der zuständigen Aufsichtsbehörde alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung und gewährt ihr den in diesem Zusammenhang erforderlichen Zugang zu seinen Verarbeitungstätigkeiten.
- (7) Die Zertifizierung wird einem Verantwortlichen oder einem Auftragsverarbeiter für eine Höchstdauer von drei Jahren erteilt und kann unter denselben Bedingungen verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden. Die Zertifizierung wird gegebenenfalls durch die Zertifizierungsstellen nach Artikel 43 oder durch die zuständige Aufsichtsbehörde widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.
- (8) Der Ausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen in ein Register auf und veröffentlicht sie in geeigneter Weise.

Artikel 43

Zertifizierungsstellen

- (1) Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 57 und 58 erteilen oder verlängern Zertifizierungsstellen, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügen, nach Unterrichtung der Aufsichtsbehörde — damit diese erforderlichenfalls von ihren Befugnissen gemäß Artikel 58 Absatz 2 Buchstabe h Gebrauch machen kann — die Zertifizierung. Die Mitgliedstaaten stellen sicher, dass diese Zertifizierungsstellen von einer oder beiden der folgenden Stellen akkreditiert werden:
- a) der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde;
 - b) der nationalen Akkreditierungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates ⁽¹⁾ im Einklang mit EN-ISO/IEC 17065/2012 und mit den zusätzlichen von der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde festgelegten Anforderungen benannt wurde.
- (2) Zertifizierungsstellen nach Absatz 1 dürfen nur dann gemäß dem genannten Absatz akkreditiert werden, wenn sie
- a) ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstands der Zertifizierung zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen haben;

⁽¹⁾ Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30).

- b) sich verpflichtet haben, die Kriterien nach Artikel 42 Absatz 5, die von der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde oder — gemäß Artikel 63 — von dem Ausschuss genehmigt wurden, einzuhalten;
- c) Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der Datenschutzzertifizierung sowie der Datenschutzsiegel und -prüfzeichen festgelegt haben;
- d) Verfahren und Strukturen festgelegt haben, mit denen sie Beschwerden über Verletzungen der Zertifizierung oder die Art und Weise, in der die Zertifizierung von dem Verantwortlichen oder dem Auftragsverarbeiter umgesetzt wird oder wurde, nachgehen und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent machen, und
- e) zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen haben, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

(3) Die Akkreditierung von Zertifizierungsstellen nach den Absätzen 1 und 2 erfolgt anhand der Kriterien, die von der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde oder — gemäß Artikel 63 — von dem Ausschuss genehmigt wurden. Im Fall einer Akkreditierung nach Absatz 1 Buchstabe b des vorliegenden Artikels ergänzen diese Anforderungen diejenigen, die in der Verordnung (EG) Nr. 765/2008 und in den technischen Vorschriften, in denen die Methoden und Verfahren der Zertifizierungsstellen beschrieben werden, vorgesehen sind.

(4) Die Zertifizierungsstellen nach Absatz 1 sind unbeschadet der Verantwortung, die der Verantwortliche oder der Auftragsverarbeiter für die Einhaltung dieser Verordnung hat, für die angemessene Bewertung, die der Zertifizierung oder dem Widerruf einer Zertifizierung zugrunde liegt, verantwortlich. Die Akkreditierung wird für eine Höchstdauer von fünf Jahren erteilt und kann unter denselben Bedingungen verlängert werden, sofern die Zertifizierungsstelle die Anforderungen dieses Artikels erfüllt.

(5) Die Zertifizierungsstellen nach Absatz 1 teilen den zuständigen Aufsichtsbehörden die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mit.

(6) Die Anforderungen nach Absatz 3 des vorliegenden Artikels und die Kriterien nach Artikel 42 Absatz 5 werden von der Aufsichtsbehörde in leicht zugänglicher Form veröffentlicht. Die Aufsichtsbehörden übermitteln diese Anforderungen und Kriterien auch dem Ausschuss. Der Ausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel in ein Register auf und veröffentlicht sie in geeigneter Weise.

(7) Unbeschadet des Kapitels VIII widerruft die zuständige Aufsichtsbehörde oder die nationale Akkreditierungsstelle die Akkreditierung einer Zertifizierungsstelle nach Absatz 1, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn eine Zertifizierungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zu erlassen, um die Anforderungen festzulegen, die für die in Artikel 42 Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren zu berücksichtigen sind.

(9) Die Kommission kann Durchführungsrechtsakte erlassen, mit denen technische Standards für Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen sowie Mechanismen zur Förderung und Anerkennung dieser Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen festgelegt werden. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

KAPITEL V

Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen

Artikel 44

Allgemeine Grundsätze der Datenübermittlung

Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

Artikel 45

Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

(1) Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

(2) Bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus berücksichtigt die Kommission insbesondere das Folgende:

- a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. bei der betreffenden internationalen Organisation geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art — auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten — sowie die Anwendung dieser Rechtsvorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, die Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,
- b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und
- c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

(3) Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels bieten. In dem Durchführungsrechtsakt ist ein Mechanismus für eine regelmäßige Überprüfung, die mindestens alle vier Jahre erfolgt, vorzusehen, bei der allen maßgeblichen Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b des vorliegenden Artikels genannte Aufsichtsbehörde bzw. genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

(4) Die Kommission überwacht fortlaufend die Entwicklungen in Drittländern und bei internationalen Organisationen, die die Wirkungsweise der nach Absatz 3 des vorliegenden Artikels erlassenen Beschlüsse und der nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassenen Feststellungen beeinträchtigen könnten.

(5) Die Kommission widerruft, ändert oder setzt die in Absatz 3 des vorliegenden Artikels genannten Beschlüsse im Wege von Durchführungsrechtsakten aus, soweit dies nötig ist und ohne rückwirkende Kraft, soweit entsprechende Informationen — insbesondere im Anschluss an die in Absatz 3 des vorliegenden Artikels genannte Überprüfung — dahingehend vorliegen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifischer Sektor in einem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels mehr gewährleistet. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.

In hinreichend begründeten Fällen äußerster Dringlichkeit erlässt die Kommission gemäß dem in Artikel 93 Absatz 3 genannten Verfahren sofort geltende Durchführungsrechtsakte.

(6) Die Kommission nimmt Beratungen mit dem betreffenden Drittland bzw. der betreffenden internationalen Organisation auf, um Abhilfe für die Situation zu schaffen, die zu dem gemäß Absatz 5 erlassenen Beschluss geführt hat.

(7) Übermittlungen personenbezogener Daten an das betreffende Drittland, das Gebiet oder einen oder mehrere spezifische Sektoren in diesem Drittland oder an die betreffende internationale Organisation gemäß den Artikeln 46 bis 49 werden durch einen Beschluss nach Absatz 5 des vorliegenden Artikels nicht berührt.

(8) Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* und auf ihrer Website eine Liste aller Drittländer beziehungsweise Gebiete und spezifischen Sektoren in einem Drittland und aller internationalen Organisationen, für die sie durch Beschluss festgestellt hat, dass sie ein angemessenes Schutzniveau gewährleisten bzw. nicht mehr gewährleisten.

(9) Von der Kommission auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie durch einen nach dem Prüfverfahren gemäß den Absätzen 3 oder 5 des vorliegenden Artikels erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

Artikel 46

Datenübermittlung vorbehaltlich geeigneter Garantien

(1) Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

(2) Die in Absatz 1 genannten geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in

- a) einem rechtlich bindenden und durchsetzbaren Dokument zwischen den Behörden oder öffentlichen Stellen,
- b) verbindlichen internen Datenschutzvorschriften gemäß Artikel 47,
- c) Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen werden,
- d) von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 genehmigt wurden,
- e) genehmigten Verhaltensregeln gemäß Artikel 40 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder
- f) einem genehmigten Zertifizierungsmechanismus gemäß Artikel 42 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

(3) Vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde können die geeigneten Garantien gemäß Absatz 1 auch insbesondere bestehen in

- a) Vertragsklauseln, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, oder
- b) Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen.

(4) Die Aufsichtsbehörde wendet das Kohärenzverfahren nach Artikel 63 an, wenn ein Fall gemäß Absatz 3 des vorliegenden Artikels vorliegt.

(5) Von einem Mitgliedstaat oder einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilte Genehmigungen bleiben so lange gültig, bis sie erforderlichenfalls von dieser Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden. Von der Kommission auf der Grundlage von Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie erforderlichenfalls mit einem nach Absatz 2 des vorliegenden Artikels erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

Artikel 47

Verbindliche interne Datenschutzvorschriften

(1) Die zuständige Aufsichtsbehörde genehmigt gemäß dem Kohärenzverfahren nach Artikel 63 verbindliche interne Datenschutzvorschriften, sofern diese

- a) rechtlich bindend sind, für alle betreffenden Mitglieder der Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gelten und von diesen Mitgliedern durchgesetzt werden, und dies auch für ihre Beschäftigten gilt,

- b) den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten übertragen und
 - c) die in Absatz 2 festgelegten Anforderungen erfüllen.
- (2) Die verbindlichen internen Datenschutzvorschriften nach Absatz 1 enthalten mindestens folgende Angaben:
- a) Struktur und Kontaktdaten der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und jedes ihrer Mitglieder;
 - b) die betreffenden Datenübermittlungen oder Reihen von Datenübermittlungen einschließlich der betreffenden Arten personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;
 - c) interne und externe Rechtsverbindlichkeit der betreffenden internen Datenschutzvorschriften;
 - d) die Anwendung der allgemeinen Datenschutzgrundsätze, insbesondere Zweckbindung, Datenminimierung, begrenzte Speicherfristen, Datenqualität, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Rechtsgrundlage für die Verarbeitung, Verarbeitung besonderer Kategorien von personenbezogenen Daten, Maßnahmen zur Sicherstellung der Datensicherheit und Anforderungen für die Weiterübermittlung an nicht an diese internen Datenschutzvorschriften gebundene Stellen;
 - e) die Rechte der betroffenen Personen in Bezug auf die Verarbeitung und die diesen offenstehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung nach Artikel 22 unterworfen zu werden sowie des in Artikel 79 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen internen Datenschutzvorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;
 - f) die von dem in einem Mitgliedstaat niedergelassenen Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße eines nicht in der Union niedergelassenen betreffenden Mitglieds der Unternehmensgruppe gegen die verbindlichen internen Datenschutzvorschriften; der Verantwortliche oder der Auftragsverarbeiter ist nur dann teilweise oder vollständig von dieser Haftung befreit, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;
 - g) die Art und Weise, wie die betroffenen Personen über die Bestimmungen der Artikel 13 und 14 hinaus über die verbindlichen internen Datenschutzvorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;
 - h) die Aufgaben jedes gemäß Artikel 37 benannten Datenschutzbeauftragten oder jeder anderen Person oder Einrichtung, die mit der Überwachung der Einhaltung der verbindlichen internen Datenschutzvorschriften in der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, sowie mit der Überwachung der Schulungsmaßnahmen und dem Umgang mit Beschwerden befasst ist;
 - i) die Beschwerdeverfahren;
 - j) die innerhalb der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen internen Datenschutzvorschriften. Derartige Verfahren beinhalten Datenschutzüberprüfungen und Verfahren zur Gewährleistung von Abhilfemaßnahmen zum Schutz der Rechte der betroffenen Person. Die Ergebnisse derartiger Überprüfungen sollten der in Buchstabe h genannten Person oder Einrichtung sowie dem Verwaltungsrat des herrschenden Unternehmens einer Unternehmensgruppe oder der Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, mitgeteilt werden und sollten der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden;
 - k) die Verfahren für die Meldung und Erfassung von Änderungen der Vorschriften und ihre Meldung an die Aufsichtsbehörde;
 - l) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gewährleisten, insbesondere durch Offenlegung der Ergebnisse von Überprüfungen der unter Buchstabe j genannten Maßnahmen gegenüber der Aufsichtsbehörde;
 - m) die Meldeverfahren zur Unterrichtung der zuständigen Aufsichtsbehörde über jegliche für ein Mitglied der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem Drittland geltenden rechtlichen Bestimmungen, die sich nachteilig auf die Garantien auswirken könnten, die die verbindlichen internen Datenschutzvorschriften bieten, und
 - n) geeignete Datenschulungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten.

(3) Die Kommission kann das Format und die Verfahren für den Informationsaustausch über verbindliche interne Datenschutzvorschriften im Sinne des vorliegenden Artikels zwischen Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden festlegen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.

Artikel 48

Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung

Jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, dürfen unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel jedenfalls nur dann anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.

Artikel 49

Ausnahmen für bestimmte Fälle

(1) Falls weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 46, einschließlich verbindlicher interner Datenschutzvorschriften, bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig:

- a) die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde,
- b) die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich,
- c) die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich,
- d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig,
- e) die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich,
- f) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,
- g) die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

Falls die Übermittlung nicht auf eine Bestimmung der Artikel 45 oder 46 — einschließlich der verbindlichen internen Datenschutzvorschriften — gestützt werden könnte und keine der Ausnahmen für einen bestimmten Fall gemäß dem ersten Unterabsatz anwendbar ist, darf eine Übermittlung an ein Drittland oder eine internationale Organisation nur dann erfolgen, wenn die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Der Verantwortliche setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis. Der Verantwortliche unterrichtet die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen; dies erfolgt zusätzlich zu den der betroffenen Person nach den Artikeln 13 und 14 mitgeteilten Informationen.

(2) Datenübermittlungen gemäß Absatz 1 Unterabsatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.

- (3) Absatz 1 Unterabsatz 1 Buchstaben a, b und c und sowie Absatz 1 Unterabsatz 2 gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.
- (4) Das öffentliche Interesse im Sinne des Absatzes 1 Unterabsatz 1 Buchstabe d muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt sein.
- (5) Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im Recht der Mitgliedstaaten aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von personenbezogenen Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten teilen der Kommission derartige Bestimmungen mit.
- (6) Der Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien im Sinne des Absatzes 1 Unterabsatz 2 des vorliegenden Artikels in der Dokumentation gemäß Artikel 30.

Artikel 50

Internationale Zusammenarbeit zum Schutz personenbezogener Daten

In Bezug auf Drittländer und internationale Organisationen treffen die Kommission und die Aufsichtsbehörden geeignete Maßnahmen zur

- a) Entwicklung von Mechanismen der internationalen Zusammenarbeit, durch die die wirksame Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtert wird,
- b) gegenseitigen Leistung internationaler Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten, unter anderem durch Meldungen, Beschwerdeverweisungen, Amtshilfe bei Untersuchungen und Informationsaustausch, sofern geeignete Garantien für den Schutz personenbezogener Daten und anderer Grundrechte und Grundfreiheiten bestehen,
- c) Einbindung maßgeblicher Interessenträger in Diskussionen und Tätigkeiten, die zum Ausbau der internationalen Zusammenarbeit bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten dienen,
- d) Förderung des Austauschs und der Dokumentation von Rechtsvorschriften und Praktiken zum Schutz personenbezogener Daten einschließlich Zuständigkeitskonflikten mit Drittländern.

KAPITEL VI

Unabhängige Aufsichtsbehörden

Abschnitt 1

Unabhängigkeit

Artikel 51

Aufsichtsbehörde

- (1) Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird (im Folgenden „Aufsichtsbehörde“).
- (2) Jede Aufsichtsbehörde leistet einen Beitrag zur einheitlichen Anwendung dieser Verordnung in der gesamten Union. Zu diesem Zweck arbeiten die Aufsichtsbehörden untereinander sowie mit der Kommission gemäß Kapitel VII zusammen.
- (3) Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so bestimmt dieser Mitgliedstaat die Aufsichtsbehörde, die diese Behörden im Ausschuss vertritt, und führt ein Verfahren ein, mit dem sichergestellt wird, dass die anderen Behörden die Regeln für das Kohärenzverfahren nach Artikel 63 einhalten.
- (4) Jeder Mitgliedstaat teilt der Kommission bis spätestens 25. Mai 2018 die Rechtsvorschriften, die er aufgrund dieses Kapitels erlässt, sowie unverzüglich alle folgenden Änderungen dieser Vorschriften mit.

*Artikel 52***Unabhängigkeit**

- (1) Jede Aufsichtsbehörde handelt bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse gemäß dieser Verordnung völlig unabhängig.
- (2) Das Mitglied oder die Mitglieder jeder Aufsichtsbehörde unterliegen bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Verordnung weder direkter noch indirekter Beeinflussung von außen und ersuchen weder um Weisung noch nehmen sie Weisungen entgegen.
- (3) Das Mitglied oder die Mitglieder der Aufsichtsbehörde sehen von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen ab und üben während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus.
- (4) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können.
- (5) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde ihr eigenes Personal auswählt und hat, das ausschließlich der Leitung des Mitglieds oder der Mitglieder der betreffenden Aufsichtsbehörde untersteht.
- (6) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt und dass sie über eigene, öffentliche, jährliche Haushaltspläne verfügt, die Teil des gesamten Staatshaushalts oder nationalen Haushalts sein können.

*Artikel 53***Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde**

- (1) Die Mitgliedstaaten sehen vor, dass jedes Mitglied ihrer Aufsichtsbehörden im Wege eines transparenten Verfahrens ernannt wird, und zwar
- vom Parlament,
 - von der Regierung,
 - vom Staatsoberhaupt oder
 - von einer unabhängigen Stelle, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird.
- (2) Jedes Mitglied muss über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen.
- (3) Das Amt eines Mitglieds endet mit Ablauf der Amtszeit, mit seinem Rücktritt oder verpflichtender Versetzung in den Ruhestand gemäß dem Recht des betroffenen Mitgliedstaats.
- (4) Ein Mitglied wird seines Amtes nur enthoben, wenn es eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung seiner Aufgaben nicht mehr erfüllt.

*Artikel 54***Errichtung der Aufsichtsbehörde**

- (1) Jeder Mitgliedstaat sieht durch Rechtsvorschriften Folgendes vor:
- a) die Errichtung jeder Aufsichtsbehörde;

- b) die erforderlichen Qualifikationen und sonstigen Voraussetzungen für die Ernennung zum Mitglied jeder Aufsichtsbehörde;
- c) die Vorschriften und Verfahren für die Ernennung des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde;
- d) die Amtszeit des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde von mindestens vier Jahren; dies gilt nicht für die erste Amtszeit nach 24. Mai 2016, die für einen Teil der Mitglieder kürzer sein kann, wenn eine zeitlich versetzte Ernennung zur Wahrung der Unabhängigkeit der Aufsichtsbehörde notwendig ist;
- e) die Frage, ob und — wenn ja — wie oft das Mitglied oder die Mitglieder jeder Aufsichtsbehörde wiederernannt werden können;
- f) die Bedingungen im Hinblick auf die Pflichten des Mitglieds oder der Mitglieder und der Bediensteten jeder Aufsichtsbehörde, die Verbote von Handlungen, beruflichen Tätigkeiten und Vergütungen während und nach der Amtszeit, die mit diesen Pflichten unvereinbar sind, und die Regeln für die Beendigung des Beschäftigungsverhältnisses.

(2) Das Mitglied oder die Mitglieder und die Bediensteten jeder Aufsichtsbehörde sind gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten sowohl während ihrer Amts- beziehungsweise Dienstzeit als auch nach deren Beendigung verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben oder der Ausübung ihrer Befugnisse bekannt geworden sind, Verschwiegenheit zu wahren. Während dieser Amts- beziehungsweise Dienstzeit gilt diese Verschwiegenheitspflicht insbesondere für die von natürlichen Personen gemeldeten Verstößen gegen diese Verordnung.

Abschnitt 2

Zuständigkeit, Aufgaben und Befugnisse

Artikel 55

Zuständigkeit

- (1) Jede Aufsichtsbehörde ist für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig.
- (2) Erfolgt die Verarbeitung durch Behörden oder private Stellen auf der Grundlage von Artikel 6 Absatz 1 Buchstabe c oder e, so ist die Aufsichtsbehörde des betroffenen Mitgliedstaats zuständig. In diesem Fall findet Artikel 56 keine Anwendung.
- (3) Die Aufsichtsbehörden sind nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

Artikel 56

Zuständigkeit der federführenden Aufsichtsbehörde

- (1) Unbeschadet des Artikels 55 ist die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters gemäß dem Verfahren nach Artikel 60 die zuständige federführende Aufsichtsbehörde für die von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführte grenzüberschreitende Verarbeitung.
- (2) Abweichend von Absatz 1 ist jede Aufsichtsbehörde dafür zuständig, sich mit einer bei ihr eingereichten Beschwerde oder einem etwaigen Verstoß gegen diese Verordnung zu befassen, wenn der Gegenstand nur mit einer Niederlassung in ihrem Mitgliedstaat zusammenhängt oder betroffene Personen nur ihres Mitgliedstaats erheblich beeinträchtigt.
- (3) In den in Absatz 2 des vorliegenden Artikels genannten Fällen unterrichtet die Aufsichtsbehörde unverzüglich die federführende Aufsichtsbehörde über diese Angelegenheit. Innerhalb einer Frist von drei Wochen nach der Unterrichtung entscheidet die federführende Aufsichtsbehörde, ob sie sich mit dem Fall gemäß dem Verfahren nach Artikel 60 befasst oder nicht, wobei sie berücksichtigt, ob der Verantwortliche oder der Auftragsverarbeiter in dem Mitgliedstaat, dessen Aufsichtsbehörde sie unterrichtet hat, eine Niederlassung hat oder nicht.

(4) Entscheidet die federführende Aufsichtsbehörde, sich mit dem Fall zu befassen, so findet das Verfahren nach Artikel 60 Anwendung. Die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, kann dieser einen Beschlussentwurf vorlegen. Die federführende Aufsichtsbehörde trägt diesem Entwurf bei der Ausarbeitung des Beschlussentwurfs nach Artikel 60 Absatz 3 weitestgehend Rechnung.

(5) Entscheidet die federführende Aufsichtsbehörde, sich mit dem Fall nicht selbst zu befassen, so befasst die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, sich mit dem Fall gemäß den Artikeln 61 und 62.

(6) Die federführende Aufsichtsbehörde ist der einzige Ansprechpartner der Verantwortlichen oder der Auftragsverarbeiter für Fragen der von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführten grenzüberschreitenden Verarbeitung.

Artikel 57

Aufgaben

(1) Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet

- a) die Anwendung dieser Verordnung überwachen und durchsetzen;
- b) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;
- c) im Einklang mit dem Recht des Mitgliedsstaats das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten;
- d) die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren;
- e) auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Verordnung zur Verfügung stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenarbeiten;
- f) sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 80 befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;
- g) mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten;
- h) Untersuchungen über die Anwendung dieser Verordnung durchführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;
- i) maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken;
- j) Standardvertragsklauseln im Sinne des Artikels 28 Absatz 8 und des Artikels 46 Absatz 2 Buchstabe d festlegen;
- k) eine Liste der Verarbeitungsarten erstellen und führen, für die gemäß Artikel 35 Absatz 4 eine Datenschutz-Folgenabschätzung durchzuführen ist;
- l) Beratung in Bezug auf die in Artikel 36 Absatz 2 genannten Verarbeitungsvorgänge leisten;
- m) die Ausarbeitung von Verhaltensregeln gemäß Artikel 40 Absatz 1 fördern und zu diesen Verhaltensregeln, die ausreichende Garantien im Sinne des Artikels 40 Absatz 5 bieten müssen, Stellungnahmen abgeben und sie billigen;
- n) die Einführung von Datenschutzzertifizierungsmechanismen und von Datenschutzsiegeln und -prüfzeichen nach Artikel 42 Absatz 1 anregen und Zertifizierungskriterien nach Artikel 42 Absatz 5 billigen;
- o) gegebenenfalls die nach Artikel 42 Absatz 7 erteilten Zertifizierungen regelmäßig überprüfen;

- p) die Kriterien für die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 abfassen und veröffentlichen;
- q) die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 vornehmen;
- r) Vertragsklauseln und Bestimmungen im Sinne des Artikels 46 Absatz 3 genehmigen;
- s) verbindliche interne Vorschriften gemäß Artikel 47 genehmigen;
- t) Beiträge zur Tätigkeit des Ausschusses leisten;
- u) interne Verzeichnisse über Verstöße gegen diese Verordnung und gemäß Artikel 58 Absatz 2 ergriffene Maßnahmen und
- v) jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen.

(2) Jede Aufsichtsbehörde erleichtert das Einreichen von in Absatz 1 Buchstabe f genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(3) Die Erfüllung der Aufgaben jeder Aufsichtsbehörde ist für die betroffene Person und gegebenenfalls für den Datenschutzbeauftragten unentgeltlich.

(4) Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anfragen kann die Aufsichtsbehörde eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

Artikel 58

Befugnisse

- (1) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Untersuchungsbefugnisse, die es ihr gestatten,
- a) den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind,
 - b) Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen,
 - c) eine Überprüfung der nach Artikel 42 Absatz 7 erteilten Zertifizierungen durchzuführen,
 - d) den Verantwortlichen oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen diese Verordnung hinzuweisen,
 - e) von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten,
 - f) gemäß dem Verfahrensrecht der Union oder dem Verfahrensrecht des Mitgliedstaats Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten.
- (2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,
- a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,
 - b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat,
 - c) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen,

- d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,
 - e) den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person entsprechend zu benachrichtigen,
 - f) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,
 - g) die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß den Artikeln 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Artikel 17 Absatz 2 und Artikel 19 offengelegt wurden, über solche Maßnahmen anzuordnen,
 - h) eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,
 - i) eine Geldbuße gemäß Artikel 83 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls,
 - j) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.
- (3) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Genehmigungsbefugnisse und beratenden Befugnisse, die es ihr gestatten,
- a) gemäß dem Verfahren der vorherigen Konsultation nach Artikel 36 den Verantwortlichen zu beraten,
 - b) zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an das nationale Parlament, die Regierung des Mitgliedstaats oder im Einklang mit dem Recht des Mitgliedstaats an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten,
 - c) die Verarbeitung gemäß Artikel 36 Absatz 5 zu genehmigen, falls im Recht des Mitgliedstaats eine derartige vorherige Genehmigung verlangt wird,
 - d) eine Stellungnahme abzugeben und Entwürfe von Verhaltensregeln gemäß Artikel 40 Absatz 5 zu billigen,
 - e) Zertifizierungsstellen gemäß Artikel 43 zu akkreditieren,
 - f) im Einklang mit Artikel 42 Absatz 5 Zertifizierungen zu erteilen und Kriterien für die Zertifizierung zu billigen,
 - g) Standarddatenschutzklauseln nach Artikel 28 Absatz 8 und Artikel 46 Absatz 2 Buchstabe d festzulegen,
 - h) Vertragsklauseln gemäß Artikel 46 Absatz 3 Buchstabe a zu genehmigen,
 - i) Verwaltungsvereinbarungen gemäß Artikel 46 Absatz 3 Buchstabe b zu genehmigen
 - j) verbindliche interne Vorschriften gemäß Artikel 47 zu genehmigen.
- (4) Die Ausübung der der Aufsichtsbehörde gemäß diesem Artikel übertragenen Befugnisse erfolgt vorbehaltlich geeigneter Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta.
- (5) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass seine Aufsichtsbehörde befugt ist, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die Bestimmungen dieser Verordnung durchzusetzen.
- (6) Jeder Mitgliedstaat kann durch Rechtsvorschriften vorsehen, dass seine Aufsichtsbehörde neben den in den Absätzen 1, 2 und 3 aufgeführten Befugnissen über zusätzliche Befugnisse verfügt. Die Ausübung dieser Befugnisse darf nicht die effektive Durchführung des Kapitels VII beeinträchtigen.

Artikel 59

Tätigkeitsbericht

Jede Aufsichtsbehörde erstellt einen Jahresbericht über ihre Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen nach Artikel 58 Absatz 2 enthalten kann. Diese Berichte werden dem nationalen Parlament, der Regierung und anderen nach dem Recht der Mitgliedstaaten bestimmten Behörden übermittelt. Sie werden der Öffentlichkeit, der Kommission und dem Ausschuss zugänglich gemacht.

KAPITEL VII

Zusammenarbeit und Kohärenz

Abschnitt 1

Zusammenarbeit

Artikel 60

Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden

- (1) Die federführende Aufsichtsbehörde arbeitet mit den anderen betroffenen Aufsichtsbehörden im Einklang mit diesem Artikel zusammen und bemüht sich dabei, einen Konsens zu erzielen. Die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden tauschen untereinander alle zweckdienlichen Informationen aus.
- (2) Die federführende Aufsichtsbehörde kann jederzeit andere betroffene Aufsichtsbehörden um Amtshilfe gemäß Artikel 61 ersuchen und gemeinsame Maßnahmen gemäß Artikel 62 durchführen, insbesondere zur Durchführung von Untersuchungen oder zur Überwachung der Umsetzung einer Maßnahme in Bezug auf einen Verantwortlichen oder einen Auftragsverarbeiter, der in einem anderen Mitgliedstaat niedergelassen ist.
- (3) Die federführende Aufsichtsbehörde übermittelt den anderen betroffenen Aufsichtsbehörden unverzüglich die zweckdienlichen Informationen zu der Angelegenheit. Sie legt den anderen betroffenen Aufsichtsbehörden unverzüglich einen Beschlussentwurf zur Stellungnahme vor und trägt deren Standpunkten gebührend Rechnung.
- (4) Legt eine der anderen betroffenen Aufsichtsbehörden innerhalb von vier Wochen, nachdem sie gemäß Absatz 3 des vorliegenden Artikels konsultiert wurde, gegen diesen Beschlussentwurf einen maßgeblichen und begründeten Einspruch ein und schließt sich die federführende Aufsichtsbehörde dem maßgeblichen und begründeten Einspruch nicht an oder ist der Ansicht, dass der Einspruch nicht maßgeblich oder nicht begründet ist, so leitet die federführende Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 für die Angelegenheit ein.
- (5) Beabsichtigt die federführende Aufsichtsbehörde, sich dem maßgeblichen und begründeten Einspruch anzuschließen, so legt sie den anderen betroffenen Aufsichtsbehörden einen überarbeiteten Beschlussentwurf zur Stellungnahme vor. Der überarbeitete Beschlussentwurf wird innerhalb von zwei Wochen dem Verfahren nach Absatz 4 unterzogen.
- (6) Legt keine der anderen betroffenen Aufsichtsbehörden Einspruch gegen den Beschlussentwurf ein, der von der federführenden Aufsichtsbehörde innerhalb der in den Absätzen 4 und 5 festgelegten Frist vorgelegt wurde, so gelten die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden als mit dem Beschlussentwurf einverstanden und sind an ihn gebunden.
- (7) Die federführende Aufsichtsbehörde erlässt den Beschluss und teilt ihn der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder gegebenenfalls des Auftragsverarbeiters mit und setzt die anderen betroffenen Aufsichtsbehörden und den Ausschuss von dem betreffenden Beschluss einschließlich einer Zusammenfassung der maßgeblichen Fakten und Gründe in Kenntnis. Die Aufsichtsbehörde, bei der eine Beschwerde eingereicht worden ist, unterrichtet den Beschwerdeführer über den Beschluss.
- (8) Wird eine Beschwerde abgelehnt oder abgewiesen, so erlässt die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, abweichend von Absatz 7 den Beschluss, teilt ihn dem Beschwerdeführer mit und setzt den Verantwortlichen in Kenntnis.
- (9) Sind sich die federführende Aufsichtsbehörde und die betreffenden Aufsichtsbehörden darüber einig, Teile der Beschwerde abzulehnen oder abzuweisen und bezüglich anderer Teile dieser Beschwerde tätig zu werden, so wird in dieser Angelegenheit für jeden dieser Teile ein eigener Beschluss erlassen. Die federführende Aufsichtsbehörde erlässt den Beschluss für den Teil, der das Tätigwerden in Bezug auf den Verantwortlichen betrifft, teilt ihn der Hauptniederlassung oder einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters im Hoheitsgebiet ihres Mitgliedstaats mit und setzt den Beschwerdeführer hiervon in Kenntnis, während die für den Beschwerdeführer zuständige Aufsichtsbehörde den Beschluss für den Teil erlässt, der die Ablehnung oder Abweisung dieser Beschwerde betrifft, und ihn diesem Beschwerdeführer mitteilt und den Verantwortlichen oder den Auftragsverarbeiter hiervon in Kenntnis setzt.
- (10) Nach der Unterrichtung über den Beschluss der federführenden Aufsichtsbehörde gemäß den Absätzen 7 und 9 ergreift der Verantwortliche oder der Auftragsverarbeiter die erforderlichen Maßnahmen, um die Verarbeitungstätigkeiten all seiner Niederlassungen in der Union mit dem Beschluss in Einklang zu bringen. Der Verantwortliche oder der Auftragsverarbeiter teilt der federführenden Aufsichtsbehörde die Maßnahmen mit, die zur Einhaltung des Beschlusses ergriffen wurden; diese wiederum unterrichtet die anderen betroffenen Aufsichtsbehörden.

(11) Hat — in Ausnahmefällen — eine betroffene Aufsichtsbehörde Grund zu der Annahme, dass zum Schutz der Interessen betroffener Personen dringender Handlungsbedarf besteht, so kommt das Dringlichkeitsverfahren nach Artikel 66 zur Anwendung.

(12) Die federführende Aufsichtsbehörde und die anderen betroffenen Aufsichtsbehörden übermitteln einander die nach diesem Artikel geforderten Informationen auf elektronischem Wege unter Verwendung eines standardisierten Formats.

Artikel 61

Gegenseitige Amtshilfe

(1) Die Aufsichtsbehörden übermitteln einander maßgebliche Informationen und gewähren einander Amtshilfe, um diese Verordnung einheitlich durchzuführen und anzuwenden, und treffen Vorkehrungen für eine wirksame Zusammenarbeit. Die Amtshilfe bezieht sich insbesondere auf Auskunftersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um vorherige Genehmigungen und eine vorherige Konsultation, um Vornahme von Nachprüfungen und Untersuchungen.

(2) Jede Aufsichtsbehörde ergreift alle geeigneten Maßnahmen, um einem 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 ersuchte Aufsichtsbehörde lehnt das Ersuchen nur ab, wenn

a) sie für den Gegenstand des Ersuchens oder für die Maßnahmen, die sie durchführen soll, nicht zuständig ist oder

b) ein Eingehen auf das Ersuchen gegen diese Verordnung verstoßen würde oder gegen das Unionsrecht oder das Recht der Mitgliedstaaten, dem die Aufsichtsbehörde, bei der das Ersuchen eingeht, unterliegt.

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

(6) Die ersuchten Aufsichtsbehörden übermitteln die Informationen, um die von einer anderen Aufsichtsbehörde ersucht wurde, in der Regel auf elektronischem Wege unter Verwendung eines standardisierten Formats.

(7) Ersuchte Aufsichtsbehörden verlangen für Maßnahmen, die sie 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.

(8) Erteilt eine ersuchte Aufsichtsbehörde nicht binnen eines Monats nach Eingang des Ersuchens einer anderen Aufsichtsbehörde die Informationen gemäß Absatz 5, so kann die ersuchende Aufsichtsbehörde eine einstweilige Maßnahme im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 55 Absatz 1 ergreifen. In diesem Fall wird von einem dringenden Handlungsbedarf gemäß Artikel 66 Absatz 1 ausgegangen, der einen im Dringlichkeitsverfahren angenommenen verbindlichen Beschluss des Ausschuss gemäß Artikel 66 Absatz 2 erforderlich macht.

(9) Die Kommission kann im Wege von Durchführungsrechtsakten Form und Verfahren der Amtshilfe nach diesem Artikel und die Ausgestaltung des elektronischen Informationsaustauschs zwischen den Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Ausschuss, insbesondere das in Absatz 6 des vorliegenden Artikels genannte standardisierte Format, festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 62

Gemeinsame Maßnahmen der Aufsichtsbehörden

(1) Die Aufsichtsbehörden führen gegebenenfalls gemeinsame Maßnahmen einschließlich gemeinsamer Untersuchungen und gemeinsamer Durchsetzungsmaßnahmen durch, an denen Mitglieder oder Bedienstete der Aufsichtsbehörden anderer Mitgliedstaaten teilnehmen.

(2) Verfügt der Verantwortliche oder der Auftragsverarbeiter über Niederlassungen in mehreren Mitgliedstaaten oder werden die Verarbeitungsvorgänge voraussichtlich auf eine bedeutende Zahl betroffener Personen in mehr als einem Mitgliedstaat erhebliche Auswirkungen haben, ist die Aufsichtsbehörde jedes dieser Mitgliedstaaten berechtigt, an den gemeinsamen Maßnahmen teilzunehmen. Die gemäß Artikel 56 Absatz 1 oder Absatz 4 zuständige Aufsichtsbehörde lädt die Aufsichtsbehörde jedes dieser Mitgliedstaaten zur Teilnahme an den gemeinsamen Maßnahmen ein und antwortet unverzüglich auf das Ersuchen einer Aufsichtsbehörde um Teilnahme.

(3) Eine Aufsichtsbehörde kann gemäß dem Recht des Mitgliedstaats und mit Genehmigung der unterstützenden Aufsichtsbehörde den an den gemeinsamen Maßnahmen beteiligten Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde Befugnisse einschließlich Untersuchungsbefugnisse übertragen oder, soweit dies nach dem Recht des Mitgliedstaats der einladenden Aufsichtsbehörde zulässig ist, den Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde gestatten, ihre Untersuchungsbefugnisse nach dem Recht des Mitgliedstaats der unterstützenden Aufsichtsbehörde auszuüben. Diese Untersuchungsbefugnisse können nur unter der Leitung und in Gegenwart der Mitglieder oder Bediensteten der einladenden Aufsichtsbehörde ausgeübt werden. Die Mitglieder oder Bediensteten der unterstützenden Aufsichtsbehörde unterliegen dem Recht des Mitgliedstaats der einladenden Aufsichtsbehörde.

(4) Sind gemäß Absatz 1 Bedienstete einer unterstützenden Aufsichtsbehörde in einem anderen Mitgliedstaat im Einsatz, so übernimmt der Mitgliedstaat der einladenden Aufsichtsbehörde nach Maßgabe des Rechts des Mitgliedstaats, in dessen Hoheitsgebiet der Einsatz erfolgt, die Verantwortung für ihr Handeln, einschließlich der Haftung für alle von ihnen bei ihrem Einsatz verursachten Schäden.

(5) Der Mitgliedstaat, in dessen Hoheitsgebiet der Schaden verursacht wurde, ersetzt diesen Schaden so, wie er ihn ersetzen müsste, wenn seine eigenen Bediensteten ihn verursacht hätten. Der Mitgliedstaat der unterstützenden Aufsichtsbehörde, deren Bedienstete im Hoheitsgebiet eines anderen Mitgliedstaats einer Person Schaden zugefügt haben, erstattet diesem anderen Mitgliedstaat den Gesamtbetrag des Schadenersatzes, den dieser an die Berechtigten geleistet hat.

(6) Unbeschadet der Ausübung seiner Rechte gegenüber Dritten und mit Ausnahme des Absatzes 5 verzichtet jeder Mitgliedstaat in dem Fall des Absatzes 1 darauf, den in Absatz 4 genannten Betrag des erlittenen Schadens anderen Mitgliedstaaten gegenüber geltend zu machen.

(7) Ist eine gemeinsame Maßnahme geplant und kommt eine Aufsichtsbehörde binnen eines Monats nicht der Verpflichtung nach Absatz 2 Satz 2 des vorliegenden Artikels nach, so können die anderen Aufsichtsbehörden eine einstweilige Maßnahme im Hoheitsgebiet ihres Mitgliedstaats gemäß Artikel 55 ergreifen. In diesem Fall wird von einem dringenden Handlungsbedarf gemäß Artikel 66 Absatz 1 ausgegangen, der eine im Dringlichkeitsverfahren angenommene Stellungnahme oder einen im Dringlichkeitsverfahren angenommenen verbindlichen Beschluss des Ausschusses gemäß Artikel 66 Absatz 2 erforderlich macht.

Abschnitt 2

Kohärenz

Artikel 63

Kohärenzverfahren

Um zur einheitlichen Anwendung dieser Verordnung in der gesamten Union beizutragen, arbeiten die Aufsichtsbehörden im Rahmen des in diesem Abschnitt beschriebenen Kohärenzverfahrens untereinander und gegebenenfalls mit der Kommission zusammen.

Artikel 64

Stellungnahme Ausschusses

(1) Der Ausschuss gibt eine Stellungnahme ab, wenn die zuständige Aufsichtsbehörde beabsichtigt, eine der nachstehenden Maßnahmen zu erlassen. Zu diesem Zweck übermittelt die zuständige Aufsichtsbehörde dem Ausschuss den Entwurf des Beschlusses, wenn dieser

- a) der Annahme einer Liste der Verarbeitungsvorgänge dient, die der Anforderung einer Datenschutz-Folgenabschätzung gemäß Artikel 35 Absatz 4 unterliegen,
- b) eine Angelegenheit gemäß Artikel 40 Absatz 7 und damit die Frage betrifft, ob ein Entwurf von Verhaltensregeln oder eine Änderung oder Ergänzung von Verhaltensregeln mit dieser Verordnung in Einklang steht,

- c) der Billigung der Kriterien für die Akkreditierung einer Stelle nach Artikel 41 Absatz 3 oder einer Zertifizierungsstelle nach Artikel 43 Absatz 3 dient,
- d) der Festlegung von Standard-Datenschutzklauseln gemäß Artikel 46 Absatz 2 Buchstabe d und Artikel 28 Absatz 8 dient,
- e) der Genehmigung von Vertragsklauseln gemäß Artikels 46 Absatz 3 Buchstabe a dient, oder
- f) der Annahme verbindlicher interner Vorschriften im Sinne von Artikel 47 dient.

(2) Jede Aufsichtsbehörde, der Vorsitz des Ausschuss oder die Kommission können beantragen, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat vom Ausschuss geprüft wird, um eine Stellungnahme zu erhalten, insbesondere wenn eine zuständige Aufsichtsbehörde den Verpflichtungen zur Amtshilfe gemäß Artikel 61 oder zu gemeinsamen Maßnahmen gemäß Artikel 62 nicht nachkommt.

(3) In den in den Absätzen 1 und 2 genannten Fällen gibt der Ausschuss eine Stellungnahme zu der Angelegenheit ab, die ihm vorgelegt wurde, sofern er nicht bereits eine Stellungnahme zu derselben Angelegenheit abgegeben hat. Diese Stellungnahme wird binnen acht Wochen mit der einfachen Mehrheit der Mitglieder des Ausschusses angenommen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit um weitere sechs Wochen verlängert werden. Was den in Absatz 1 genannten Beschlussentwurf angeht, der gemäß Absatz 5 den Mitgliedern des Ausschusses übermittelt wird, so wird angenommen, dass ein Mitglied, das innerhalb einer vom Vorsitz angegebenen angemessenen Frist keine Einwände erhoben hat, dem Beschlussentwurf zustimmt.

(4) Die Aufsichtsbehörden und die Kommission übermitteln unverzüglich dem Ausschuss auf elektronischem Wege unter Verwendung eines standardisierten Formats alle zweckdienlichen Informationen, einschließlich — je nach Fall — einer kurzen Darstellung des Sachverhalts, des Beschlussentwurfs, der Gründe, warum eine solche Maßnahme ergriffen werden muss, und der Standpunkte anderer betroffener Aufsichtsbehörden.

(5) Der Vorsitz des Ausschusses unterrichtet unverzüglich auf elektronischem Wege

- a) unter Verwendung eines standardisierten Formats die Mitglieder des Ausschusses und die Kommission über alle zweckdienlichen Informationen, die ihm zugegangen sind. Soweit erforderlich stellt das Sekretariat des Ausschusses Übersetzungen der zweckdienlichen Informationen zur Verfügung und
- b) je nach Fall die in den Absätzen 1 und 2 genannte Aufsichtsbehörde und die Kommission über die Stellungnahme und veröffentlicht sie.

(6) Die zuständige Aufsichtsbehörde nimmt den in Absatz 1 genannten Beschlussentwurf nicht vor Ablauf der in Absatz 3 genannten Frist an.

(7) Die in Absatz 1 genannte Aufsichtsbehörde trägt der Stellungnahme des Ausschusses s weitestgehend Rechnung und teilt dessen Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme auf elektronischem Wege unter Verwendung eines standardisierten Formats mit, ob sie den Beschlussentwurf beibehalten oder ändern wird; gegebenenfalls übermittelt sie den geänderten Beschlussentwurf.

(8) Teilt die betroffene Aufsichtsbehörde dem Vorsitz des Ausschusses innerhalb der Frist nach Absatz 7 des vorliegenden Artikels unter Angabe der maßgeblichen Gründe mit, dass sie beabsichtigt, der Stellungnahme des Ausschusses insgesamt oder teilweise nicht zu folgen, so gilt Artikel 65 Absatz 1.

Artikel 65

Streitbeilegung durch den Ausschuss

(1) Um die ordnungsgemäße und einheitliche Anwendung dieser Verordnung in Einzelfällen sicherzustellen, erlässt der Ausschuss in den folgenden Fällen einen verbindlichen Beschluss:

- a) wenn eine betroffene Aufsichtsbehörde in einem Fall nach Artikel 60 Absatz 4 einen maßgeblichen und begründeten Einspruch gegen einen Beschlussentwurf der federführenden Behörde eingelegt hat oder die federführende Behörde einen solchen Einspruch als nicht maßgeblich oder nicht begründet abgelehnt hat. Der verbindliche Beschluss betrifft alle Angelegenheiten, die Gegenstand des maßgeblichen und begründeten Einspruchs sind, insbesondere die Frage, ob ein Verstoß gegen diese Verordnung vorliegt;

- b) wenn es widersprüchliche Standpunkte dazu gibt, welche der betroffenen Aufsichtsbehörden für die Hauptniederlassung zuständig ist,
- c) wenn eine zuständige Aufsichtsbehörde in den in Artikel 64 Absatz 1 genannten Fällen keine Stellungnahme des Ausschusses einholt oder der Stellungnahme des Ausschusses gemäß Artikel 64 nicht folgt. In diesem Fall kann jede betroffene Aufsichtsbehörde oder die Kommission die Angelegenheit dem Ausschuss vorlegen.
- (2) Der in Absatz 1 genannte Beschluss wird innerhalb eines Monats nach der Befassung mit der Angelegenheit mit einer Mehrheit von zwei Dritteln der Mitglieder des Ausschusses angenommen. Diese Frist kann wegen der Komplexität der Angelegenheit um einen weiteren Monat verlängert werden. Der in Absatz 1 genannte Beschluss wird begründet und an die federführende Aufsichtsbehörde und alle betroffenen Aufsichtsbehörden übermittelt und ist für diese verbindlich.
- (3) War der Ausschuss nicht in der Lage, innerhalb der in Absatz 2 genannten Fristen einen Beschluss anzunehmen, so nimmt er seinen Beschluss innerhalb von zwei Wochen nach Ablauf des in Absatz 2 genannten zweiten Monats mit einfacher Mehrheit der Mitglieder des Ausschusses an. Bei Stimmengleichheit zwischen den Mitgliedern des Ausschusses gibt die Stimme des Vorsitzes den Ausschlag.
- (4) Die betroffenen Aufsichtsbehörden nehmen vor Ablauf der in den Absätzen 2 und 3 genannten Fristen keinen Beschluss über die dem Ausschuss vorgelegte Angelegenheit an.
- (5) Der Vorsitz des Ausschusses unterrichtet die betroffenen Aufsichtsbehörden unverzüglich über den in Absatz 1 genannten Beschluss. Er setzt die Kommission hiervon in Kenntnis. Der Beschluss wird unverzüglich auf der Website des Ausschusses veröffentlicht, nachdem die Aufsichtsbehörde den in Absatz 6 genannten endgültigen Beschluss mitgeteilt hat.
- (6) Die federführende Aufsichtsbehörde oder gegebenenfalls die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, trifft den endgültigen Beschluss auf der Grundlage des in Absatz 1 des vorliegenden Artikels genannten Beschlusses unverzüglich und spätestens einen Monat, nachdem der Europäische Datenschutzausschuss seinen Beschluss mitgeteilt hat. Die federführende Aufsichtsbehörde oder gegebenenfalls die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, setzt den Ausschuss von dem Zeitpunkt, zu dem ihr endgültiger Beschluss dem Verantwortlichen oder dem Auftragsverarbeiter bzw. der betroffenen Person mitgeteilt wird, in Kenntnis. Der endgültige Beschluss der betroffenen Aufsichtsbehörden wird gemäß Artikel 60 Absätze 7, 8 und 9 angenommen. Im endgültigen Beschluss wird auf den in Absatz 1 genannten Beschluss verwiesen und festgelegt, dass der in Absatz 1 des vorliegenden Artikels genannte Beschluss gemäß Absatz 5 auf der Website des Ausschusses veröffentlicht wird. Dem endgültigen Beschluss wird der in Absatz 1 des vorliegenden _Artikels genannte Beschluss beigefügt.

Artikel 66

Dringlichkeitsverfahren

- (1) Unter außergewöhnlichen Umständen kann eine betroffene Aufsichtsbehörde abweichend vom Kohärenzverfahren nach Artikel 63, 64 und 65 oder dem Verfahren nach Artikel 60 sofort einstweilige Maßnahmen mit festgelegter Geltungsdauer von höchstens drei Monaten treffen, die in ihrem Hoheitsgebiet rechtliche Wirkung entfalten sollen, wenn sie zu der Auffassung gelangt, dass dringender Handlungsbedarf besteht, um Rechte und Freiheiten von betroffenen Personen zu schützen. Die Aufsichtsbehörde setzt die anderen betroffenen Aufsichtsbehörden, den Ausschuss und die Kommission unverzüglich von diesen Maßnahmen und den Gründen für deren Erlass in Kenntnis.
- (2) Hat eine Aufsichtsbehörde eine Maßnahme nach Absatz 1 ergriffen und ist sie der Auffassung, dass dringend endgültige Maßnahmen erlassen werden müssen, kann sie unter Angabe von Gründen im Dringlichkeitsverfahren um eine Stellungnahme oder einen verbindlichen Beschluss des Ausschusses ersuchen.
- (3) Jede Aufsichtsbehörde kann unter Angabe von Gründen, auch für den dringenden Handlungsbedarf, im Dringlichkeitsverfahren um eine Stellungnahme oder gegebenenfalls einen verbindlichen Beschluss des Ausschusses ersuchen, wenn eine zuständige Aufsichtsbehörde trotz dringenden Handlungsbedarfs keine geeignete Maßnahme getroffen hat, um die Rechte und Freiheiten von betroffenen Personen zu schützen.
- (4) Abweichend von Artikel 64 Absatz 3 und Artikel 65 Absatz 2 wird eine Stellungnahme oder ein verbindlicher Beschluss im Dringlichkeitsverfahren nach den Absätzen 2 und 3 binnen zwei Wochen mit einfacher Mehrheit der Mitglieder des Ausschusses angenommen.

*Artikel 67***Informationsaustausch**

Die Kommission kann Durchführungsrechtsakte von allgemeiner Tragweite zur Festlegung der Ausgestaltung des elektronischen Informationsaustauschs zwischen den Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Ausschuss, insbesondere des standardisierten Formats nach Artikel 64, erlassen.

Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.

Abschnitt 3

Europäischer Datenschutzausschuss*Artikel 68***Europäischer Datenschutzausschuss**

- (1) Der Europäische Datenschutzausschuss (im Folgenden „Ausschuss“) wird als Einrichtung der Union mit eigener Rechtspersönlichkeit eingerichtet.
- (2) Der Ausschuss wird von seinem Vorsitz vertreten.
- (3) Der Ausschuss besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern.
- (4) Ist in einem Mitgliedstaat mehr als eine Aufsichtsbehörde für die Überwachung der Anwendung der nach Maßgabe dieser Verordnung erlassenen Vorschriften zuständig, so wird im Einklang mit den Rechtsvorschriften dieses Mitgliedstaats ein gemeinsamer Vertreter benannt.
- (5) Die Kommission ist berechtigt, ohne Stimmrecht an den Tätigkeiten und Sitzungen des Ausschusses teilzunehmen. Die Kommission benennt einen Vertreter. Der Vorsitz des Ausschusses unterrichtet die Kommission über die Tätigkeiten des Ausschusses.
- (6) In den in Artikel 65 genannten Fällen ist der Europäische Datenschutzbeauftragte nur bei Beschlüssen stimmberechtigt, die Grundsätze und Vorschriften betreffen, die für die Organe, Einrichtungen, Ämter und Agenturen der Union gelten und inhaltlich den Grundsätzen und Vorschriften dieser Verordnung entsprechen.

*Artikel 69***Unabhängigkeit**

- (1) Der Ausschuss handelt bei der Erfüllung seiner Aufgaben oder in Ausübung seiner Befugnisse gemäß den Artikeln 70 und 71 unabhängig.
- (2) Unbeschadet der Ersuchen der Kommission gemäß Artikel 70 Absatz 1 Buchstabe b und Absatz 2 ersucht der Ausschuss bei der Erfüllung seiner Aufgaben oder in Ausübung seiner Befugnisse weder um Weisung noch nimmt er Weisungen entgegen.

*Artikel 70***Aufgaben des Ausschusses**

- (1) Der Ausschuss stellt die einheitliche Anwendung dieser Verordnung sicher. Hierzu nimmt der Ausschuss von sich aus oder gegebenenfalls auf Ersuchen der Kommission insbesondere folgende Tätigkeiten wahr:
 - a) Überwachung und Sicherstellung der ordnungsgemäßen Anwendung dieser Verordnung in den in den Artikeln 64 und 65 genannten Fällen unbeschadet der Aufgaben der nationalen Aufsichtsbehörden;

- b) Beratung der Kommission in allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten in der Union stehen, einschließlich etwaiger Vorschläge zur Änderung dieser Verordnung;
- c) Beratung der Kommission über das Format und die Verfahren für den Austausch von Informationen zwischen den Verantwortlichen, den Auftragsverarbeitern und den Aufsichtsbehörden in Bezug auf verbindliche interne Datenschutzvorschriften;
- d) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren zu Verfahren für die Löschung gemäß Artikel 17 Absatz 2 von Links zu personenbezogenen Daten oder Kopien oder Replikationen dieser Daten aus öffentlich zugänglichen Kommunikationsdiensten;
- e) Prüfung — von sich aus, auf Antrag eines seiner Mitglieder oder auf Ersuchen der Kommission — von die Anwendung dieser Verordnung betreffenden Fragen und Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren zwecks Sicherstellung einer einheitlichen Anwendung dieser Verordnung;
- f) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes zur näheren Bestimmung der Kriterien und Bedingungen für die auf Profiling beruhenden Entscheidungen gemäß Artikel 22 Absatz 2;
- g) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes für die Feststellung von Verletzungen des Schutzes personenbezogener Daten und die Festlegung der Unverzüglichkeit im Sinne des Artikels 33 Absätze 1 und 2, und zu den spezifischen Umständen, unter denen der Verantwortliche oder der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten zu melden hat;
- h) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes zu den Umständen, unter denen eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen im Sinne des Artikels 34 Absatz 1 zur Folge hat;
- i) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes zur näheren Bestimmung der in Artikel 47 aufgeführten Kriterien und Anforderungen für die Übermittlungen personenbezogener Daten, die auf verbindlichen internen Datenschutzvorschriften von Verantwortlichen oder Auftragsverarbeitern beruhen, und der dort aufgeführten weiteren erforderlichen Anforderungen zum Schutz personenbezogener Daten der betroffenen Personen;
- j) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes zur näheren Bestimmung der Kriterien und Bedingungen für die Übermittlungen personenbezogener Daten gemäß Artikel 49 Absatz 1;
- k) Ausarbeitung von Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Artikel 58 Absätze 1, 2 und 3 und die Festsetzung von Geldbußen gemäß Artikel 83;
- l) Überprüfung der praktischen Anwendung der unter den Buchstaben e und f genannten Leitlinien, Empfehlungen und bewährten Verfahren;
- m) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes zur Festlegung gemeinsamer Verfahren für die von natürlichen Personen vorgenommene Meldung von Verstößen gegen diese Verordnung gemäß Artikel 54 Absatz 2;
- n) Förderung der Ausarbeitung von Verhaltensregeln und der Einrichtung von datenschutzspezifischen Zertifizierungsverfahren sowie Datenschutzsiegeln und -prüfzeichen gemäß den Artikeln 40 und 42;
- o) Akkreditierung von Zertifizierungsstellen und deren regelmäßige Überprüfung gemäß Artikel 43 und Führung eines öffentlichen Registers der akkreditierten Einrichtungen gemäß Artikel 43 Absatz 6 und der in Drittländern niedergelassenen akkreditierten Verantwortlichen oder Auftragsverarbeiter gemäß Artikel 42 Absatz 7;
- p) Präzisierung der in Artikel 43 Absatz 3 genannten Anforderungen im Hinblick auf die Akkreditierung von Zertifizierungsstellen gemäß Artikel 42;
- q) Abgabe einer Stellungnahme für die Kommission zu den Zertifizierungsanforderungen gemäß Artikel 43 Absatz 8;
- r) Abgabe einer Stellungnahme für die Kommission zu den Bildsymbolen gemäß Artikel 12 Absatz 7;
- s) Abgabe einer Stellungnahme für die Kommission zur Beurteilung der Angemessenheit des in einem Drittland oder einer internationalen Organisation gebotenen Schutzniveaus einschließlich zur Beurteilung der Frage, ob das Drittland, das Gebiet, ein oder mehrere spezifische Sektoren in diesem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau mehr gewährleistet. Zu diesem Zweck gibt die Kommission dem Ausschuss alle erforderlichen Unterlagen, darunter den Schriftwechsel mit der Regierung des Drittlands, dem Gebiet oder spezifischen Sektor oder der internationalen Organisation;

- t) Abgabe von Stellungnahmen im Kohärenzverfahren gemäß Artikel 64 Absatz 1 zu Beschlussentwürfen von Aufsichtsbehörden, zu Angelegenheiten, die nach Artikel 64 Absatz 2 vorgelegt wurden und um Erlass verbindlicher Beschlüsse gemäß Artikel 65, einschließlich der in Artikel 66 genannten Fälle;
 - u) Förderung der Zusammenarbeit und eines wirksamen bilateralen und multilateralen Austauschs von Informationen und bewährten Verfahren zwischen den Aufsichtsbehörden;
 - v) Förderung von Schulungsprogrammen und Erleichterung des Personalaustausches zwischen Aufsichtsbehörden sowie gegebenenfalls mit Aufsichtsbehörden von Drittländern oder mit internationalen Organisationen;
 - w) Förderung des Austausches von Fachwissen und von Dokumentationen über Datenschutzvorschriften und -praxis mit Datenschutzaufsichtsbehörden in aller Welt;
 - x) Abgabe von Stellungnahmen zu den auf Unionsebene erarbeiteten Verhaltensregeln gemäß Artikel 40 Absatz 9 und
 - y) Führung eines öffentlich zugänglichen elektronischen Registers der Beschlüsse der Aufsichtsbehörden und Gerichte in Bezug auf Fragen, die im Rahmen des Kohärenzverfahrens behandelt wurden.
- (2) Die Kommission kann, wenn sie den Ausschuss um Rat ersucht, unter Berücksichtigung der Dringlichkeit des Sachverhalts eine Frist angeben.
- (3) Der Ausschuss leitet seine Stellungnahmen, Leitlinien, Empfehlungen und bewährten Verfahren an die Kommission und an den in Artikel 93 genannten Ausschuss weiter und veröffentlicht sie.
- (4) Der Ausschuss konsultiert gegebenenfalls interessierte Kreise und gibt ihnen Gelegenheit, innerhalb einer angemessenen Frist Stellung zu nehmen. Unbeschadet des Artikels 76 macht der Ausschuss die Ergebnisse der Konsultation der Öffentlichkeit zugänglich.

Artikel 71

Berichterstattung

- (1) Der Ausschuss erstellt einen Jahresbericht über den Schutz natürlicher Personen bei der Verarbeitung in der Union und gegebenenfalls in Drittländern und internationalen Organisationen. Der Bericht wird veröffentlicht und dem Europäischen Parlament, dem Rat und der Kommission übermittelt.
- (2) Der Jahresbericht enthält eine Überprüfung der praktischen Anwendung der in Artikel 70 Absatz 1 Buchstabe l genannten Leitlinien, Empfehlungen und bewährten Verfahren sowie der in Artikel 65 genannten verbindlichen Beschlüsse.

Artikel 72

Verfahrensweise

- (1) Sofern in dieser Verordnung nichts anderes bestimmt ist, fasst der Ausschuss seine Beschlüsse mit einfacher Mehrheit seiner Mitglieder.
- (2) Der Ausschuss gibt sich mit einer Mehrheit von zwei Dritteln seiner Mitglieder eine Geschäftsordnung und legt seine Arbeitsweise fest.

Artikel 73

Vorsitz

- (1) Der Ausschuss wählt aus dem Kreis seiner Mitglieder mit einfacher Mehrheit einen Vorsitzenden und zwei stellvertretende Vorsitzende.
- (2) Die Amtszeit des Vorsitzenden und seiner beiden Stellvertreter beträgt fünf Jahre; ihre einmalige Wiederwahl ist zulässig.

*Artikel 74***Aufgaben des Vorsitzes**

- (1) Der Vorsitz hat folgende Aufgaben:
- a) Einberufung der Sitzungen des Ausschusses und Erstellung der Tagesordnungen,
 - b) Übermittlung der Beschlüsse des Ausschusses nach Artikel 65 an die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden,
 - c) Sicherstellung einer rechtzeitigen Ausführung der Aufgaben des Ausschusses, insbesondere der Aufgaben im Zusammenhang mit dem Kohärenzverfahren nach Artikel 63.
- (2) Der Ausschuss legt die Aufteilung der Aufgaben zwischen dem Vorsitzenden und dessen Stellvertretern in seiner Geschäftsordnung fest.

*Artikel 75***Sekretariat**

- (1) Der Ausschuss wird von einem Sekretariat unterstützt, das von dem Europäischen Datenschutzbeauftragten bereitgestellt wird.
- (2) Das Sekretariat führt seine Aufgaben ausschließlich auf Anweisung des Vorsitzes des Ausschusses aus.
- (3) Das Personal des Europäischen Datenschutzbeauftragten, das an der Wahrnehmung der dem Ausschuss gemäß dieser Verordnung übertragenen Aufgaben beteiligt ist, unterliegt anderen Berichtspflichten als das Personal, das an der Wahrnehmung der dem Europäischen Datenschutzbeauftragten übertragenen Aufgaben beteiligt ist.
- (4) Soweit angebracht, erstellen und veröffentlichen der Ausschuss und der Europäische Datenschutzbeauftragte eine Vereinbarung zur Anwendung des vorliegenden Artikels, in der die Bedingungen ihrer Zusammenarbeit festgelegt sind und die für das Personal des Europäischen Datenschutzbeauftragten gilt, das an der Wahrnehmung der dem Ausschuss gemäß dieser Verordnung übertragenen Aufgaben beteiligt ist.
- (5) Das Sekretariat leistet dem Ausschuss analytische, administrative und logistische Unterstützung.
- (6) Das Sekretariat ist insbesondere verantwortlich für
- a) das Tagesgeschäft des Ausschusses,
 - b) die Kommunikation zwischen den Mitgliedern des Ausschusses, seinem Vorsitz und der Kommission,
 - c) die Kommunikation mit anderen Organen und mit der Öffentlichkeit,
 - d) den Rückgriff auf elektronische Mittel für die interne und die externe Kommunikation,
 - e) die Übersetzung sachdienlicher Informationen,
 - f) die Vor- und Nachbereitung der Sitzungen des Ausschusses,
 - g) die Vorbereitung, Abfassung und Veröffentlichung von Stellungnahmen, von Beschlüssen über die Beilegung von Streitigkeiten zwischen Aufsichtsbehörden und von sonstigen vom Ausschuss angenommenen Dokumenten.

*Artikel 76***Vertraulichkeit**

- (1) Die Beratungen des Ausschusses sind gemäß seiner Geschäftsordnung vertraulich, wenn der Ausschuss dies für erforderlich hält.

(2) Der Zugang zu Dokumenten, die Mitgliedern des Ausschusses, Sachverständigen und Vertretern von Dritten vorgelegt werden, wird durch die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates ⁽¹⁾ geregelt.

KAPITEL VIII

Rechtsbehelfe, Haftung und Sanktionen

Artikel 77

Recht auf Beschwerde bei einer Aufsichtsbehörde

(1) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.

(2) Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 78.

Artikel 78

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde

(1) Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde.

(2) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die nach den Artikeln 55 und 56 zuständige Aufsichtsbehörde sich nicht mit einer Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Artikel 77 erhobenen Beschwerde in Kenntnis gesetzt hat.

(3) Für Verfahren gegen eine Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.

(4) Kommt es zu einem Verfahren gegen den Beschluss einer Aufsichtsbehörde, dem eine Stellungnahme oder ein Beschluss des Ausschusses im Rahmen des Kohärenzverfahrens vorangegangen ist, so leitet die Aufsichtsbehörde diese Stellungnahme oder diesen Beschluss dem Gericht zu.

Artikel 79

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter

(1) Jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 77 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

(2) Für Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

⁽¹⁾ Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. L 145 vom 31.5.2001, S. 43).

*Artikel 80***Vertretung von betroffenen Personen**

(1) Die betroffene Person hat das Recht, eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen, in ihrem Namen die in den Artikeln 77, 78 und 79 genannten Rechte wahrzunehmen und das Recht auf Schadenersatz gemäß Artikel 82 in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist.

(2) Die Mitgliedstaaten können vorsehen, dass jede der in Absatz 1 des vorliegenden Artikels genannten Einrichtungen, Organisationen oder Vereinigungen unabhängig von einem Auftrag der betroffenen Person in diesem Mitgliedstaat das Recht hat, bei der gemäß Artikel 77 zuständigen Aufsichtsbehörde eine Beschwerde einzulegen und die in den Artikeln 78 und 79 aufgeführten Rechte in Anspruch zu nehmen, wenn ihres Erachtens die Rechte einer betroffenen Person gemäß dieser Verordnung infolge einer Verarbeitung verletzt worden sind.

*Artikel 81***Aussetzung des Verfahrens**

(1) Erhält ein zuständiges Gericht in einem Mitgliedstaat Kenntnis von einem Verfahren zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter, das vor einem Gericht in einem anderen Mitgliedstaat anhängig ist, so nimmt es mit diesem Gericht Kontakt auf, um sich zu vergewissern, dass ein solches Verfahren existiert.

(2) Ist ein Verfahren zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter vor einem Gericht in einem anderen Mitgliedstaat anhängig, so kann jedes später angerufene zuständige Gericht das bei ihm anhängige Verfahren aussetzen.

(3) Sind diese Verfahren in erster Instanz anhängig, so kann sich jedes später angerufene Gericht auf Antrag einer Partei auch für unzuständig erklären, wenn das zuerst angerufene Gericht für die betreffenden Klagen zuständig ist und die Verbindung der Klagen nach seinem Recht zulässig ist.

*Artikel 82***Haftung und Recht auf Schadenersatz**

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

(4) Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadenersatz für die betroffene Person sichergestellt ist.

(5) Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(6) Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.

Artikel 83

Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

- a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
- b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
- c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
- d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
- e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
- f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuweichen und seine möglichen nachteiligen Auswirkungen zu mindern;
- g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
- h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
- i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
- j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und
- k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

- a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;
- b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;
- c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

- a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;
- b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
- c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;
- d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;
- e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

(7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

(8) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

(9) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

Artikel 84

Sanktionen

(1) Die Mitgliedstaaten legen die Vorschriften über andere Sanktionen für Verstöße gegen diese Verordnung — insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 unterliegen — fest und treffen alle zu deren Anwendung erforderlichen Maßnahmen. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

(2) Jeder Mitgliedstaat teilt der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften, die er aufgrund von Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

KAPITEL IX

Vorschriften für besondere Verarbeitungssituationen

Artikel 85

Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit

(1) Die Mitgliedstaaten bringen durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang.

(2) Für die Verarbeitung, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, sehen die Mitgliedstaaten Abweichungen oder Ausnahmen von Kapitel II (Grundsätze), Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) vor, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.

(3) Jeder Mitgliedstaat teilt der Kommission die Rechtsvorschriften, die er aufgrund von Absatz 2 erlassen hat, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften mit.

Artikel 86

Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten

Personenbezogene Daten in amtlichen Dokumenten, die sich im Besitz einer Behörde oder einer öffentlichen Einrichtung oder einer privaten Einrichtung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe befinden, können von der Behörde oder der Einrichtung gemäß dem Unionsrecht oder dem Recht des Mitgliedstaats, dem die Behörde oder Einrichtung unterliegt, offengelegt werden, um den Zugang der Öffentlichkeit zu amtlichen Dokumenten mit dem Recht auf Schutz personenbezogener Daten gemäß dieser Verordnung in Einklang zu bringen.

Artikel 87

Verarbeitung der nationalen Kennziffer

Die Mitgliedstaaten können näher bestimmen, unter welchen spezifischen Bedingungen eine nationale Kennziffer oder andere Kennzeichen von allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen. In diesem Fall darf die nationale Kennziffer oder das andere Kennzeichen von allgemeiner Bedeutung nur unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung verwendet werden.

Artikel 88

Datenverarbeitung im Beschäftigungskontext

(1) Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarung en festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen.

(2) Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.

(3) Jeder Mitgliedstaat teilt der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften, die er aufgrund von Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

Artikel 89

Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

(1) Die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken unterliegt geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung. Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung

gewährleistet wird. Zu diesen Maßnahmen kann die Pseudonymisierung gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen. In allen Fällen, in denen diese Zwecke durch die Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, werden diese Zwecke auf diese Weise erfüllt.

(2) Werden personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet, können vorbehaltlich der Bedingungen und Garantien gemäß Absatz 1 des vorliegenden Artikels im Unionsrecht oder im Recht der Mitgliedstaaten insoweit Ausnahmen von den Rechten gemäß der Artikel 15, 16, 18 und 21 vorgesehen werden, als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.

(3) Werden personenbezogene Daten für im öffentlichen Interesse liegende Archivzwecke verarbeitet, können vorbehaltlich der Bedingungen und Garantien gemäß Absatz 1 des vorliegenden Artikels im Unionsrecht oder im Recht der Mitgliedstaaten insoweit Ausnahmen von den Rechten gemäß der Artikel 15, 16, 18, 19, 20 und 21 vorgesehen werden, als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.

(4) Dient die in den Absätzen 2 und 3 genannte Verarbeitung gleichzeitig einem anderen Zweck, gelten die Ausnahmen nur für die Verarbeitung zu den in diesen Absätzen genannten Zwecken.

Artikel 90

Geheimhaltungspflichten

(1) Die Mitgliedstaaten können die Befugnisse der Aufsichtsbehörden im Sinne des Artikels 58 Absatz 1 Buchstaben e und f gegenüber den Verantwortlichen oder den Auftragsverarbeitern, die nach Unionsrecht oder dem Recht der Mitgliedstaaten oder nach einer von den zuständigen nationalen Stellen erlassenen Verpflichtung dem Berufsgeheimnis oder einer gleichwertigen Geheimhaltungspflicht unterliegen, regeln, soweit dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen. Diese Vorschriften gelten nur in Bezug auf personenbezogene Daten, die der Verantwortliche oder der Auftragsverarbeiter bei einer Tätigkeit erlangt oder erhoben hat, die einer solchen Geheimhaltungspflicht unterliegt.

(2) Jeder Mitgliedstaat teilt der Kommission bis zum 25. Mai 2018 die Vorschriften mit, die er aufgrund von Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.

Artikel 91

Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften

(1) Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.

(2) Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 umfassende Datenschutzregeln anwenden, unterliegen der Aufsicht durch eine unabhängige Aufsichtsbehörde, die spezifischer Art sein kann, sofern sie die in Kapitel VI niedergelegten Bedingungen erfüllt.

KAPITEL X

Delegierte Rechtsakte und Durchführungsrechtsakte

Artikel 92

Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 12 Absatz 8 und Artikel 43 Absatz 8 wird der Kommission auf unbestimmte Zeit ab dem 24. Mai 2016 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 12 Absatz 8 und Artikel 43 Absatz 8 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(5) Ein delegierter Rechtsakt, der gemäß Artikel 12 Absatz 8 und Artikel 43 Absatz 8 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von drei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Veranlassung des Europäischen Parlaments oder des Rates wird diese Frist um drei Monate verlängert.

Artikel 93

Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

(3) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 8 der Verordnung (EU) Nr. 182/2011 in Verbindung mit deren Artikel 5.

KAPITEL XI

Schlussbestimmungen

Artikel 94

Aufhebung der Richtlinie 95/46/EG

(1) Die Richtlinie 95/46/EG wird mit Wirkung vom 25. Mai 2018 aufgehoben.

(2) Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser Verordnung errichteten Europäischen Datenschutzausschuss.

Artikel 95

Verhältnis zur Richtlinie 2002/58/EG

Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

*Artikel 96***Verhältnis zu bereits geschlossenen Übereinkünften**

Internationale Übereinkünfte, die die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen mit sich bringen, die von den Mitgliedstaaten vor dem 24. Mai 2016 abgeschlossen wurden und die im Einklang mit dem vor diesem Tag geltenden Unionsrecht stehen, bleiben in Kraft, bis sie geändert, ersetzt oder gekündigt werden.

*Artikel 97***Berichte der Kommission**

- (1) Bis zum 25. Mai 2020 und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Verordnung vor. Die Berichte werden öffentlich gemacht.
- (2) Im Rahmen der Bewertungen und Überprüfungen nach Absatz 1 prüft die Kommission insbesondere die Anwendung und die Wirkungsweise
 - a) des Kapitels V über die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen insbesondere im Hinblick auf die gemäß Artikel 45 Absatz 3 der vorliegenden Verordnung erlassenen Beschlüsse sowie die gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassenen Feststellungen,
 - b) des Kapitels VII über Zusammenarbeit und Kohärenz.
- (3) Für den in Absatz 1 genannten Zweck kann die Kommission Informationen von den Mitgliedstaaten und den Aufsichtsbehörden anfordern.
- (4) Bei den in den Absätzen 1 und 2 genannten Bewertungen und Überprüfungen berücksichtigt die Kommission die Standpunkte und Feststellungen des Europäischen Parlaments, des Rates und anderer einschlägiger Stellen oder Quellen.
- (5) Die Kommission legt erforderlichenfalls geeignete Vorschläge zur Änderung dieser Verordnung vor und berücksichtigt dabei insbesondere die Entwicklungen in der Informationstechnologie und die Fortschritte in der Informationsgesellschaft.

*Artikel 98***Überprüfung anderer Rechtsakte der Union zum Datenschutz**

Die Kommission legt gegebenenfalls Gesetzgebungsvorschläge zur Änderung anderer Rechtsakte der Union zum Schutz personenbezogener Daten vor, damit ein einheitlicher und kohärenter Schutz natürlicher Personen bei der Verarbeitung sichergestellt wird. Dies betrifft insbesondere die Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung solcher Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union und zum freien Verkehr solcher Daten.

*Artikel 99***Inkrafttreten und Anwendung**

- (1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.
- (2) Sie gilt ab dem 25. Mai 2018.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am 27. April 2016.

Im Namen des Europäischen Parlaments

Der Präsident

M. SCHULZ

Im Namen des Rates

Die Präsidentin

J.A. HENNIS-PLASSCHAERT

<https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597>

Gesamte Rechtsvorschrift für Datenschutzgesetz, Fassung vom 13.02.2019

Langtitel

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSGVO)

StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.)
[CELEX-Nr.: 395L0046]

Änderung

BGBl. I Nr. 136/2001 (NR: GP XXI RV 742 AB 824 S. 81. BR: 6458 AB 6459 S. 681.)
BGBl. I Nr. 13/2005 (NR: GP XXII IA 515/A AB 821 S. 96. BR: AB 7228 S. 719.)
BGBl. I Nr. 2/2008 (1. BVRBG) (NR: GP XXIII RV 314 AB 370 S. 41. BR: 7799 AB 7830 S. 751.)
BGBl. I Nr. 133/2009 (NR: GP XXIV RV 472 AB 531 S. 49. BR: 8220 AB 8225 S. 780.)
BGBl. I Nr. 135/2009 (NR: GP XXIV RV 485 AB 558 S. 49. BR: 8217 AB 8228 S. 780.)
BGBl. I Nr. 112/2011 (NR: GP XXIV RV 1494 AB 1500 S. 130. BR: 8602 AB 8603 S. 802.)
[CELEX-Nr.: 32009L0133, 32010L0024]
BGBl. I Nr. 51/2012 (NR: GP XXIV RV 1618 AB 1771 S. 155. BR: 8730 AB 8731 S. 809.)
BGBl. I Nr. 57/2013 (NR: GP XXIV RV 2131 AB 2245 S. 194. BR: AB 8940 S. 819.)
BGBl. I Nr. 83/2013 (NR: GP XXIV RV 2168 AB 2268 S. 200. BR: AB 8968 S. 820.)
[CELEX-Nr.: 31995L0046]
BGBl. I Nr. 132/2015 (VfGH)
BGBl. I Nr. 120/2017 (NR: GP XXV RV 1664 AB 1761 S. 190. BR: 9824 AB 9856 S. 871.)
[CELEX-Nr.: 32016L0680]
BGBl. I Nr. 23/2018 (NR: GP XXVI IA 188/A AB 99 S. 21. BR: AB 9958 S. 879.)
BGBl. I Nr. 24/2018 (NR: GP XXVI IA 189/A AB 98 S. 21. BR: AB 9948 S. 879.)
BGBl. I Nr. 14/2019 (NR: GP XXVI RV 301 AB 463 S. 57. BR: AB 10104 S. 888.)

Präambel/Promulgationsklausel

Inhaltsverzeichnis

Artikel 1

(Verfassungsbestimmung)

- § 1 Grundrecht auf Datenschutz
- § 2 Zuständigkeit
- § 3 Räumlicher Anwendungsbereich

Artikel 2

1. Hauptstück

Durchführung der Datenschutz-Grundverordnung und ergänzende Regelungen

1. Abschnitt

Allgemeine Bestimmungen

- § 4. Anwendungsbereich und Durchführungsbestimmung
- § 5. Datenschutzbeauftragter
- § 6. Datengeheimnis

2. Abschnitt

Datenverarbeitungen zu spezifischen Zwecken

- § 7. Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke
- § 8. Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen

- § 9. Freiheit der Meinungsäußerung und Informationsfreiheit
- § 10. Verarbeitung personenbezogener Daten im Katastrophenfall
- § 11. Verwarnung durch die Datenschutzbehörde

**3. Abschnitt
Bildverarbeitung**

- § 12. Zulässigkeit der Bildaufnahme
- § 13. Besondere Datensicherheitsmaßnahmen und Kennzeichnung

**2. Hauptstück
Organe**

**1. Abschnitt
Datenschutzrat**

- § 14. Einrichtung und Aufgaben
- § 15. Zusammensetzung
- § 16. Vorsitz und Geschäftsführung
- § 17. Sitzungen und Beschlussfassung

**2. Abschnitt
Datenschutzbehörde**

- § 18. Einrichtung
- § 19. Unabhängigkeit
- § 20. Leiter der Datenschutzbehörde
- § 21. Aufgaben
- § 22. Befugnisse
- § 23. Tätigkeitsbericht und Veröffentlichung von Entscheidungen

**3. Abschnitt
Rechtsbehelfe, Haftung und Sanktionen**

- § 24. Beschwerde an die Datenschutzbehörde
- § 25. Begleitende Maßnahmen im Beschwerdeverfahren
- § 26. Verantwortliche des öffentlichen und des privaten Bereichs
- § 27. Beschwerde an das Bundesverwaltungsgericht
- § 28. Vertretung von betroffenen Personen
- § 29. Haftung und Recht auf Schadenersatz
- § 30. Allgemeine Bedingungen für die Verhängung von Geldbußen

**4. Abschnitt
Aufsichtsbehörde nach der Richtlinie (EU) 2016/680**

- § 31. Datenschutzbehörde
- § 32. Aufgaben der Datenschutzbehörde
- § 33. Befugnisse der Datenschutzbehörde
- § 34. Allgemeine Bestimmungen

**5. Abschnitt
Besondere Befugnisse der Datenschutzbehörde**

- § 35.

3. Hauptstück

Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs

**1. Abschnitt
Allgemeine Bestimmungen**

- § 36. Anwendungsbereich und Begriffsbestimmungen
- § 37. Grundsätze für die Datenverarbeitung, Kategorisierung und Datenqualität
- § 38. Rechtmäßigkeit der Verarbeitung
- § 39. Verarbeitung besonderer Kategorien personenbezogener Daten
- § 40. Verarbeitung für andere Zwecke und Übermittlung
- § 41. Automatisierte Entscheidungsfindung im Einzelfall

**2. Abschnitt
Rechte der betroffenen Person**

- § 42. Grundsätze
- § 43. Information der betroffenen Person
- § 44. Auskunftsrecht der betroffenen Person
- § 45. Recht auf Berichtigung oder Löschung personenbezogener Daten und auf Einschränkung der Verarbeitung

**3. Abschnitt
Verantwortlicher und Auftragsverarbeiter**

- § 46. Pflichten des Verantwortlichen
- § 47. Gemeinsam Verantwortliche
- § 48. Auftragsverarbeiter und Aufsicht über die Verarbeitung
- § 49. Verzeichnis von Verarbeitungstätigkeiten
- § 50. Protokollierung
- § 51. Zusammenarbeit mit der Datenschutzbehörde
- § 52. Datenschutz-Folgenabschätzung
- § 53. Vorherige Konsultation der Datenschutzbehörde
- § 54. Datensicherheitsmaßnahmen
- § 55. Meldung von Verletzungen an die Datenschutzbehörde
- § 56. Benachrichtigung der betroffenen Person von Verletzungen
- § 57. Benennung, Stellung und Aufgaben des Datenschutzbeauftragten

**4. Abschnitt
Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen**

- § 58. Allgemeine Grundsätze für die Übermittlung personenbezogener Daten
- § 59. Datenübermittlung an Drittländer oder internationale Organisationen
- (Anm.: § 60. mit Ablauf des 15.1.2019 außer Kraft getreten (vgl. BGBl. I Nr. 14/2019)*
- § 61. aufgehoben durch BGBl. I Nr. 14/2019)*

**4. Hauptstück
Besondere Strafbestimmungen**

- § 62. Verwaltungsstrafbestimmung
- § 63. Datenverarbeitung in Gewinn- oder Schädigungsabsicht

**5. Hauptstück
Schlussbestimmungen**

- § 64. Durchführung und Umsetzung von Rechtsakten der EU
- § 65. Sprachliche Gleichbehandlung
- § 66. Erlassung von Verordnungen
- § 67. Verweisungen
- § 68. Vollziehung
- § 69. Übergangsbestimmungen
- § 70. Inkrafttreten

Text

**Artikel 1
(Verfassungsbestimmung)**

Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung

nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

(Anm.: Abs. 5 aufgehoben durch BGBl. I Nr. 51/2012)

Beachte für folgende Bestimmung

Verfassungsbestimmung

Zuständigkeit

§ 2. (1) Bundessache ist die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr.

(2) Die Vollziehung solcher Bundesgesetze steht dem Bund zu. Soweit solche Daten von einem Land, im Auftrag eines Landes, von oder im Auftrag von juristischen Personen, die durch Gesetz eingerichtet sind und deren Einrichtung hinsichtlich der Vollziehung in die Zuständigkeit der Länder fällt, verwendet werden, sind diese Bundesgesetze von den Ländern zu vollziehen, soweit nicht durch Bundesgesetz die Datenschutzbehörde, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden.

Beachte für folgende Bestimmung

Verfassungsbestimmung

Räumlicher Anwendungsbereich

§ 3. (1) Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von personenbezogenen Daten im Inland anzuwenden. Darüber hinaus ist dieses Bundesgesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung (§ 4 Z 15) eines Auftraggebers (§ 4 Z 4) geschieht.

(2) Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.

(3) Weiters ist dieses Bundesgesetz nicht anzuwenden, soweit personenbezogene Daten durch das Inland nur durchgeführt werden.

(4) Von den Abs. 1 bis 3 abweichende gesetzliche Regelungen sind nur in Angelegenheiten zulässig, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

Artikel 2

1. Hauptstück

Durchführung der Datenschutz-Grundverordnung und ergänzende Regelungen

1. Abschnitt

Allgemeine Bestimmungen

Anwendungsbereich und Durchführungsbestimmung

§ 4. (1) Die Bestimmungen der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1, (im Folgenden: DSGVO) und dieses Bundesgesetzes gelten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten natürlicher Personen sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten natürlicher Personen, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, soweit nicht die spezifischeren Bestimmungen des 3. Hauptstücks dieses Bundesgesetzes vorgehen.

(2) Kann die Berichtigung oder Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO bis zu diesem Zeitpunkt einzuschränken.

(3) Die Verarbeitung von personenbezogenen Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen ist unter Einhaltung der Vorgaben der DSGVO zulässig, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verarbeitung solcher Daten besteht oder
2. sich sonst die Zulässigkeit der Verarbeitung dieser Daten aus gesetzlichen Sorgfaltspflichten ergibt oder die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten gemäß Art. 6 Abs. 1 lit. f DSGVO erforderlich ist, und die Art und Weise, in der die Datenverarbeitung vorgenommen wird, die Wahrung der Interessen der betroffenen Person nach der DSGVO und diesem Bundesgesetz gewährleistet.

(4) Bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, ist die Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO zur Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das vierzehnte Lebensjahr vollendet hat.

(5) Das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO besteht gegenüber einem hoheitlich tätigen Verantwortlichen unbeschadet anderer gesetzlicher Beschränkungen dann nicht, wenn durch die Erteilung dieser Auskunft die Erfüllung einer dem Verantwortlichen gesetzlich übertragenen Aufgabe gefährdet wird.

(6) Das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO besteht gegenüber einem Verantwortlichen unbeschadet anderer gesetzlicher Beschränkungen in der Regel dann nicht, wenn durch die Erteilung dieser Auskunft ein Geschäfts- oder Betriebsgeheimnis des Verantwortlichen bzw. Dritter gefährdet würde.

(7) Soweit manuell, dh. nichtautomatisiert geführte Dateisysteme für Zwecke solcher Angelegenheiten bestehen, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist, gelten sie als Datenverarbeitungen im Sinne der DSGVO und dieses Bundesgesetzes.

Datenschutzbeauftragter

§ 5. (1) Der Datenschutzbeauftragte und die für ihn tätigen Personen sind unbeschadet sonstiger Verschwiegenheitspflichten bei der Erfüllung der Aufgaben zur Geheimhaltung verpflichtet. Dies gilt insbesondere in Bezug auf die Identität betroffener Personen, die sich an den Datenschutzbeauftragten gewandt haben, sowie über Umstände, die Rückschlüsse auf diese Personen zulassen, es sei denn, es erfolgte eine ausdrückliche Entbindung von der Verschwiegenheit durch die betroffene Person. Der Datenschutzbeauftragte und die für ihn tätigen Personen dürfen die zugänglich gemachten Informationen ausschließlich für die Erfüllung der Aufgaben verwenden und sind auch nach Ende ihrer Tätigkeit zur Geheimhaltung verpflichtet.

(2) Erhält ein Datenschutzbeauftragter bei seiner Tätigkeit Kenntnis von Daten, für die einer der Kontrolle des Datenschutzbeauftragten unterliegenden Stelle beschäftigten Person ein gesetzliches Aussageverweigerungsrecht zusteht, steht dieses Recht auch dem Datenschutzbeauftragten und den für ihn tätigen Personen insoweit zu, als die Person, der das gesetzliche Aussageverweigerungsrecht zusteht, davon Gebrauch gemacht hat. Im Umfang des Aussageverweigerungsrechts des Datenschutzbeauftragten unterliegen seine Akten und andere Schriftstücke einem Sicherstellungs- und Beschlagnahmeverbot.

(3) Der Datenschutzbeauftragte im öffentlichen Bereich (in Formen des öffentlichen Rechts eingerichtet, insbesondere auch als Organ einer Gebietskörperschaft) ist bezüglich der Ausübung seiner Aufgaben weisungsfrei. Das oberste Organ hat das Recht, sich über die Gegenstände der Geschäftsführung beim Datenschutzbeauftragten im öffentlichen Bereich zu unterrichten. Dem ist vom Datenschutzbeauftragten nur insoweit zu entsprechen, als dies nicht der Unabhängigkeit des Datenschutzbeauftragten im Sinne von Art. 38 Abs. 3 DSGVO widerspricht.

(4) Im Wirkungsbereich jedes Bundesministeriums sind unter Bedachtnahme auf Art und Umfang der Datenverarbeitungen sowie je nach Einrichtung des Bundesministeriums ein oder mehrere Datenschutzbeauftragte vorzusehen. Diese müssen dem jeweiligen Bundesministerium oder der jeweiligen nachgeordneten Dienststelle oder sonstigen Einrichtung angehören.

(5) Die Datenschutzbeauftragten im öffentlichen Bereich gemäß Abs. 4 pflegen einen regelmäßigen Erfahrungsaustausch, insbesondere im Hinblick auf die Gewährleistung eines einheitlichen Datenschutzstandards.

Datengeheimnis

§ 6. (1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

2. Abschnitt

Datenverarbeitungen zu spezifischen Zwecken

Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke

§ 7. (1) Für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Verantwortliche alle personenbezogenen Daten verarbeiten, die

1. öffentlich zugänglich sind,
2. er für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für ihn pseudonymisierte personenbezogene Daten sind und der Verantwortliche die Identität der betroffenen Person mit rechtlich zulässigen Mitteln nicht bestimmen kann.

(2) Bei Datenverarbeitungen für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke, die nicht unter Abs. 1 fallen, dürfen personenbezogene Daten nur

1. gemäß besonderen gesetzlichen Vorschriften,
2. mit Einwilligung der betroffenen Person oder
3. mit Genehmigung der Datenschutzbehörde gemäß Abs. 3

verarbeitet werden.

(3) Eine Genehmigung der Datenschutzbehörde für die Verarbeitung von personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke ist auf Antrag des Verantwortlichen der Untersuchung zu erteilen, wenn

1. die Einholung der Einwilligung der betroffenen Person mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet,
2. ein öffentliches Interesse an der beantragten Verarbeitung besteht und
3. die fachliche Eignung des Verantwortlichen glaubhaft gemacht wird.

Sollen besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) ermittelt werden, muss ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muss gewährleistet sein, dass die personenbezogenen Daten beim Verantwortlichen der Untersuchung nur von Personen verarbeitet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist. Die Datenschutzbehörde hat die Genehmigung an die Erfüllung von Bedingungen und Auflagen zu knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der betroffenen Person notwendig ist.

(4) Einem Antrag nach Abs. 3 ist jedenfalls eine vom Verfügungsbefugten über die Datenbestände, aus denen die personenbezogenen Daten ermittelt werden sollen, unterfertigte Erklärung anzuschließen, dass er dem Verantwortlichen die Datenbestände für die Untersuchung zur Verfügung stellt. Anstelle dieser Erklärung kann auch ein diese Erklärung ersetzender Exekutionstitel (§ 367 Abs. 1 der Exekutionsordnung – EO, RGBl. Nr. 79/1896) vorgelegt werden.

(5) Auch in jenen Fällen, in welchen die Verarbeitung von personenbezogenen Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der Personenbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit personenbezogenen Daten gemäß Abs. 1 Z 3 das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, ist der Personenbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

(6) Rechtliche Beschränkungen der Zulässigkeit der Benützung von personenbezogenen Daten aus anderen, insbesondere urheberrechtlichen Gründen, bleiben unberührt.

Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen

§ 8. (1) Soweit gesetzlich nicht ausdrücklich anderes bestimmt ist, bedarf die Übermittlung von Adressdaten eines bestimmten Kreises von betroffenen Personen zum Zweck ihrer Benachrichtigung oder Befragung der Einwilligung der betroffenen Personen.

(2) Wenn allerdings eine Beeinträchtigung der Geheimhaltungsinteressen der betroffenen Personen angesichts der Auswahlkriterien für den Betroffenenkreis und des Gegenstands der Benachrichtigung oder Befragung unwahrscheinlich ist, bedarf es keiner Einwilligung, wenn

1. Daten desselben Verantwortlichen verarbeitet werden oder
2. bei einer beabsichtigten Übermittlung der Adressdaten an Dritte
 - a) an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht oder
 - b) keiner der betroffenen Personen nach entsprechender Information über Anlass und Inhalt der Übermittlung innerhalb angemessener Frist Widerspruch gegen die Übermittlung erhoben hat.

(3) Liegen die Voraussetzungen des Abs. 2 nicht vor und würde die Einholung der Einwilligung der betroffenen Personen gemäß Abs. 1 einen unverhältnismäßigen Aufwand erfordern, ist die Übermittlung der Adressdaten mit Genehmigung der Datenschutzbehörde gemäß Abs. 4 zulässig, falls die Übermittlung an Dritte

1. zum Zweck der Benachrichtigung oder Befragung aus einem wichtigen Interesse des Betroffenen selbst,

2. aus einem wichtigen öffentlichen Benachrichtigungs- oder Befragungsinteresse oder
3. zur Befragung der betroffenen Personen für wissenschaftliche oder statistische Zwecke erfolgen soll.

(4) Die Datenschutzbehörde hat auf Antrag eines Verantwortlichen, der Adressdaten verarbeitet, die Genehmigung zur Übermittlung zu erteilen, wenn der Antragsteller das Vorliegen der in Abs. 3 genannten Voraussetzungen glaubhaft macht und überwiegende schutzwürdige Geheimhaltungsinteressen der betroffenen Personen der Übermittlung nicht entgegenstehen. Die Datenschutzbehörde hat die Genehmigung an die Erfüllung von Bedingungen und Auflagen zu knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der betroffenen Personen notwendig ist.

(5) Die übermittelten Adressdaten dürfen ausschließlich für den genehmigten Zweck verarbeitet werden und sind zu löschen, sobald sie für die Benachrichtigung oder Befragung nicht mehr benötigt werden.

(6) Sofern es gemäß den vorstehenden Bestimmungen zulässig ist, Namen und Adresse von Personen, die einem bestimmten Betroffenenkreis angehören, zu übermitteln, dürfen auch die zum Zweck der Auswahl der zu übermittelnden Adressdaten notwendigen Verarbeitungen vorgenommen werden.

Freiheit der Meinungsäußerung und Informationsfreiheit

§ 9. (1) Auf die Verarbeitung von personenbezogenen Daten durch Medieninhaber, Herausgeber, Medienmitarbeiter und Arbeitnehmer eines Medienunternehmens oder Mediendienstes im Sinne des Mediengesetzes – MedienG, BGBl. Nr. 314/1981, zu journalistischen Zwecken des Medienunternehmens oder Mediendienstes finden die Bestimmungen dieses Bundesgesetzes sowie von der DSGVO die Kapitel II (Grundsätze), III (Rechte der betroffenen Person), IV (Verantwortlicher und Auftragsverarbeiter), V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), VI (Unabhängige Aufsichtsbehörden), VII (Zusammenarbeit und Kohärenz) und IX (Vorschriften für besondere Verarbeitungssituationen) keine Anwendung. Die Datenschutzbehörde hat bei Ausübung ihrer Befugnisse gegenüber den im ersten Satz genannten Personen den Schutz des Redaktionsgeheimnisses (§ 31 MedienG) zu beachten.

(2) Soweit dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen, finden von der DSGVO die Kapitel II (Grundsätze), mit Ausnahme des Art. 5, Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), mit Ausnahme der Art. 28, 29 und 32, Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) auf die Verarbeitung, die zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, keine Anwendung. Von den Bestimmungen dieses Bundesgesetzes ist in solchen Fällen § 6 (Datengeheimnis) anzuwenden.

Verarbeitung personenbezogener Daten im Katastrophenfall

§ 10. (1) Verantwortliche des öffentlichen Bereichs und Hilfsorganisationen sind im Katastrophenfall ermächtigt, personenbezogene Daten gemeinsam zu verarbeiten, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig ist.

(2) Wer rechtmäßig über personenbezogene Daten verfügt, darf diese an Verantwortliche des öffentlichen Bereichs und Hilfsorganisationen übermitteln, sofern diese die personenbezogenen Daten zur Bewältigung der Katastrophe für die in Abs. 1 genannten Zwecke benötigen.

(3) Eine Übermittlung von personenbezogenen Daten in das Ausland ist zulässig, soweit dies für die Erfüllung der in Abs. 1 genannten Zwecke unbedingt notwendig ist. Daten, die für sich allein die betroffene Person strafrechtlich belasten, dürfen nicht übermittelt werden, es sei denn, dass diese zur Identifizierung im Einzelfall unbedingt notwendig sind. Die Datenschutzbehörde ist von den veranlassten Übermittlungen und den näheren Umständen des Anlass gebenden Sachverhaltes unverzüglich zu verständigen. Die Datenschutzbehörde hat zum Schutz der Betroffenenrechte weitere Datenübermittlungen zu untersagen, wenn der durch die Datenweitergabe bewirkte Eingriff in das Grundrecht auf Datenschutz durch die besonderen Umstände der Katastrophensituation nicht gerechtfertigt ist.

(4) Auf Grund einer konkreten Anfrage eines nahen Angehörigen einer tatsächlich oder vermutlich von der Katastrophe unmittelbar betroffenen Person sind Verantwortliche ermächtigt, dem Anfragenden personenbezogene Daten zum Aufenthalt der betroffenen Person und dem Stand der Ausforschung zu übermitteln, wenn der Angehörige seine Identität und das Naheverhältnis glaubhaft darlegt. Besondere

Kategorien personenbezogener Daten (Art. 9 DSGVO) dürfen an nahe Angehörige nur übermittelt werden, wenn sie ihre Identität und ihre Angehörigeneigenschaft nachweisen und die Übermittlung zur Wahrung ihrer Rechte oder jener der betroffenen Person erforderlich ist. Die Sozialversicherungsträger und Behörden sind verpflichtet, die Verantwortlichen des öffentlichen Bereichs und Hilfsorganisationen zu unterstützen, soweit dies zur Überprüfung der Angaben des Anfragenden erforderlich ist.

(5) Als nahe Angehörige im Sinne dieser Bestimmung sind Eltern, Kinder, Ehegatten, eingetragene Partner und Lebensgefährten der betroffenen Personen zu verstehen. Andere Angehörige dürfen die erwähnten Auskünfte unter denselben Voraussetzungen wie nahe Angehörige dann erhalten, wenn sie eine besondere Nahebeziehung zu der von der Katastrophe tatsächlich oder vermutlich unmittelbar betroffenen Person glaubhaft machen.

(6) Die zu Zwecken der Bewältigung des Katastrophenfalles verarbeiteten personenbezogenen Daten sind unverzüglich zu löschen, wenn sie für die Erfüllung des konkreten Zwecks nicht mehr benötigt werden.

Verwarnung durch die Datenschutzbehörde

§ 11. Die Datenschutzbehörde wird den Katalog des Art. 83 Abs. 2 bis 6 DSGVO so zur Anwendung bringen, dass die Verhältnismäßigkeit gewahrt wird. Insbesondere bei erstmaligen Verstößen wird die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen.

3. Abschnitt Bildverarbeitung

Zulässigkeit der Bildaufnahme

§ 12. (1) Eine Bildaufnahme im Sinne dieses Abschnittes bezeichnet die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken. Zur Bildaufnahme gehören auch dabei mitverarbeitete akustische Informationen. Für eine derartige Bildaufnahme gilt dieser Abschnitt, soweit nicht durch andere Gesetze Besonderes bestimmt ist.

- (2) Eine Bildaufnahme ist unter Berücksichtigung der Vorgaben gemäß § 13 zulässig, wenn
1. sie im lebenswichtigen Interesse einer Person erforderlich ist,
 2. die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat,
 3. sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist, oder
 4. im Einzelfall überwiegende berechnete Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.
- (3) Eine Bildaufnahme ist gemäß Abs. 2 Z 4 insbesondere dann zulässig, wenn
1. sie dem vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, dient, und räumlich nicht über die Liegenschaft hinausreicht, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen,
 2. sie für den vorbeugenden Schutz von Personen oder Sachen an öffentlich zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials erforderlich ist, oder
 3. sie ein privates Dokumentationsinteresse verfolgt, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist.
- (4) Unzulässig ist
1. eine Bildaufnahme ohne ausdrückliche Einwilligung der betroffenen Person in deren höchstpersönlichen Lebensbereich,
 2. eine Bildaufnahme zum Zweck der Kontrolle von Arbeitnehmern,
 3. der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten ohne ausdrückliche Einwilligung und für das Erstellen von Persönlichkeitsprofilen mit anderen personenbezogenen Daten oder
 4. die Auswertung von mittels Bildaufnahmen gewonnenen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) als Auswahlkriterium.

(5) Im Wege einer zulässigen Bildaufnahme ermittelte personenbezogene Daten dürfen im erforderlichen Ausmaß übermittelt werden, wenn für die Übermittlung eine der Voraussetzungen des Abs. 2 Z 1 bis 4 gegeben ist. Abs. 4 gilt sinngemäß.

Besondere Datensicherheitsmaßnahmen und Kennzeichnung

§ 13. (1) Der Verantwortliche hat dem Risiko des Eingriffs angepasste geeignete Datensicherheitsmaßnahmen zu ergreifen und dafür zu sorgen, dass der Zugang zur Bildaufnahme und eine nachträgliche Veränderung derselben durch Unbefugte ausgeschlossen ist.

(2) Der Verantwortliche hat – außer in den Fällen einer Echtzeitüberwachung – jeden Verarbeitungsvorgang zu protokollieren.

(3) Aufgenommene personenbezogene Daten sind vom Verantwortlichen zu löschen, wenn sie für den Zweck, für den sie ermittelt wurden, nicht mehr benötigt werden und keine andere gesetzlich vorgesehene Aufbewahrungspflicht besteht. Eine länger als 72 Stunden andauernde Aufbewahrung muss verhältnismäßig sein und ist gesondert zu protokollieren und zu begründen.

(4) Die Abs. 1 bis 3 finden keine Anwendung auf Bildaufnahmen nach § 12 Abs. 3 Z 3.

(5) Der Verantwortliche einer Bildaufnahme hat diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen, es sei denn, dieser ist den betroffenen Personen nach den Umständen des Falles bereits bekannt.

(6) Die Kennzeichnungspflicht gilt nicht in den Fällen des § 12 Abs. 3 Z 3 und für zeitlich strikt zu begrenzende Verarbeitungen im Einzelfall, deren Zweck ausschließlich mittels einer verdeckten Ermittlung erreicht werden kann, unter der Bedingung, dass der Verantwortliche ausreichende Garantien zur Wahrung der Betroffeneninteressen vorsieht, insbesondere durch eine nachträgliche Information der betroffenen Personen.

(7) Werden entgegen Abs. 5 keine ausreichenden Informationen bereitgestellt, kann jeder von einer Verarbeitung potenziell Betroffene vom Eigentümer oder Nutzungsberechtigten einer Liegenschaft oder eines Gebäudes oder sonstigen Objekts, von dem aus eine solche Verarbeitung augenscheinlich ausgeht, Auskunft über die Identität des Verantwortlichen begehren. Die unbegründete Nichterteilung einer derartigen Auskunft ist einer Verweigerung der Auskunft nach Art. 15 DSGVO gleichzuhalten.

2. Hauptstück

Organe

1. Abschnitt

Datenschutzrat

Einrichtung und Aufgaben

§ 14. (1) Beim Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz ist ein Datenschutzrat eingerichtet. Dieser nimmt zu Fragen von grundsätzlicher Bedeutung für den Datenschutz Stellung, fördert die einheitliche Fortentwicklung des Datenschutzes und berät die Bundesregierung in rechtspolitischer Hinsicht bei datenschutzrechtlich relevanten Vorhaben.

(2) Zur Erfüllung seiner Aufgaben nach Abs. 1

1. kann der Datenschutzrat Empfehlungen in datenschutzrechtlicher Hinsicht an die Bundesregierung und die Bundesminister richten;
2. kann der Datenschutzrat Gutachten erstellen oder in Auftrag geben;
3. ist dem Datenschutzrat Gelegenheit zur Stellungnahme zu Gesetzesentwürfen der Bundesministerien, soweit diese datenschutzrechtlich von Bedeutung sind, sowie zu Verordnungen im Vollzugsbereich des Bundes, die wesentliche Fragen des Datenschutzes betreffen, zu geben;
4. hat der Datenschutzrat das Recht, von Verantwortlichen des öffentlichen Bereichs Auskünfte und Berichte zu verlangen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist;
5. kann der Datenschutzrat seine Beobachtungen, Bedenken und Anregungen veröffentlichen und den Verantwortlichen des öffentlichen Bereichs zur Kenntnis bringen.

(3) Abs. 2 Z 3 und 4 gilt nicht, soweit innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften betroffen sind.

Zusammensetzung

§ 15. (1) Dem Datenschutzrat gehören an:

1. Vertreter der politischen Parteien: Zwölf Mitglieder entsenden die politischen Parteien nach dem System von d'Hondt im Verhältnis ihrer Mandatsstärke im Hauptausschuss des Nationalrates. Jede im Hauptausschuss des Nationalrates vertretene politische Partei hat Anspruch, im Datenschutzrat vertreten zu sein. Eine im Hauptausschuss des Nationalrates vertretene Partei, der nach der obigen Berechnung kein Mitglied zukommt, kann ein Mitglied namhaft machen;
2. je ein Vertreter der Bundeskammer für Arbeiter und Angestellte und der Wirtschaftskammer Österreich;
3. zwei Vertreter der Länder;
4. je ein Vertreter des Gemeindebundes und des Städtebundes;
5. ein vom Bundesminister für Verfassung, Reformen, Deregulierung und Justiz zu entsendender Vertreter des Bundes;
6. ein von der Bundesregierung zu entsendender Vertreter aus dem Kreis der Datenschutzbeauftragten der Bundesministerien;
7. zwei vom Datenschutzrat nach seiner Konstituierung zu benennende nationale oder internationale Experten aus dem Bereich des Datenschutzes.

(2) Die in Abs. 1 genannten Vertreter sollen Kenntnisse sowie Erfahrungen auf den Gebieten des Datenschutzrechtes, des Unionsrechtes und der Grundrechte haben.

(3) Für jedes Mitglied gemäß Abs. 1 Z 1 bis 6 ist ein Ersatzmitglied zu entsenden, welches bei Verhinderung des Mitgliedes an dessen Stelle tritt. Die Entsendung der Mitglieder und Ersatzmitglieder ist dem Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz schriftlich mitzuteilen.

(4) Nicht angehören können dem Datenschutzrat Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre und weiters Personen, die zum Nationalrat nicht wählbar sind.

(5) Die Funktionsperiode der Mitglieder und Ersatzmitglieder gemäß Abs. 1 Z 1 bis 6 beginnt mit deren Entsendung in den Datenschutzrat und endet

1. mit der Abberufung durch die entsendende Stelle (Abs. 1) im Wege einer schriftlichen Mitteilung an das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz unter gleichzeitiger Namhaftmachung eines neuen Mitgliedes oder Ersatzmitgliedes,
2. mit der Bekanntgabe des Ausscheidens durch das Mitglied oder Ersatzmitglied im Wege einer schriftliche Mitteilung an das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz oder
3. spätestens mit der Neuwahl des Hauptausschusses des Nationalrates nach den §§ 29 und 30 des Geschäftsordnungsgesetzes 1975, BGBl. Nr. 410/1975.

Auf gemäß Abs. 1 Z 7 benannte Mitglieder des Datenschutzrates findet Z 3 Anwendung.

(6) Nach Neuwahl des Hauptausschusses des Nationalrates (Abs. 5 Z 3) führt das bisherige Präsidium gemäß § 17 Abs. 4 die Geschäfte bis zur konstituierenden Sitzung der neubestellten Mitglieder und Ersatzmitglieder fort. Binnen eines Zeitraumes von zwei Wochen ab der Neuwahl des Hauptausschusses des Nationalrates haben die entsendenden Stellen eine dem Abs. 1 entsprechende Anzahl von Mitgliedern und Ersatzmitgliedern dem Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz schriftlich bekannt zu geben. Die Wiederbestellung von Mitgliedern und Ersatzmitgliedern ist zulässig.

(7) Die konstituierende Sitzung des Datenschutzrates hat spätestens sechs Wochen nach der Wahl des Hauptausschusses des Nationalrates stattzufinden und ist vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz einzuberufen.

(8) Die Tätigkeit der Mitglieder und Ersatzmitglieder des Datenschutzrates ist ehrenamtlich. Mitglieder und Ersatzmitglieder des Datenschutzrates, die außerhalb von Wien wohnen, haben im Fall der Teilnahme an Sitzungen des Datenschutzrates Anspruch auf Ersatz der angemessenen Reisekosten nach Maßgabe der Reisegebührenschriften des Bundes. Die Vergütungen und Erstattungen sind im Nachhinein quartalsweise vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz anzuweisen.

Vorsitz und Geschäftsführung

§ 16. (1) Der Datenschutzrat gibt sich mit Beschluss eine Geschäftsordnung.

(2) Der Datenschutzrat hat in der konstituierenden Sitzung aus den vorliegenden Wahlvorschlägen mit einfacher Mehrheit aus seiner Mitte einen Vorsitzenden und zwei stellvertretende Vorsitzende zu

wählen. Stichwahlen sind zulässig. Die Wahlvorschläge sind den Mitgliedern und Ersatzmitgliedern gleichzeitig mit der Einladung zur konstituierenden Sitzung bekannt zu geben. Die Wiederwahl ist zulässig.

- (3) Die Funktionsperiode des Vorsitzenden und der stellvertretenden Vorsitzenden endet
1. mit Eintritt einer der Voraussetzungen des § 15 Abs. 5 Z 1 bis 3,
 2. mit Bekanntgabe der Zurücklegung der Funktion durch den Vorsitzenden oder einen der stellvertretenden Vorsitzenden im Wege einer Erklärung in der Sitzung des Datenschutzrates oder einer schriftlichen Mitteilung an das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz oder
 3. nach Abwahl durch den Datenschutzrat mit einfacher Mehrheit der abgegebenen Stimmen und Anwesenheit von mehr als zwei Drittel seiner Mitglieder oder Ersatzmitglieder.

Nach dem Ende der Funktionsperiode des Vorsitzenden oder eines stellvertretenden Vorsitzenden ist umgehend ein neuer Vorsitzender oder ein neuer stellvertretender Vorsitzender zu wählen.

- (4) Der gemäß Abs. 2 gewählte Vorsitzende vertritt den Datenschutzrat nach außen.

(5) Die Geschäftsführung des Datenschutzrates obliegt dem Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz. Der Bundesminister für Verfassung, Reformen, Deregulierung und Justiz hat das hierfür notwendige Personal zur Verfügung zu stellen. Bei ihrer Tätigkeit für den Datenschutzrat sind die Bediensteten des Bundesministeriums für Verfassung, Reformen, Deregulierung und Justiz fachlich an die Weisungen des Vorsitzenden des Datenschutzrates gebunden.

Sitzungen und Beschlussfassung

§ 17. (1) Die Sitzungen des Datenschutzrates werden vom Vorsitzenden nach Bedarf einberufen. Jedes Mitglied des Datenschutzrates kann schriftlich die Einberufung des Datenschutzrates unter Angabe des gewünschten Verhandlungsgegenstandes begehren. Liegt ein solches Begehren vor, so hat der Vorsitzende die Sitzung so anzuberaumen, dass sie spätestens vier Wochen nach Einlangen des Begehrens stattfindet.

(2) Jedes Mitglied des Datenschutzrates ist – außer im Fall der gerechtfertigten Verhinderung – verpflichtet, an den Sitzungen des Datenschutzrates teilzunehmen. Nur bei Verhinderung des Mitglieds nimmt das Ersatzmitglied an der Sitzung teil.

(3) Für Beratungen und Beschlussfassung im Datenschutzrat ist die Anwesenheit von mehr als der Hälfte seiner Mitglieder oder Ersatzmitglieder erforderlich. Zur Beschlussfassung genügt die einfache Mehrheit der abgegebenen Stimmen. Bei Stimmgleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig. Minderheitenvoten sind zulässig.

(4) Bei dringlichen Angelegenheiten kann der Vorsitzende die stellvertretenden Vorsitzenden und je einen Vertreter der politischen Parteien (§ 15 Abs. 1 Z 1) zu einer außerordentlichen Sitzung (Präsidium) einladen.

(5) Der Datenschutzrat kann aus seiner Mitte ständige oder nichtständige Arbeitsausschüsse bilden, denen er die Vorbereitung, Begutachtung und Bearbeitung einzelner Angelegenheiten übertragen kann. Er ist auch berechtigt, die Geschäftsführung, Vorbegutachtung und die Bearbeitung einzelner Angelegenheiten einem einzelnen Mitglied (Berichterstatter) zu übertragen.

(6) Der Leiter der Datenschutzbehörde ist berechtigt, an den Sitzungen des Datenschutzrates oder seiner Arbeitsausschüsse teilzunehmen. Ein Stimmrecht steht ihm nicht zu.

(7) Der Vorsitzende kann bei Bedarf Sachverständige zu den Sitzungen des Datenschutzrates oder zu Arbeitsausschüssen beziehen. Auch zur Vorbereitung von Sitzungen des Datenschutzrates oder Arbeitsausschüssen kann der Vorsitzende des Datenschutzrates Experten des jeweiligen Fachgebietes beziehen, soweit dies zur Klärung von Fragen von besonderer Bedeutung für den Datenschutz erforderlich ist.

(8) Die Beratungen in den Sitzungen des Datenschutzrates sind, soweit er nicht selbst anderes beschließt, nicht öffentlich. Die Mitglieder und Ersatzmitglieder des Datenschutzrates, der Leiter der Datenschutzbehörde sowie sein Stellvertreter und die zur Sitzung zugezogenen Sachverständigen sind zur Verschwiegenheit über alle ihnen ausschließlich aus ihrer Tätigkeit im Datenschutzrat bekanntgewordenen Tatsachen verpflichtet.

2. Abschnitt Datenschutzbehörde

Einrichtung

§ 18. (1) Die Datenschutzbehörde wird als nationale Aufsichtsbehörde gemäß Art. 51 DSGVO eingerichtet.

(2) Der Datenschutzbehörde steht ein Leiter vor. In seiner Abwesenheit leitet sein Stellvertreter die Datenschutzbehörde. Auf ihn finden die Regelungen hinsichtlich des Leiters der Datenschutzbehörde Anwendung.

Unabhängigkeit

§ 19. (1) Die Datenschutzbehörde ist eine Dienstbehörde und Personalstelle.

(2) Der Leiter darf für die Dauer seines Amtes keine Tätigkeit ausüben, die

1. Zweifel an der unabhängigen Ausübung seines Amtes oder seiner Unbefangenheit hervorrufen könnte,
2. ihn bei der Erfüllung seiner dienstlichen Aufgaben behindert oder
3. wesentliche dienstliche Interessen gefährdet.

Er ist verpflichtet, Tätigkeiten, die er neben seiner Tätigkeit als Leiter der Datenschutzbehörde ausübt, unverzüglich dem Bundesminister für Verfassung, Reformen, Deregulierung und Justiz zur Kenntnis zu bringen.

(3) Der Bundesminister für Verfassung, Reformen, Deregulierung und Justiz kann sich beim Leiter der Datenschutzbehörde über die Gegenstände der Geschäftsführung unterrichten. Dem ist vom Leiter der Datenschutzbehörde nur insoweit zu entsprechen, als dies nicht der völligen Unabhängigkeit der Aufsichtsbehörde im Sinne von Art. 52 DSGVO widerspricht.

Leiter der Datenschutzbehörde

§ 20. (1) Der Leiter der Datenschutzbehörde wird vom Bundespräsidenten auf Vorschlag der Bundesregierung für eine Dauer von fünf Jahren bestellt; die Wiederbestellung ist zulässig. Dem Vorschlag hat eine Ausschreibung zur allgemeinen Bewerbung voranzugehen.

(2) Der Leiter der Datenschutzbehörde hat

1. das Studium der Rechtswissenschaften abgeschlossen zu haben,
2. die persönliche und fachliche Eignung durch eine entsprechende Vorbildung und einschlägige Berufserfahrung in den von der Datenschutzbehörde zu besorgenden Angelegenheiten aufzuweisen,
3. über ausgezeichnete Kenntnisse des österreichischen Datenschutzrechtes, des Unionsrechtes und der Grundrechte zu verfügen und
4. über eine mindestens fünfjährige juristische Berufserfahrung zu verfügen.

(3) Zum Leiter der Datenschutzbehörde dürfen nicht bestellt werden:

1. Mitglieder der Bundesregierung, Staatssekretäre, Mitglieder einer Landesregierung, Mitglieder des Nationalrates, des Bundesrates oder sonst eines allgemeinen Vertretungskörpers oder des Europäischen Parlaments, ferner Volksanwälte und der Präsident des Rechnungshofes,
2. Personen, die eine in Z 1 genannte Funktion innerhalb der letzten zwei Jahre ausgeübt haben, und
3. Personen, die von der Wählbarkeit in den Nationalrat ausgeschlossen sind.

(4) Die Enthebung des Leiters ist auf Vorschlag der Bundesregierung durch den Bundespräsidenten vorzunehmen.

(5) Der Stellvertreter des Leiters der Datenschutzbehörde wird vom Bundespräsidenten auf Vorschlag der Bundesregierung nach Maßgabe der Abs. 1 bis 3 bestellt. Auf die Enthebung des Stellvertreters findet Abs. 4 Anwendung.

Aufgaben

§ 21. (1) Die Datenschutzbehörde berät die Ausschüsse des Nationalrates und des Bundesrates, die Bundesregierung und die Landesregierungen auf deren Ersuchen über legislative und administrative Maßnahmen. Die Datenschutzbehörde ist vor Erlassung von Bundesgesetzen sowie von Verordnungen im Vollzugsbereich des Bundes, die Fragen des Datenschutzes unmittelbar betreffen, anzuhören.

(2) Die Datenschutzbehörde hat die Listen nach Art. 35 Abs. 4 und 5 DSGVO im Wege einer Verordnung im Bundesgesetzblatt kundzumachen.

(3) Die Datenschutzbehörde hat die nach Art. 57 Abs. 1 lit. p DSGVO festzulegenden Kriterien im Wege einer Verordnung kundzumachen. Sie fungiert zugleich als einzige nationale Akkreditierungsstelle gemäß Art. 43 Abs. 1 lit. a DSGVO.

Befugnisse

§ 22. (1) Die Datenschutzbehörde kann vom Verantwortlichen oder Auftragsverarbeiter der überprüften Datenverarbeitung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenverarbeitungen und diesbezügliche Unterlagen begehren. Der Verantwortliche oder Auftragsverarbeiter hat die notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglicher Schonung der Rechte des Verantwortlichen oder des Auftragsverarbeiters und Dritter auszuüben.

(2) Zum Zweck der Einschau ist die Datenschutzbehörde nach Verständigung des Inhabers der Räumlichkeiten und des Verantwortlichen oder des Auftragsverarbeiters berechtigt, Räume, in welchen Datenverarbeitungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen.

(3) Informationen, die der Datenschutzbehörde oder den von ihr Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Im Übrigen besteht die Pflicht zur Verschwiegenheit auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, dass dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach § 63 dieses Bundesgesetzes oder nach §§ 118a, 119, 119a, 126a bis 126c, 148a oder § 278a des Strafgesetzbuches – StGB, BGBl. Nr. 60/1974, oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch Ersuchen nach § 76 der Strafprozeßordnung – StPO, BGBl. Nr. 631/1975, zu entsprechen ist.

(4) Liegt durch den Betrieb einer Datenverarbeitung eine wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen der betroffenen Personen (Gefahr im Verzug) vor, so kann die Datenschutzbehörde die Weiterführung der Datenverarbeitung mit Bescheid gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG, BGBl. Nr. 51/1991, untersagen. Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenverarbeitung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Ebenso kann die Datenschutzbehörde auf Antrag einer betroffenen Person eine Einschränkung der Verarbeitung nach Art. 18 DSGVO mit Bescheid gemäß § 57 Abs. 1 AVG anordnen, wenn der Verantwortliche einer diesbezüglichen Verpflichtung nicht fristgerecht nachkommt. Wird einer Untersagung nicht unverzüglich Folge geleistet, hat die Datenschutzbehörde nach Art. 83 Abs. 5 DSGVO vorzugehen.

(5) Der Datenschutzbehörde obliegt im Rahmen ihrer Zuständigkeit die Verhängung von Geldbußen gegenüber natürlichen und juristischen Personen.

(6) Bestehen im Zuge einer auf § 29 gestützten Klage einer betroffenen Person, die sich von einer Einrichtung, Organisation oder Vereinigung im Sinne des Art. 80 Abs. 1 DSGVO vertreten lässt, Zweifel am Vorliegen der diesbezüglichen Kriterien, trifft die Datenschutzbehörde auf Antrag des Einbringungsgerichtes entsprechende Feststellungen mit Bescheid. Diese Einrichtung, Organisation oder Vereinigung hat im Verfahren Parteistellung. Gegen einen negativen Feststellungsbescheid steht ihr die Beschwerde an das Bundesverwaltungsgericht offen.

Tätigkeitsbericht und Veröffentlichung von Entscheidungen

§ 23. (1) Die Datenschutzbehörde hat bis zum 31. März eines jeden Jahres einen dem Art. 59 DSGVO entsprechenden Tätigkeitsbericht zu erstellen und dem Bundesminister für Verfassung, Reformen, Deregulierung und Justiz vorzulegen. Der Bericht ist vom Bundesminister für Verfassung, Reformen, Deregulierung und Justiz der Bundesregierung, dem Nationalrat und dem Bundesrat vorzulegen. Die Datenschutzbehörde hat den Bericht der Öffentlichkeit, der Europäischen Kommission, dem Europäischen Datenschutzausschuss (Art. 68 DSGVO) und dem Datenschutzrat zugänglich zu machen.

(2) Entscheidungen der Datenschutzbehörde von grundsätzlicher Bedeutung für die Allgemeinheit sind von der Datenschutzbehörde unter Beachtung der Erfordernisse der Amtsverschwiegenheit in geeigneter Weise zu veröffentlichen.

3. Abschnitt

Rechtsbehelfe, Haftung und Sanktionen

Beschwerde an die Datenschutzbehörde

§ 24. (1) Jede betroffene Person hat das Recht auf Beschwerde bei der Datenschutzbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO oder gegen § 1 oder Artikel 2 1. Hauptstück verstößt.

(2) Die Beschwerde hat zu enthalten:

1. die Bezeichnung des als verletzt erachteten Rechts,
2. soweit dies zumutbar ist, die Bezeichnung des Rechtsträgers oder Organs, dem die behauptete Rechtsverletzung zugerechnet wird (Beschwerdegegner),
3. den Sachverhalt, aus dem die Rechtsverletzung abgeleitet wird,
4. die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt,
5. das Begehren, die behauptete Rechtsverletzung festzustellen und
6. die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist.

(3) Einer Beschwerde sind gegebenenfalls der zu Grunde liegende Antrag und eine allfällige Antwort des Beschwerdegegners anzuschließen. Die Datenschutzbehörde hat im Falle einer Beschwerde auf Ersuchen der betroffenen Person weitere Unterstützung zu leisten.

(4) Der Anspruch auf Behandlung einer Beschwerde erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behaupteter Maßen stattgefunden hat, einbringt. Verspätete Beschwerden sind zurückzuweisen.

(5) Soweit sich eine Beschwerde als berechtigt erweist, ist ihr Folge zu geben. Ist eine Verletzung einem Verantwortlichen des privaten Bereichs zuzurechnen, so ist diesem aufzutragen, den Anträgen des Beschwerdeführers auf Auskunft, Berichtigung, Löschung, Einschränkung oder Datenübertragung in jenem Umfang zu entsprechen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen. Soweit sich die Beschwerde als nicht berechtigt erweist, ist sie abzuweisen.

(6) Ein Beschwerdegegner kann bis zum Abschluss des Verfahrens vor der Datenschutzbehörde die behauptete Rechtsverletzung nachträglich beseitigen, indem er den Anträgen des Beschwerdeführers entspricht. Erscheint der Datenschutzbehörde die Beschwerde insofern als gegenstandslos, so hat sie den Beschwerdeführer dazu zu hören. Gleichzeitig ist er darauf aufmerksam zu machen, dass die Datenschutzbehörde das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begründet, warum er die ursprünglich behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet. Wird durch eine derartige Äußerung des Beschwerdeführers die Sache ihrem Wesen nach geändert (§ 13 Abs. 8 AVG), so ist von der Zurückziehung der ursprünglichen Beschwerde und der gleichzeitigen Einbringung einer neuen Beschwerde auszugehen. Auch diesfalls ist das ursprüngliche Beschwerdeverfahren formlos einzustellen und der Beschwerdeführer davon zu verständigen. Verspätete Äußerungen sind nicht zu berücksichtigen.

(7) Der Beschwerdeführer wird von der Datenschutzbehörde innerhalb von drei Monaten ab Einbringung der Beschwerde über den Stand und das Ergebnis der Ermittlung unterrichtet.

(8) Jede betroffene Person kann das Bundesverwaltungsgericht befassen, wenn die Datenschutzbehörde sich nicht mit der Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der erhobenen Beschwerde in Kenntnis gesetzt hat.

(9) Die Datenschutzbehörde kann – soweit erforderlich – Amtssachverständige im Verfahren beiziehen.

(10) In die Entscheidungsfrist gemäß § 73 AVG werden nicht eingerechnet:

1. die Zeit, während deren das Verfahren bis zur rechtskräftigen Entscheidung einer Vorfrage ausgesetzt ist;
2. die Zeit während eines Verfahrens nach Art. 56, 60 und 63 DSGVO.

Begleitende Maßnahmen im Beschwerdeverfahren

§ 25. (1) Macht der Beschwerdeführer im Rahmen einer Beschwerde eine wesentliche Beeinträchtigung seiner schutzwürdigen Geheimhaltungsinteressen durch die Verarbeitung seiner personenbezogenen Daten glaubhaft, kann die Datenschutzbehörde nach § 22 Abs. 4 vorgehen.

(2) Ist in einem Verfahren die Richtigkeit von personenbezogenen Daten strittig, so ist vom Beschwerdegegner bis zum Abschluss des Verfahrens ein Bestreitungsvermerk anzubringen. Erforderlichenfalls hat dies die Datenschutzbehörde auf Antrag des Beschwerdeführers mit Bescheid gemäß § 57 Abs. 1 AVG anzuordnen.

(3) Berufet sich ein Verantwortlicher gegenüber der Datenschutzbehörde auf eine Beschränkung im Sinne des Art. 23 DSGVO, so hat diese die Rechtmäßigkeit der Anwendung der Beschränkungen zu überprüfen. Kommt sie zur Auffassung, dass die Geheimhaltung von verarbeiteten personenbezogenen Daten gegenüber der betroffenen Person nicht gerechtfertigt war, ist die Offenlegung der personenbezogenen Daten mit Bescheid aufzutragen. Wird dem Bescheid der Datenschutzbehörde binnen acht Wochen nicht entsprochen, so hat die Datenschutzbehörde die Offenlegung der personenbezogenen Daten gegenüber der betroffenen Person selbst vorzunehmen und ihr die verlangte Auskunft zu erteilen oder ihr mitzuteilen, welche personenbezogenen Daten bereits berichtet oder gelöscht wurden.

(4) Bescheide, mit denen Übermittlungen von personenbezogenen Daten ins Ausland genehmigt wurden, sind zu widerrufen, wenn die rechtlichen oder tatsächlichen Voraussetzungen für die Erteilung der Genehmigung nicht mehr bestehen.

Verantwortliche des öffentlichen und des privaten Bereichs

§ 26. (1) Unbeschadet des § 5 Abs. 3 sind Verantwortliche des öffentlichen Bereichs alle Verantwortlichen,

1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder
2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

(2) Verantwortliche des öffentlichen Bereichs sind Partei in Verfahren vor der Datenschutzbehörde.

(3) Verantwortliche des öffentlichen Bereichs können Beschwerde an das Bundesverwaltungsgericht und Revision beim Verwaltungsgerichtshof erheben.

(4) Die dem Abs. 1 nicht unterliegenden Verantwortlichen gelten als Verantwortliche des privaten Bereichs im Sinne dieses Bundesgesetzes.

Beschwerde an das Bundesverwaltungsgericht

§ 27. (1) Das Bundesverwaltungsgericht entscheidet durch Senat über Beschwerden gegen Bescheide, wegen der Verletzung der Unterrichtungspflicht gemäß § 24 Abs. 7 und der Entscheidungspflicht der Datenschutzbehörde.

(2) Der Senat besteht aus einem Vorsitzenden und je einem fachkundigen Laienrichter aus dem Kreis der Arbeitgeber und aus dem Kreis der Arbeitnehmer. Die fachkundigen Laienrichter werden auf Vorschlag der Wirtschaftskammer Österreich und der Bundeskammer für Arbeiter und Angestellte bestellt. Es sind entsprechende Vorkehrungen zu treffen, dass zeitgerecht eine hinreichende Anzahl von fachkundigen Laienrichtern zur Verfügung steht.

(3) Die fachkundigen Laienrichter müssen eine mindestens fünfjährige einschlägige Berufserfahrung und besondere Kenntnisse des Datenschutzrechtes besitzen.

(4) Der Vorsitzende hat den fachkundigen Laienrichtern alle entscheidungsrelevanten Dokumente unverzüglich zu übermitteln oder, wenn dies unzulässig oder zur Wahrung der Vertraulichkeit von Dokumenten unbedingt erforderlich ist, zur Verfügung zu stellen.

(5) Kommt es zu einem Verfahren gegen den Bescheid der Datenschutzbehörde, der eine Stellungnahme oder ein Beschluss des Europäischen Ausschusses im Rahmen des Kohärenzverfahrens vorangegangen ist, so leitet die Datenschutzbehörde diese Stellungnahme oder diesen Beschluss dem Bundesverwaltungsgericht zu.

Vertretung von betroffenen Personen

§ 28. Die betroffene Person hat das Recht, eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen und in ihrem Namen die in den §§ 24 bis 27 genannten Rechte wahrzunehmen.

Haftung und Recht auf Schadenersatz

§ 29. (1) Jede Person, der wegen eines Verstoßes gegen die DSGVO oder gegen § 1 oder Artikel 2 1. Hauptstück ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz

gegen den Verantwortlichen oder gegen den Auftragsverarbeiter nach Art. 82 DSGVO. Im Einzelnen gelten für diesen Schadenersatzanspruch die allgemeinen Bestimmungen des bürgerlichen Rechts.

(2) Für Klagen auf Schadenersatz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Kläger (Antragsteller) seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen (Anträge) können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder eine Niederlassung hat.

Allgemeine Bedingungen für die Verhängung von Geldbußen

§ 30. (1) Die Datenschutzbehörde kann Geldbußen gegen eine juristische Person verhängen, wenn Verstöße gegen Bestimmungen der DSGVO und des § 1 oder Artikel 2 1. Hauptstück durch Personen begangen wurden, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt haben und eine Führungsposition innerhalb der juristischen Person aufgrund

1. der Befugnis zur Vertretung der juristischen Person,
2. der Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder
3. einer Kontrollbefugnis innerhalb der juristischen Person

innehaben.

(2) Juristische Personen können wegen Verstößen gegen Bestimmungen der DSGVO und des § 1 oder Artikel 2 1. Hauptstück auch verantwortlich gemacht werden, wenn mangelnde Überwachung oder Kontrolle durch eine in Abs. 1 genannte Person die Begehung dieser Verstöße durch eine für die juristische Person tätige Person ermöglicht hat, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet.

(3) Die Datenschutzbehörde hat von der Bestrafung eines Verantwortlichen gemäß § 9 des Verwaltungsstrafgesetzes 1991 – VStG, BGBl. Nr. 52/1991, abzusehen, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird.

(4) Die gemäß § 22 Abs. 5 verhängten Geldbußen fließen dem Bund zu und sind nach den Bestimmungen über die Eintreibung von gerichtlichen Geldstrafen einzubringen. Rechtskräftige Bescheide der Datenschutzbehörde sind Exekutionstitel. Die Bewilligung und der Vollzug der Exekution ist auf Grund des Exekutionstitels der Datenschutzbehörde bei dem Bezirksgericht, in dessen Sprengel der Verpflichtete seinen allgemeinen Gerichtsstand in Streitsachen hat (§§ 66, 75 der Jurisdiktionsnorm – JN, RGBl. Nr. 111/1895), oder bei dem in den §§ 18 und 19 EO bezeichneten Exekutionsgericht zu beantragen.

(5) Gegen Behörden und öffentliche Stellen, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, die im gesetzlichen Auftrag handeln, und gegen Körperschaften des öffentlichen Rechts können keine Geldbußen verhängt werden.

4. Abschnitt

Aufsichtsbehörde nach der Richtlinie (EU) 2016/680

Datenschutzbehörde

§ 31. (1) Die Datenschutzbehörde wird als nationale Aufsichtsbehörde für den in § 36 Abs. 1 genannten Anwendungsbereich eingerichtet. Die Datenschutzbehörde ist nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

(2) Hinsichtlich der Unabhängigkeit, der allgemeinen Bedingungen und der Errichtung der Aufsichtsbehörde finden die Art. 52, 53 und 54 DSGVO sowie der § 18 Abs. 2, §§ 19 und 20 sinngemäß Anwendung.

Aufgaben der Datenschutzbehörde

§ 32. (1) Die Datenschutzbehörde hat im Anwendungsbereich des § 36 Abs. 1

1. die Anwendung des § 1 und der im 3. Hauptstück erlassenen Vorschriften sowie der Durchführungsvorschriften zur Richtlinie (EU) 2016/680 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. Nr. L 119 vom 4.5.2016 S. 89, 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;

3. die in Art. 57 Abs. 1 lit. c bis e, g, h und t DSGVO festgelegten Aufgaben im Hinblick auf das 3. Hauptstück zu erfüllen;
4. sich mit Beschwerden einer betroffenen Person oder einer Stelle, einer Organisation oder einer Vereinigung gemäß § 28 zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer Frist von drei Monaten über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;
5. die Rechtmäßigkeit der Verarbeitung gemäß § 42 Abs. 8 zu überprüfen und die betroffene Person innerhalb einer angemessenen Frist über das Ergebnis der Überprüfung gemäß § 42 Abs. 9 zu unterrichten oder ihr die Gründe mitzuteilen, aus denen die Überprüfung nicht vorgenommen wurde;
6. maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie,
7. Beratung in Bezug auf die in § 53 genannten Verarbeitungsvorgänge zu leisten, und
8. die Rechte der betroffenen Person in den Fällen der §§ 43 Abs. 4, 44 Abs. 3 und 45 Abs. 4 auszuüben.

(2) Die Datenschutzbehörde erleichtert das Einreichen von in Abs. 1 Z 4 genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(3) Art. 57 Abs. 3 und 4 DSGVO finden sinngemäß Anwendung.

Befugnisse der Datenschutzbehörde

§ 33. (1) Die Datenschutzbehörde verfügt im Anwendungsbereich des § 36 Abs. 1 über die zur Vollziehung ihres Aufgabenbereichs erforderlichen wirksamen Untersuchungsbefugnisse. Diese umfassen insbesondere die in § 22 Abs. 2 genannten Befugnisse.

(2) Die Datenschutzbehörde verfügt im Anwendungsbereich des § 36 Abs. 1 über die zur Vollziehung ihres Aufgabenbereichs erforderlichen wirksamen Abhilfebefugnisse. Dazu zählen jedenfalls die Befugnisse, die es ihr gestatten

1. einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die im Anwendungsbereich der Richtlinie (EU) 2016/680 erlassenen Vorschriften verstoßen;
2. den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge, auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den im Anwendungsbereich der Richtlinie (EU) 2016/680 erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung gemäß § 45;
3. eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen.

(3) Die Datenschutzbehörde verfügt im Anwendungsbereich des § 36 Abs. 1 über die zur Vollziehung erforderlichen wirksamen Beratungsbefugnisse, die es ihr gestatten, gemäß dem Verfahren der vorherigen Konsultation nach § 53 den Verantwortlichen zu beraten und zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Antrag Stellungnahmen an den Nationalrat oder den Bundesrat, die Bundes- oder Landesregierung oder an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten.

(4) Die Ausübung der der Aufsichtsbehörde übertragenen Befugnisse richtet sich im Anwendungsbereich § 36 Abs. 1 sinngemäß nach Art. 58 Abs. 4 DSGVO.

(5) § 22 Abs. 3 2. Satz gilt sinngemäß für Verstöße im Anwendungsbereich des § 36 Abs. 1.

Allgemeine Bestimmungen

§ 34. (1) Verantwortliche haben im Anwendungsbereich des § 36 Abs. 1 wirksame Vorkehrungen zu treffen, um vertrauliche Meldungen über Verstöße zu fördern. In diesem Sinne haben Verantwortliche insbesondere angemessene Verfahren einzurichten, die es ermöglichen, Verstöße gegen die Bestimmungen des 3. Hauptstücks an eine geeignete Stelle zu melden.

(2) Die in Abs. 1 angeführten Vorkehrungen umfassen zumindest

1. spezielle Verfahren für den Empfang der Meldungen über Verstöße und deren Weiterverfolgung;

2. den Schutz personenbezogener Daten sowohl für die Person, die die Verstöße anzeigt, als auch für die natürliche Person, die mutmaßlich für einen Verstoß verantwortlich ist;
3. klare Regeln, welche die Geheimhaltung der Identität der Person, die die Verstöße anzeigt, gewährleisten, soweit nicht die Offenlegung der Identität im Rahmen eines staatsanwaltschaftlichen, gerichtlichen oder verwaltungsrechtlichen Verfahrens zwingend zu erfolgen hat.

(3) Die Datenschutzbehörde hat im Rahmen des Tätigkeitsberichtes nach § 23 über die Tätigkeiten nach dem 4. und 5. Abschnitt zu berichten. Die Vorgaben des Art. 59 DSGVO und § 23 für den Tätigkeitsbericht und die Veröffentlichung von Entscheidungen finden sinngemäß Anwendung.

(4) Auf die gegenseitige Amtshilfe im Anwendungsbereich des § 36 Abs. 1 findet Art. 61 Abs. 1 bis 7 DSGVO sinngemäß Anwendung.

(5) Im Anwendungsbereich des § 36 Abs. 1 finden die Regelungen des 3. Abschnitts des 2. Hauptstücks – mit Ausnahme des § 30 – sinngemäß Anwendung.

5. Abschnitt

Besondere Befugnisse der Datenschutzbehörde

§ 35. (1) Die Datenschutzbehörde ist nach den näheren Bestimmungen der DSGVO und dieses Bundesgesetzes zur Wahrung des Datenschutzes berufen.

(2) (**Verfassungsbestimmung**) Die Datenschutzbehörde übt ihre Befugnisse auch gegenüber den in Art. 19 B-VG bezeichneten obersten Organen der Vollziehung sowie gegenüber den obersten Organen gemäß Art. 30 Abs. 3 bis 6, 125, 134 Abs. 8 und 148h Abs. 1 und 2 B-VG im Bereich der diesen zustehenden Verwaltungsangelegenheiten aus.

3. Hauptstück

Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs

1. Abschnitt

Allgemeine Bestimmungen

Anwendungsbereich und Begriffsbestimmungen

§ 36. (1) Die Bestimmungen dieses Hauptstücks gelten für die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung.

(2) Im Sinne dieses Hauptstücks 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung 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. „zuständige Behörde“
 - a) eine staatliche Stelle, 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, die nationale Sicherheit, den Nachrichtendienst oder die militärische Eigensicherung zuständig ist, oder
 - b) eine andere Stelle oder Einrichtung, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zum Zweck der nationalen Sicherheit, des Nachrichtendienstes oder der militärischen Eigensicherung übertragen wurde;
8. „Verantwortlicher“ die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
9. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
10. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags aufgrund von Gesetzen möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;
11. „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;
12. „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;
13. „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;
14. „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;
15. „Aufsichtsbehörde“ ist die Datenschutzbehörde;
16. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

Grundsätze für die Datenverarbeitung, Kategorisierung und Datenqualität

§ 37. (1) Personenbezogene Daten

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

2. müssen für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,
3. müssen dem Verarbeitungszweck entsprechen und müssen maßgeblich sein und dürfen in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sein,
4. müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,
5. dürfen nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht,
6. müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

(2) Für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke im Anwendungsbereich des § 36 Abs. 1 gilt § 38.

(3) Der Verantwortliche ist für die Einhaltung der Abs. 1 und 2 verantwortlich und muss deren Einhaltung nachweisen können.

(4) Soweit möglich und zumutbar, ist zwischen den personenbezogenen Daten insbesondere folgender Kategorien betroffener Personen zu unterscheiden:

1. Personen, die aufgrund bestimmter Tatsachen konkret verdächtig sind, eine strafbare Handlung begangen zu haben,
2. Personen, gegen die aufgrund bestimmter Tatsachen der begründete Verdacht besteht, dass sie in naher Zukunft eine strafbare Handlung begehen werden,
3. verurteilte Straftäter,
4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie Opfer einer Straftat sind, und
5. sonstige Personen, die im Zusammenhang mit einer Straftat stehen, insbesondere Personen, die als Zeugen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit den in Z 1 bis 3 genannten Personen in Kontakt oder in Verbindung stehen.

(5) Soweit möglich ist zwischen faktenbasierten und auf persönlichen Einschätzungen beruhenden personenbezogenen Daten zu unterscheiden. Auf persönlichen Einschätzungen beruhende personenbezogene Daten sind entsprechend zu kennzeichnen und können mit einer Begründung versehen werden, welche die Nachvollziehbarkeit der Einschätzung ermöglicht.

(6) Unrichtige, unvollständige, nicht mehr aktuelle oder zu löschende personenbezogene Daten dürfen weder übermittelt noch zum automatisierten Abruf aus Dateisystemen bereitgestellt werden. Die Behörde hat zu diesem Zweck vor einer Übermittlung die Datenqualität soweit möglich entsprechend zu überprüfen. Zum automatisierten Abruf bereit gehaltene personenbezogene Daten sind entsprechend laufend vollständig und aktuell zu halten.

(7) Bei jeder Übermittlung personenbezogener Daten sind soweit möglich die zur Beurteilung der Aktualität, Richtigkeit, Vollständigkeit und Zuverlässigkeit der personenbezogenen Daten durch den Empfänger erforderlichen Informationen beizufügen.

(8) Wird von Amts wegen oder infolge einer Mitteilung eines Betroffenen festgestellt, dass personenbezogene Daten übermittelt worden sind, die nicht den Anforderungen nach Abs. 6 entsprechen, teilt die übermittelnde bzw. dateisystemführende Dienststelle und Behörde dies der empfangenden Stelle oder Behörde unverzüglich mit. Letztere hat unverzüglich die Löschung unrechtmäßig übermittelter Daten, die Berichtigung unrichtiger Daten, die Ergänzung unvollständiger Daten oder eine Einschränkung der Verarbeitung vorzunehmen.

(9) Hat die empfangende Dienststelle oder Behörde Grund zur Annahme, dass übermittelte personenbezogene Daten unrichtig oder nicht aktuell sind oder zu löschen oder in der Verarbeitung einzuschränken wären, so unterrichtet sie die übermittelnde Dienststelle oder Behörde unverzüglich hierüber. Letztere ergreift unverzüglich die erforderlichen Maßnahmen.

Rechtmäßigkeit der Verarbeitung

§ 38. Die Verarbeitung personenbezogener Daten ist, soweit sie nicht zur Wahrung lebenswichtiger Interessen einer Person erforderlich ist, nur rechtmäßig, soweit sie gesetzlich oder in unmittelbar

anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, vorgesehen und für die Erfüllung einer Aufgabe erforderlich und verhältnismäßig ist, die von der zuständigen Behörde zu den in § 36 Abs. 1 genannten Zwecken wahrgenommen wird.

Verarbeitung besonderer Kategorien personenbezogener Daten

§ 39. Die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person für die in § 36 Abs. 1 genannten Zwecke ist nur zulässig, wenn die Verarbeitung unbedingt erforderlich ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden und

1. die Verarbeitung gemäß § 38 zulässig ist oder
2. sie sich auf Daten bezieht, die die betroffene Person offensichtlich selbst öffentlich gemacht hat.

Verarbeitung für andere Zwecke und Übermittlung

§ 40. (1) Eine Verarbeitung von personenbezogenen Daten nach den Bestimmungen dieses Hauptstücks durch denselben oder einen anderen Verantwortlichen für einen anderen Verarbeitungszweck, als jenen, für den sie erhoben wurden, ist nur zulässig, wenn dieser andere Zweck vom Anwendungsbereich des § 36 Abs. 1 umfasst ist und die Voraussetzungen der §§ 38 und 39 erfüllt sind.

(2) Die Übermittlung von nach den Bestimmungen dieses Hauptstücks verarbeiteten personenbezogenen Daten für einen nicht in § 36 Abs. 1 genannten Zweck ist nur zulässig, wenn dies gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, ausdrücklich vorgesehen ist und der Empfänger zur Verarbeitung dieser personenbezogenen Daten für diesen anderen Zweck befugt ist.

(3) Unterliegt die Verarbeitung von personenbezogenen Daten besonderen Bedingungen, so hat die übermittelnde zuständige Behörde den Empfänger der personenbezogenen Daten darauf hinzuweisen, dass diese Bedingungen gelten und einzuhalten sind. Die Übermittlung an Empfänger in anderen Mitgliedstaaten oder nach Titel V Kapitel 4 und 5 AEUV errichtete Einrichtungen und sonstige Stellen darf keinen Bedingungen unterworfen werden, die nicht auch für entsprechende Datenübermittlungen im Inland gelten.

Automatisierte Entscheidungsfindung im Einzelfall

§ 41. (1) Ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidungen einschließlich Profiling, die für die betroffene Person nachteilige Rechtsfolgen haben oder sie erheblich beeinträchtigen können, sind nur zulässig, soweit sie gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, ausdrücklich vorgesehen sind.

(2) Entscheidungen nach Abs. 1 dürfen nur auf besonderen Kategorien personenbezogener Daten nach § 39 beruhen, wenn und soweit wirksame Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

(3) Entscheidungen nach Abs. 1, die zur Folge haben, dass natürliche Personen auf Grundlage von personenbezogenen Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung diskriminiert werden, sind verboten.

2. Abschnitt

Rechte der betroffenen Person

Grundsätze

§ 42. (1) Der Verantwortliche hat der betroffenen Person alle Informationen und Mitteilungen gemäß §§ 43 bis 45, die sich auf die Verarbeitung beziehen, in möglichst präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die Informationen sind in geeigneter Form, im Falle eines Antrags nach Möglichkeit in der gleichen Form wie der Antrag, zu übermitteln.

(2) Der Verantwortliche hat den betroffenen Personen die Ausübung der ihnen gemäß §§ 43 bis 45 zustehenden Rechte zu erleichtern.

(3) Der Verantwortliche hat die betroffene Person unverzüglich schriftlich darüber in Kenntnis zu setzen, wie mit ihrem Antrag verfahren wurde.

(4) Der Verantwortliche stellt der betroffenen Person Informationen über die aufgrund eines Antrags gemäß §§ 44 bis 45 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(5) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(6) Informationen gemäß § 43 sowie alle Mitteilungen und Maßnahmen gemäß den §§ 44 und 45 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder

1. ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder
2. sich weigern, aufgrund des Antrags tätig zu werden.

Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(7) Der Verantwortliche kann zur Bestätigung der Identität der Person, die einen Antrag gemäß §§ 44 oder 45 gestellt hat, erforderliche zusätzliche Informationen verlangen.

(8) In den Fällen der §§ 43 Abs. 4, 44 Abs. 3 und 45 Abs. 4 ist die betroffene Person berechtigt, eine Überprüfung der Rechtmäßigkeit der bezüglichen Einschränkung ihrer Rechte durch die Datenschutzbehörde zu verlangen. Der Verantwortliche hat die betroffene Person über dieses Recht zu unterrichten.

(9) Wird das in Abs. 8 genannte Recht ausgeübt, hat die Datenschutzbehörde die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen oder eine Überprüfung durch die Datenschutzbehörde erfolgt sind. Die Datenschutzbehörde hat zudem die betroffene Person über ihr Recht zu unterrichten, Beschwerde an das Bundesverwaltungsgericht zu erheben.

Information der betroffenen Person

§ 43. (1) Der Verantwortliche hat der betroffenen Person zumindest die folgenden Informationen zur Verfügung zu stellen:

1. den Namen und die Kontaktdaten des Verantwortlichen,
2. gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten,
3. die Zwecke, für die die personenbezogenen Daten verarbeitet werden,
4. das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,
5. das Bestehen eines Rechts auf Auskunft und Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung der personenbezogenen Daten der betroffenen Person durch den Verantwortlichen.

(2) Zusätzlich zu den in Abs. 1 genannten Informationen hat der Verantwortliche der betroffenen Person in besonderen Fällen die folgenden zusätzlichen Informationen zu erteilen, um die Ausübung der Rechte der betroffenen Person zu ermöglichen:

1. die Rechtsgrundlage der Verarbeitung,
2. die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
3. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten, auch der Empfänger in Drittländern oder in internationalen Organisationen,
4. erforderlichenfalls weitere Informationen, insbesondere wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben werden.

(3) Im Fall der Erhebung der personenbezogenen Daten bei der betroffenen Person müssen der betroffenen Person die Informationen nach den Vorgaben des Abs. 1 und 2 zum Zeitpunkt der Erhebung

vorliegen. In allen übrigen Fällen findet Art. 14 Abs. 3 DSGVO Anwendung. Die Information gemäß Abs. 1 und 2 kann entfallen, wenn die Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Verantwortlichen oder aus Anwendungen anderer Verantwortlicher ermittelt und die Datenverarbeitung durch Gesetz vorgesehen ist.

(4) Die Unterrichtung der betroffenen Person gemäß Abs. 2 kann soweit und solange aufgeschoben, eingeschränkt oder unterlassen werden, wie dies im Einzelfall unbedingt erforderlich und verhältnismäßig ist

1. zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden, insbesondere durch die Behinderung behördlicher oder gerichtlicher Untersuchungen, Ermittlungen oder Verfahren,
2. zum Schutz der öffentlichen Sicherheit,
3. zum Schutz der nationalen Sicherheit,
4. zum Schutz der verfassungsmäßigen Einrichtungen der Republik Österreich,
5. zum Schutz der militärischen Eigensicherung oder
6. zum Schutz der Rechte und Freiheiten anderer.

Auskunftsrecht der betroffenen Person

§ 44. (1) Jede betroffene Person hat das Recht, vom Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie das Recht, Auskunft über personenbezogene Daten und zu folgenden Informationen zu erhalten:

1. die Zwecke der Verarbeitung und deren Rechtsgrundlage,
2. die Kategorien personenbezogener Daten, die verarbeitet werden,
3. die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen,
4. falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
5. das Bestehen eines Rechts auf Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung personenbezogener Daten der betroffenen Person durch den Verantwortlichen,
6. das Bestehen eines Beschwerderechts bei der Datenschutzbehörde sowie deren Kontaktdaten und
7. Mitteilung zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten.

(2) Einschränkungen des Auskunftsrechts sind nur unter den in § 43 Abs. 4 angeführten Voraussetzungen zulässig.

(3) Im Falle einer Nichterteilung der Auskunft gemäß Abs. 2 hat der Verantwortliche die betroffene Person unverzüglich schriftlich über die Verweigerung oder die Einschränkung der Auskunft und die Gründe hierfür zu unterrichten. Dies gilt nicht, wenn die Erteilung dieser Informationen einem der in § 43 Abs. 4 genannten Zwecke zuwiderliefe. Der Verantwortliche hat die betroffene Person über die Möglichkeit zu unterrichten, Beschwerde bei der Datenschutzbehörde einzulegen.

(4) Der Verantwortliche hat die Gründe für die Entscheidung über die Nichterteilung der Auskunft gemäß Abs. 2 zu dokumentieren. Diese Angaben sind der Datenschutzbehörde zur Verfügung zu stellen.

(5) In dem Umfang, in dem eine Datenverarbeitung für eine betroffene Person hinsichtlich der zu ihr verarbeiteten Daten von Gesetzes wegen einsehbar ist, hat diese das Recht auf Auskunft nach Maßgabe der das Einsichtsrecht vorsehenden Bestimmungen. Für das Verfahren der Einsichtnahme (einschließlich deren Verweigerung) gelten die näheren Regelungen des Gesetzes, das das Einsichtsrecht vorsieht. In Abs. 1 genannte Bestandteile einer Auskunft, die vom Einsichtsrecht nicht umfasst sind, können dennoch nach diesem Bundesgesetz geltend gemacht werden.

Recht auf Berichtigung oder Löschung personenbezogener Daten und auf Einschränkung der Verarbeitung

§ 45. (1) Jede betroffene Person hat das Recht, vom Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten sowie die Vervollständigung unvollständiger personenbezogener Daten zu verlangen. Die Berichtigung oder Vervollständigung kann erforderlichenfalls mittels einer ergänzenden Erklärung erfolgen, soweit eine nachträgliche Änderung mit dem Dokumentationszweck unvereinbar ist. Der Beweis der Richtigkeit der Daten obliegt dem

Verantwortlichen, soweit die personenbezogenen Daten nicht ausschließlich aufgrund von Angaben der betroffenen Person ermittelt wurden.

(2) Der Verantwortliche hat personenbezogene Daten aus eigenem oder über Antrag der betroffenen Person unverzüglich zu löschen, wenn

1. die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind,
2. die personenbezogenen Daten unrechtmäßig verarbeitet wurden oder
3. die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

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

1. die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, oder
2. die personenbezogenen Daten für Beweis Zwecke im Rahmen der Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe weiter aufbewahrt werden müssen.

Im Falle einer Einschränkung gemäß Z 1 hat der Verantwortliche die betroffene Person vor einer Aufhebung der Einschränkung zu unterrichten.

(4) Der Verantwortliche hat die betroffene Person schriftlich über eine Verweigerung der Berichtigung oder Löschung personenbezogener Daten oder eine Einschränkung der Verarbeitung und über die Gründe für die Verweigerung zu unterrichten. Der Verantwortliche hat die betroffene Person über die Möglichkeit zu unterrichten, bei der Datenschutzbehörde Beschwerde einzulegen.

(5) Der Verantwortliche hat die Berichtigung von unrichtigen personenbezogenen Daten der zuständigen Behörde, von der die unrichtigen personenbezogenen Daten stammen, mitzuteilen.

(6) In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung gemäß Abs. 1 bis 3 hat der Verantwortliche alle Empfänger der betroffenen personenbezogenen Daten in Kenntnis zu setzen. Die Empfänger sind verpflichtet, die ihrer Verantwortung unterliegenden personenbezogenen Daten unverzüglich zu berichtigen, löschen oder deren Verarbeitung einschränken.

(Anm.: Abs. 7 aufgehoben durch Z 22, BGBl. I Nr. 24/2018)

3. Abschnitt

Verantwortlicher und Auftragsverarbeiter

Pflichten des Verantwortlichen

§ 46. Der Verantwortliche hat die in Art. 24 Abs. 1 und 2 sowie Art. 25 Abs. 1 und 2 DSGVO angeführten Verpflichtungen in Bezug auf die Übereinstimmung der Verarbeitung mit den Bestimmungen dieses Hauptstücks einzuhalten.

Gemeinsam Verantwortliche

§ 47. Zwei oder mehr Verantwortliche, die gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen, sind gemeinsam Verantwortliche. Sie haben in einer Vereinbarung in transparenter Form ihre jeweiligen Aufgaben nach diesem Bundesgesetz festzulegen, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß § 43 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht gesetzlich festgelegt sind. In der Vereinbarung ist eine Anlaufstelle für die betroffenen Personen anzugeben.

Auftragsverarbeiter und Aufsicht über die Verarbeitung

§ 48. (1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieses Bundesgesetzes erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen in Anspruch.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder aufgrund ausdrücklicher gesetzlicher Ermächtigung, der oder das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in

dem 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 festgelegt sind. Dieser Vertrag oder dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

1. die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Unionsrecht oder durch Gesetze, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
2. gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
3. alle gemäß § 54 erforderlichen Maßnahmen ergreift;
4. die in den Abs. 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
5. angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in diesem Hauptstück genannten Rechte der betroffenen Person nachzukommen;
6. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 52 bis 56 genannten Pflichten unterstützt;
7. nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder aufgrund von Gesetzen eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
8. dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Abs. 1 bis 6 niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Im Hinblick auf Z 8 informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen dieses Hauptstück oder gegen andere Datenschutzbestimmungen der Union oder gesetzliche Datenschutzbestimmungen verstößt.

(4) 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 nach dem Unionsrecht oder aufgrund von Gesetzen dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Abs. 3 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 Anforderungen dieses Hauptstücks 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) Der Vertrag oder das andere Rechtsinstrument im Sinne der Abs. 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(6) Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder aufgrund von Gesetzen zur Verarbeitung verpflichtet sind.

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

Verzeichnis von Verarbeitungstätigkeiten

§ 49. (1) Jeder Verantwortliche hat sinngemäß nach Maßgabe des Art. 30 Abs. 1 bis 4 DSGVO ein Verzeichnis von Verarbeitungstätigkeiten zu führen, wobei sich die Verweise in Art. 30 Abs. 1 lit. g und

Abs. 2 lit. d DSGVO auf § 54 beziehen und die Bezugnahme auf einen Vertreter des Verantwortlichen oder des Auftragsverarbeiters gegenstandslos ist.

(2) Das Verzeichnis gemäß Abs. 1 hat auch Angaben zu enthalten über

1. die Verwendung von Profiling, wenn eine solche Verwendung vorgenommen wird, und
2. die Rechtsgrundlage der Verarbeitung, einschließlich der Übermittlungen, für die die personenbezogenen Daten bestimmt sind.

(3) Jeder Auftragsverarbeiter hat ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Verarbeitungstätigkeiten zu führen, das Folgendes enthält:

1. Name und Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie eines etwaigen 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 vom Verantwortlichen entsprechend angewiesen, einschließlich der Identifizierung des Drittlandes oder der internationalen Organisation,
4. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 54 Abs. 1.

Protokollierung

§ 50. (1) Jeder Verarbeitungsvorgang ist in geeigneter Weise so zu protokollieren, dass die Zulässigkeit der Verarbeitung nachvollzogen und überprüft werden kann.

(2) In automatisierten Verarbeitungssystemen sind alle Verarbeitungsvorgänge in automatisierter Form zu protokollieren. Aus diesen Protokolldaten müssen zumindest der Zweck, die verarbeiteten Daten, das Datum und die Uhrzeit der Verarbeitung, die Identifizierung der Person, die die personenbezogenen Daten verarbeitet hat, sowie die Identität eines allfälligen Empfängers solcher personenbezogenen Daten hervorgehen.

(3) In nicht automatisierten Verarbeitungssystemen sind zumindest Abfragen und Offenlegungen einschließlich Übermittlungen, Veränderungen sowie Löschungen zu protokollieren. Für diese Protokolldaten gilt Abs. 2 zweiter Satz.

(4) Die Protokolle dürfen ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung einschließlich der Eigenüberwachung, der Gewährleistung von Integrität und Sicherheit der personenbezogenen Daten sowie in gerichtlichen Strafverfahren verwendet werden.

(5) Der Verantwortliche und der Auftragsverarbeiter haben der Datenschutzbehörde auf deren Verlangen die Protokolle zur Verfügung zu stellen.

Zusammenarbeit mit der Datenschutzbehörde

§ 51. Der Verantwortliche und der Auftragsverarbeiter sind verpflichtet, über Aufforderung mit der Datenschutzbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten.

Datenschutz-Folgenabschätzung

§ 52. Der Verantwortliche hat zum Schutz der Rechte und berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener eine Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 1, 2, 3, 7 und 11 DSGVO durchzuführen, wobei sich der Nachweis gemäß Art. 35 Abs. 7 lit. d DSGVO auf die Einhaltung der Vorgaben dieses Hauptstücks bezieht.

Vorherige Konsultation der Datenschutzbehörde

§ 53. Der Verantwortliche hat nach Maßgabe des Art. 36 DSGVO vor der Verarbeitung personenbezogener Daten in neu anzulegenden Dateisystemen die Datenschutzbehörde zu konsultieren, wobei sich die Verweise in Art. 36 Abs. 1 und Abs. 3 lit. e DSGVO auf § 52 und der Verweis auf die Bestimmungen hinsichtlich der Befugnisse der Datenschutzbehörde in Art. 36 Abs. 2 DSGVO auf § 33 beziehen und die in Art. 36 Abs. 2 DSGVO angeführten Maßnahmen innerhalb von sechs Wochen mit der Möglichkeit einer Verlängerung um einen weiteren Monat zu treffen sind.

Datensicherheitsmaßnahmen

§ 54. (1) Der Verantwortliche und der Auftragsverarbeiter haben 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 des Risikos für die Rechte und Freiheiten natürlicher Personen, unter Berücksichtigung der unterschiedlichen Kategorien gemäß § 37, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko

angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 39.

(2) Der Verantwortliche und der Auftragsverarbeiter haben im Hinblick auf die automatisierte Verarbeitung nach einer Risikobewertung Maßnahmen zu ergreifen, um folgende Zwecke zu erreichen:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle);
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle);
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle);
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle);
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugriffskontrolle);
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle);
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle);
8. Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle);
9. Gewährleistung, dass eingesetzte Systeme im Störfall 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).

Meldung von Verletzungen an die Datenschutzbehörde

§ 55. (1) Der Verantwortliche hat nach Maßgabe des Art. 33 DSGVO Verletzungen des Schutzes personenbezogener Daten der Datenschutzbehörde zu melden.

(2) Soweit von der Verletzung des Schutzes personenbezogener Daten betroffen sind, die von dem oder an den Verantwortlichen eines anderen Mitgliedstaates der Europäischen Union übermittelt wurden, sind die in Art. 33 Abs. 3 DSGVO genannten Informationen dem Verantwortlichen jenes Mitgliedstaates der Europäischen Union unverzüglich zu übermitteln.

Benachrichtigung der betroffenen Person von Verletzungen

§ 56. (1) Der Verantwortliche hat nach Maßgabe des Art. 34 DSGVO betroffene Personen von Verletzungen des Schutzes ihrer personenbezogenen Daten zu benachrichtigen.

(2) Die Benachrichtigung gemäß Abs. 1 kann unter den in § 43 Abs. 4 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden.

Benennung, Stellung und Aufgaben des Datenschutzbeauftragten

§ 57. (1) Jeder Verantwortliche hat nach Maßgabe des Art. 37 Abs. 5 und 7 DSGVO einen Datenschutzbeauftragten zu benennen. Gerichte sind im Rahmen ihrer justiziellen Tätigkeit von der Verpflichtung zur Benennung eines Datenschutzbeauftragten ausgenommen. § 5 gilt im Hinblick auf die Bestimmungen dieses Hauptstücks sinngemäß.

(2) Für die Stellung des Datenschutzbeauftragten gilt Art. 38 DSGVO.

(3) Dem Datenschutzbeauftragten obliegen die in Art. 39 DSGVO genannten Aufgaben in Bezug auf die Einhaltung der Bestimmungen dieses Hauptstücks.

(4) Der Verantwortliche hat die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und der Datenschutzbehörde mitzuteilen.

4. Abschnitt

Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen

Allgemeine Grundsätze für die Übermittlung personenbezogener Daten

§ 58. (1) Eine Übermittlung von personenbezogenen Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, durch zuständige Behörden ist nur zulässig, wenn die Bestimmungen dieses Hauptstücks eingehalten werden und

1. die Übermittlung für die in § 36 Abs. 1 genannten Zwecke erforderlich ist,
2. die personenbezogenen Daten an einen Verantwortlichen in einem Drittland oder einer internationalen Organisation, die eine für die in § 36 Abs. 1 genannten Zwecke zuständige Behörde ist, übermittelt werden,
3. in Fällen, in denen personenbezogene Daten aus einem anderen Mitgliedstaat der EU übermittelt oder zur Verfügung gestellt werden, dieser Mitgliedstaat die Übermittlung zuvor genehmigt hat,
4. die Europäische Kommission gemäß § 59 Abs. 1 und 2 einen Angemessenheitsbeschluss gefasst hat oder, wenn kein solcher Beschluss vorliegt, geeignete Garantien im Sinne des § 59 Abs. 3 bis 5 erbracht wurden oder bestehen oder, wenn kein Angemessenheitsbeschluss gemäß § 59 Abs. 1 und 2 vorliegt und keine geeigneten Garantien im Sinne des § 59 Abs. 3 bis 5 vorhanden sind, Ausnahmen für bestimmte Fälle gemäß § 59 Abs. 6 und 7 anwendbar sind und
5. sichergestellt ist, dass eine Weiterübermittlung an ein anderes Drittland oder eine andere internationale Organisation nur aufgrund einer vorherigen Genehmigung der zuständigen Behörde, die die ursprüngliche Übermittlung durchgeführt hat, und unter gebührender Berücksichtigung sämtlicher maßgeblicher Faktoren, einschließlich der Schwere der Straftat, des Zwecks der ursprünglichen Übermittlung personenbezogener Daten und des Schutzniveaus für personenbezogene Daten in dem Drittland oder der internationalen Organisation, an das bzw. die personenbezogene Daten weiterübermittelt werden, zulässig ist.

(2) Eine Übermittlung ohne vorherige Genehmigung gemäß Abs. 1 Z 3 ist nur zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Die für die Erteilung der vorherigen Genehmigung zuständige Behörde ist unverzüglich zu unterrichten.

(3) Ersucht eine zuständige Behörde eines anderen Mitgliedstaates der EU um Genehmigung zur Übermittlung von personenbezogenen Daten, die ursprünglich aus dem Inland übermittelt wurden, an ein Drittland oder eine internationale Organisation gemäß Abs. 1 Z 3, so ist zur Erteilung dieser Genehmigung jene zuständige Behörde zuständig, die die personenbezogenen Daten ursprünglich übermittelt hat, soweit nicht gesetzlich anderes angeordnet ist.

Datenübermittlung an Drittländer oder internationale Organisationen

§ 59. (1) Die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation ist zulässig, wenn die Europäische Kommission gemäß Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 im Wege eines Durchführungsaktes beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung. Die Genehmigungspflicht gemäß § 58 Abs. 1 Z 3 bleibt davon unberührt.

(2) Übermittlungen personenbezogener Daten an ein Drittland, an ein Gebiet oder einen oder mehrere spezifischen Sektoren in einem Drittland oder an eine internationale Organisation gemäß den Abs. 3 bis 8 werden durch einen gemäß Art. 36 Abs. 5 der Richtlinie (EU) 2016/680 gefassten Beschluss der Europäischen Kommission zum Widerruf, zur Änderung oder zur Aussetzung eines Beschlusses nach Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 nicht berührt.

(3) Liegt kein Beschluss nach Abs. 1 vor, so ist die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder
2. der Verantwortliche auf Grund einer Beurteilung der für die Übermittlung personenbezogener Daten maßgeblichen Umstände zu der Auffassung gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen.

(4) Bestehen geeignete Garantien gemäß Abs. 3 Z 2 für Kategorien von Übermittlungen, so hat der Verantwortliche die Datenschutzbehörde über diese Kategorien zu unterrichten.

(5) Übermittlungen gemäß Abs. 3 Z 2 sind zu dokumentieren und die Dokumentation einschließlich Datum und Zeitpunkt der Übermittlung, Informationen über die empfangende zuständige Behörde, Begründung der Übermittlung und übermittelte personenbezogenen Daten, der Datenschutzbehörde auf Anforderung zur Verfügung zu stellen.

(6) Wenn weder ein Angemessenheitsbeschluss gemäß Abs. 1 bis 2 vorliegt noch geeignete Garantien gemäß Abs. 3 bis 5 vorhanden sind, so ist nach Maßgabe des Abs. 5 eine Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer Person,
2. wenn dies zur Wahrung berechtigter Interessen der betroffenen Person gesetzlich vorgesehen ist,
3. zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaates der EU oder eines Drittlandes,
4. im Einzelfall für die in § 36 Abs. 1 genannten Zwecke, oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 36 Abs. 1 genannten Zwecken.

(7) In den Fällen des Abs. 6 Z 4 und 5 ist die Übermittlung nur zulässig, wenn keine das öffentliche Interesse an der Übermittlung überwiegenden Grundrechte und Grundfreiheiten der betroffenen Person der Übermittlung entgegenstehen.

4. Hauptstück Besondere Strafbestimmungen

Verwaltungsstrafbestimmung

§ 62. (1) Sofern die Tat nicht einen Tatbestand nach Art. 83 DSGVO verwirklicht oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 50 000 Euro zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenverarbeitung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält,
2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 6) übermittelt, insbesondere Daten, die ihm gemäß §§ 7 oder 8 anvertraut wurden, vorsätzlich für andere unzulässige Zwecke verarbeitet,
3. sich unter Vortäuschung falscher Tatsachen vorsätzlich personenbezogene Daten gemäß § 10 verschafft,
4. eine Bildverarbeitung entgegen den Bestimmungen des 3. Abschnittes des 1. Hauptstücks betreibt oder
5. die Einschau gemäß § 22 Abs. 2 verweigert.

(2) Der Versuch ist strafbar.

(3) Gegen juristische Personen können bei Verwaltungsübertretung nach Abs. 1 und 2 Geldbußen nach Maßgabe des § 30 verhängt werden.

(4) Die Strafe des Verfalls von Datenträgern und Programmen sowie Bildübertragungs- und Bildaufzeichnungsgeräten kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 in Zusammenhang stehen.

(5) Die Datenschutzbehörde ist zuständig für Entscheidungen nach Abs. 1 bis 4.

Datenverarbeitung in Gewinn- oder Schädigungsabsicht

§ 63. Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

5. Hauptstück Schlussbestimmungen

Durchführung und Umsetzung von Rechtsakten der EU

§ 64. (1) Dieses Bundesgesetz dient der Durchführung der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1.

(2) Dieses Bundesgesetz dient weiters der Umsetzung der Richtlinie (EU) 2016/680 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. Nr. L 119 vom 4.5.2016 S. 89.

Sprachliche Gleichbehandlung

§ 65. Soweit in diesem Bundesgesetz auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise. Bei der Anwendung der Bezeichnungen auf bestimmte natürliche Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

Erlassung von Verordnungen

§ 66. Verordnungen auf Grund dieses Bundesgesetzes in seiner jeweiligen Fassung dürfen bereits von dem Tag an erlassen werden, der der Kundmachung der durchzuführenden Gesetzesbestimmungen folgt; sie dürfen jedoch nicht vor den durchzuführenden Gesetzesbestimmungen in Kraft treten.

Verweisungen

§ 67. Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

Vollziehung

§ 68. Mit der Vollziehung dieses Bundesgesetzes sind, soweit sie nicht der Bundesregierung obliegt, der Bundesminister für Verfassung, Reformen, Deregulierung und Justiz sowie der Bundeskanzler und die anderen Bundesminister im Rahmen ihres Wirkungsbereichs betraut.

Übergangsbestimmungen

§ 69. (1) Die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes laufende Funktionsperiode des Leiters der Datenschutzbehörde wird bis zu deren Ablauf fortgesetzt. Dies gilt auch für dessen Stellvertreter.

(2) Das von der Datenschutzbehörde geführte Datenverarbeitungsregister ist von der Datenschutzbehörde bis zum 31. Dezember 2019 zu Archivzwecken fortzuführen. Es dürfen keine Eintragungen und inhaltliche Änderungen im Datenverarbeitungsregister vorgenommen werden. Registrierungen im Datenverarbeitungsregister werden gegenstandslos. Jedermann kann in das Register Einsicht nehmen. In den Registrierungsakt einschließlich darin allenfalls enthaltener Genehmigungsbescheide ist Einsicht zu gewähren, wenn der Einsichtswerber glaubhaft macht, dass er eine betroffene Person ist, und soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen des Verantwortlichen (Auftraggebers) oder anderer Personen entgegenstehen.

(3) Gemäß den §§ 17 und 18 Abs. 2 DSG 2000 im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes anhängige Registrierungsverfahren gelten als eingestellt. Im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes anhängige Verfahren nach den §§ 13, 46 und 47 DSG 2000 sind fortzuführen, sofern die Genehmigung nach diesem Bundesgesetz oder der DSGVO erforderlich ist. Anderenfalls gelten sie als eingestellt.

(4) Zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bei der Datenschutzbehörde oder bei den ordentlichen Gerichten zum Datenschutzgesetz 2000 anhängige Verfahren sind nach den Bestimmungen dieses Bundesgesetzes und der DSGVO fortzuführen, mit der Maßgabe, dass die Zuständigkeit der ordentlichen Gerichte aufrecht bleibt.

(5) Verletzungen des Datenschutzgesetzes 2000, die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes noch nicht anhängig gemacht wurden, sind nach der Rechtslage nach Inkrafttreten dieses Bundesgesetzes zu beurteilen. Ein strafbarer Tatbestand, der vor dem Inkrafttreten dieses Bundesgesetzes verwirklicht wurde, ist nach jener Rechtslage zu beurteilen, die für den Täter in ihrer Gesamtauswirkung günstiger ist; dies gilt auch für das Rechtsmittelverfahren.

(6) Die Eingaben der betroffenen Personen nach § 24 sind von den Verwaltungsabgaben des Bundes befreit.

(7) Die entsendenden Stellen haben eine dem § 15 Abs. 1 Z 1 bis 6 entsprechende Anzahl von Mitgliedern und Ersatzmitgliedern des Datenschutzrates dem Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz innerhalb von zwei Wochen ab dem 25. Mai 2018 schriftlich bekannt zu geben. Die konstituierende Sitzung des Datenschutzrates hat innerhalb von sechs Wochen ab dem 25. Mai 2018 zu erfolgen. Bis zur Wahl des neuen Vorsitzenden und der beiden stellvertretenden Vorsitzenden bleiben der bisherige Vorsitzende sowie die beiden bisherigen stellvertretenden Vorsitzenden in ihrer Funktion.

(8) Besondere Bestimmungen über die Verarbeitung von personenbezogenen Daten in anderen Bundes- oder Landesgesetzen bleiben unberührt.

(9) Vor Inkrafttreten dieses Bundesgesetzes nach §§ 13, 46 und 47 DSGVO 2000 rechtskräftig erteilte Genehmigungen der Datenschutzbehörde bleiben unberührt. Nach dem Datenschutzgesetz 2000 erteilte Zustimmungen bleiben aufrecht, sofern sie den Vorgaben der DSGVO entsprechen.

Inkrafttreten

§ 70. (1) Die übrigen Bestimmungen dieses Bundesgesetzes treten ebenfalls mit 1. Jänner 2000 in Kraft.

(2) §§ 26 Abs. 6 und 52 Abs. 1 und 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 136/2001 treten mit 1. Jänner 2002 in Kraft.

(3) § 48a Abs. 5 in der Fassung des Bundesgesetzes BGBl. I Nr. 135/2009 tritt mit 1. Jänner 2010 in Kraft.

(4) Das Inhaltsverzeichnis, § 4 Abs. 1 Z 4, 5, 7 bis 9, 11 und 12, § 8 Abs. 1, 2 und 4, § 12 Abs. 1, die Ummummerierung der Absätze in § 13, § 16 Abs. 1 und 3, § 17 Abs. 1, 1a und 4, § 19 Abs. 1 Z 3a und Abs. 2, die Ummummerierung der Absätze in § 19, die §§ 20 bis 22a samt Überschriften, § 24 Abs. 2a, § 24 Abs. 4, § 26 Abs. 1 bis 8 und 10, § 28 Abs. 3, § 30 Abs. 2a, 5 bis 6a, die §§ 31 und 31a samt Überschriften, § 32 Abs. 1, 4, 6 und 7, § 34 Abs. 1, 3 und 4, § 36 Abs. 3, 3a und 9, § 39 Abs. 5, § 40 Abs. 1 und 2, § 41 Abs. 2 Z 4a, § 42 Abs. 1 Z 1, § 42 Abs. 5, § 46 Abs. 1 Z 2 und 3, Abs. 2 bis 3a, § 47 Abs. 4, § 49 Abs. 3, § 50 Abs. 1 bis 2a, der 9a. Abschnitt, § 51, § 52 Abs. 2 und 4, § 55, § 61 Abs. 6 bis 9 sowie § 64 in der Fassung des Bundesgesetzes BGBl. I Nr. 133/2009 treten mit 1. Jänner 2010 in Kraft. Gleichzeitig treten § 4 Abs. 1 Z 10, § 13 Abs. 3 sowie § 51 Abs. 2 außer Kraft.

(5) § 36 Abs. 6 in der Fassung des Bundesgesetzes BGBl. I Nr. 133/2009 tritt am 1. Juli 2010 in Kraft.

(6) § 37 Abs. 2, § 38 Abs. 2 und § 61 Abs. 9 in der Fassung des Bundesgesetzes BGBl. I Nr. 57/2013 treten mit 1. Mai 2013 in Kraft.

(7) Das Inhaltsverzeichnis, § 5 Abs. 4, § 10 Abs. 2, § 12 Abs. 4, § 13 Abs. 1, 2 Z 2, Abs. 3, 4 und 6, § 16 Abs. 1, § 17 Abs. 1, § 18 Abs. 2, § 19 Abs. 1 Z 6 und Abs. 2, § 20 Abs. 2 und 5 Z 2, § 21 Abs. 1 Z 3, § 22 Abs. 2 bis 4, § 22a Abs. 1, 3 bis 5, § 23 Abs. 2, § 26 Abs. 2, 5 und 7, § 27 Abs. 5 und 7, die Überschrift zu § 30, § 30 Abs. 1, 2, 2a, 4 bis 6a, die Überschrift zu § 31, § 31 Abs. 1, 2, 5, 6 und 8, § 31a, § 32 Abs. 5 bis 7, § 34 Abs. 3 und 4, die Überschrift zu § 35, § 35 Abs. 1, §§ 36 bis 40 samt Überschriften, § 41 Abs. 2 Z 1, § 44 Abs. 6 und 8, § 46 Abs. 2 Z 3 und Abs. 3, § 47 Abs. 3 und 4, § 48a Abs. 2, § 50 Abs. 1 und 2, § 50b Abs. 2, § 50c Abs. 1, § 52 Abs. 2 Z 2 und 3 sowie Abs. 5, § 54 Abs. 2 und § 61 Abs. 8 bis 10 in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013 treten mit 1. Jänner 2014 in Kraft. Gleichzeitig treten § 41 Abs. 2 Z 4a und die DSK-Vergütungsverordnung, BGBl. II Nr. 145/2006, außer Kraft. Die für die Bestellung des Leiters der Datenschutzbehörde und seines Stellvertreters notwendigen organisatorischen und personellen Maßnahmen können bereits vor Inkrafttreten des Bundesgesetzes BGBl. I Nr. 83/2013 getroffen werden.

(8) **(Verfassungsbestimmung)** § 2 Abs. 2 und § 35 Abs. 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013 treten mit 1. Jänner 2014 in Kraft.

(9) Der Titel, das Inhaltsverzeichnis, das 1. Hauptstück, die Bezeichnung und Überschrift des 2. Hauptstücks, der 1., 2., 3. und 4. Abschnitt, die Überschrift und Bezeichnung des 5. Abschnittes, § 35 Abs. 1, die Bezeichnung und Überschrift des 3. Hauptstücks, der 1., 2. und 3. Abschnitt, die Überschrift und Bezeichnung des 4. Abschnittes, die §§ 58 und 59 samt Überschriften sowie das 4. und 5. Hauptstück in der Fassung des Bundesgesetzes BGBl. I Nr. 120/2017 treten mit 25. Mai 2018 in Kraft. Im Art. 2 treten der 1., 2., 3., 4., 5 und 6. Abschnitt, die Bezeichnung und die Überschrift des 7. Abschnittes, die Überschrift zu § 35, die §§ 36 bis 44 samt Überschriften, der 8., 9., 9a. und 10. Abschnitt, die Bezeichnung und die Überschrift des 11. Abschnittes, die §§ 53 bis 59 samt Überschriften, § 61 Abs. 1

bis 3 und 5 bis 10 sowie die §§ 62 bis 64 samt Überschriften in der Fassung vor der Novelle BGBl. I Nr. 120/2017 mit Ablauf des 24. Mai 2018 außer Kraft.

(10) Die Standard- und Muster-Verordnung 2004 – StMV 2004, BGBl. II Nr. 312/2004, die Datenverarbeitungsregister-Verordnung 2012 – DVRV 2012, BGBl. II Nr. 257/2012, und die Datenschutzangemessenheits-Verordnung – DSAV, BGBl. II Nr. 521/1999, treten mit Ablauf des 24. Mai 2018 außer Kraft.

(11) **(Verfassungsbestimmung)** § 35 Abs. 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 23/2018 tritt mit 25. Mai 2018 in Kraft.

(12) Das Inhaltsverzeichnis, § 4 Abs. 1, 5 bis 7, § 5 Abs. 3 erster Satz und Abs. 5, § 9 samt Überschrift, § 11 samt Überschrift, § 12 Abs. 3 Z 2 und Abs. 4 Z 3, § 14 Abs. 1, § 15 Abs. 1 Z 5, Abs. 3, Abs. 5 Z 1 und 2, Abs. 6, 7 und 8, § 16 Abs. 3 Z 2 und Abs. 5, § 19 Abs. 2 und 3, § 23 Abs. 1, § 26 Abs. 1, § 28, § 30 Abs. 3 und 5, § 32 Abs. 1 Z 1, § 36 Abs. 1 und 2 Z 7, § 44 Abs. 2, § 49 Abs. 1 und 3, § 56 Abs. 1, § 64 Abs. 2, § 68 sowie § 69 Abs. 5 und 7 in der Fassung des Bundesgesetzes BGBl. I Nr. 24/2018 treten mit 25. Mai 2018 in Kraft. Gleichzeitig tritt § 45 Abs. 7 in der Fassung vor der Novelle BGBl. I Nr. 24/2018 außer Kraft. § 70 Abs. 1 bis 8 in der Fassung des Bundesgesetzes BGBl. I Nr. 24/2018 tritt mit dem auf die Kundmachung folgenden Tag in Kraft. Soweit sich die im Bundesgesetz BGBl. I Nr. 24/2018 getroffenen Anordnungen auf durch das Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017, geschaffene Vorschriften beziehen, gehen die Regelungen des Bundesgesetzes BGBl. I Nr. 24/2018 jenen des Datenschutz-Anpassungsgesetzes 2018, BGBl. I Nr. 120/2017, vor.

(13) § 16 Abs. 5 und § 70 Abs. 6, 7, 9, 10 und 12 in der Fassung des Bundesgesetzes BGBl. I Nr. 14/2019 treten mit Ablauf des Tages der Kundmachung dieses Bundesgesetzes in Kraft; gleichzeitig treten die Einträge zu den §§ 60 und 61 im Inhaltsverzeichnis außer Kraft. Die Einträge zu den §§ 2 und 3 im Inhaltsverzeichnis und § 4 Abs. 7 treten mit 1. Jänner 2020 außer Kraft.

(14) **(Verfassungsbestimmung)** Die §§ 2 und 3 samt Überschriften treten mit Ablauf des 31. Dezember 2019 außer Kraft. § 70 Abs. 8 und 11 in der Fassung des Bundesgesetzes BGBl. I Nr. 14/2019 tritt mit Ablauf des Tages der Kundmachung dieses Bundesgesetzes in Kraft; gleichzeitig tritt § 61 samt Überschrift außer Kraft.

14 Text der Datenschutz-Folgenabschätzung- Ausnahmenverordnung

BUNDESGESETZBLATT

FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2018
Ausgegeben am 25. Mai 2018
Teil II

108. Verordnung: Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV)

108. Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV)

Auf Grund des § 21 Abs. 2 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 120/2017, wird verordnet:

Ausnahmen von der Datenschutz-Folgenabschätzung

§ 1. (1) Die in der **Anlage** angeführten Datenverarbeitungen sind von der Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 1 und 5 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1, (im Folgenden: DSGVO) ausgenommen.

(2) Ebenso sind Datenanwendungen, die

1. gemäß § 18 Abs. 2 und § 50c Abs. 1 des Datenschutzgesetzes 2000 (DSG 2000), BGBl. I Nr. 165/1999 in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013, der Vorabkontrolle unterlagen und vor Ablauf des 24. Mai 2018 im Datenverarbeitungsregister registriert wurden, oder

2. gemäß § 17 Abs. 2 Z 6 DSG 2000 nicht meldepflichtig waren,

von der Datenschutz-Folgenabschätzung ausgenommen, sofern diese Datenanwendungen mit Ablauf des 24. Mai 2018 den Vorgaben der DSGVO entsprechen und ab dem Inkrafttreten dieser Verordnung keine wesentlichen Änderungen vorgenommen werden.

Personenbezogene Bezeichnungen

§ 2. Bei den in dieser Verordnung verwendeten personenbezogenen Bezeichnungen gilt die gewählte Form für beide Geschlechter.

Inkrafttreten

§ 3. Diese Verordnung tritt mit 25. Mai 2018 in Kraft.

Jelinek

Anlage

Inhaltsverzeichnis

| | |
|----------|--|
| DSFA-A01 | Kundenverwaltung, Rechnungswesen, Logistik, Buchführung |
| DSFA-A02 | Personalverwaltung |
| DSFA-A03 | Mitgliederverwaltung |
| DSFA-A04 | Kundenbetreuung und Marketing für eigene Zwecke |
| DSFA-A05 | Sach- und Inventarverwaltung |
| DSFA-A06 | Register, Evidenzen, Bücher |
| DSFA-A07 | Zugriffsverwaltung für EDV-Systeme |
| DSFA-A08 | Zutrittskontrollsysteme |
| DSFA-A09 | Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung) |

| | |
|----------|---|
| DSFA-A10 | Bild- und Akustikdatenverarbeitung in Echtzeit |
| DSFA-A11 | Bild- und Akustikverarbeitungen zu Dokumentationszwecken |
| DSFA-A12 | Patienten-/Klienten-/Kundenverwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdiensteanbieter und Apotheken |
| DSFA-A13 | Rechts- und Beratungsberufe |
| DSFA-A14 | Archivierung, wissenschaftliche Forschung und Statistik |
| DSFA-A15 | Unterstützungsbekundungen |
| DSFA-A16 | Haushaltsführung der Gebietskörperschaften und sonstigen juristischen Personen öffentlichen Rechts |
| DSFA-A17 | Öffentliche Abgabenverwaltung |
| DSFA-A18 | Förderverwaltung |
| DSFA-A19 | Öffentlichkeitsarbeit und Informationstätigkeit durch öffentliche Funktionsträger und deren Geschäftsapparate |
| DSFA-A20 | Aktenverwaltung (Büroautomation) und Verfahrensführung |
| DSFA-A21 | Organisation von Veranstaltungen |
| DSFA-A22 | Preise und Ehrungen |

DSFA-A01 Kundenverwaltung, Rechnungswesen, Logistik, Buchführung

Zweck der Datenverarbeitung:

Verarbeitung personenbezogener Daten im Rahmen jeglicher Geschäftsbeziehung mit Kunden und Lieferanten samt systematischer Aufzeichnung aller die Einnahmen und Ausgaben betreffenden Geschäftsvorgänge.

Verarbeitungstätigkeiten von Unternehmen, die Daten über Dritte verarbeiten (keine Kunden des Verantwortlichen), mit denen die Unternehmen in keiner Geschäftsbeziehung stehen (etwa Detektivbüros, Inkassobüros oder Kreditauskunfteien), sind von dieser Ausnahme nicht umfasst.

DSFA-A02 Personalverwaltung

Zweck der Datenverarbeitung:

Verarbeitung und Evidenzhaltung personenbezogener Daten für Lohn-, Gehalts-, Entgeltverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, soweit dies auf Grund von Gesetzen oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglicher Verpflichtungen jeweils erforderlich ist;

Verarbeitung und Evidenzhaltung dienstrechtlicher, besoldungsrechtlicher, ausbildungsbezogener und sonstiger mit dem Beschäftigungsverhältnis in unmittelbarem Zusammenhang stehender personenbezogener Daten von öffentlich Bediensteten und sonstigen von Verantwortlichen des öffentlichen Bereichs besoldeten Personen (wie zB von Beamten, Vertragsbediensteten, Personen in Ausbildung, Aushilfskräften, aber auch von Abgeordneten und Funktionären) sowie von Volontären und Zivildienern (jeweils ohne Entgeltbezug) durch die Dienstbehörden und Personalstellen zum Zweck von Einzelpersonalmaßnahmen und statistischer Auswertungen;

Verarbeitung und Evidenzhaltung personenbezogener Daten von Bewerbern, wenn diese Daten vom Betroffenen angegeben wurden.

Eine Verarbeitung von besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 und eine Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO im Rahmen dieser Ausnahme sind ausschließlich aufgrund einer gesetzlichen Ermächtigung oder aufgrund rechtlicher Verpflichtungen zulässig.

DSFA-A03 Mitgliederverwaltung

Zweck der Datenverarbeitung:

Führung von Mitgliederverzeichnissen, Evidenz der Mitglieds- und Förderungsbeiträge, Verkehr mit Mitgliedern oder Förderern von Körperschaften des öffentlichen und privaten Rechts, insbesondere Vereinen und Personengemeinschaften sowie Betreuung von Mitgliedern und Förderern.

DSFA-A04 Kundenbetreuung und Marketing für eigene Zwecke

Zweck der Datenverarbeitung:

Verarbeitung von eigenen oder zugekauften Kunden- und Interessentendaten für die Geschäftsanbahnung betreffend das eigene Lieferungs- oder Leistungsangebot sowie zur Durchführung von Werbemaßnahmen und Newsletter-Versand.

DSFA-A05 Sach- und Inventarverwaltung**Zweck der Datenverarbeitung:**

Inventarverwaltung (Führung von Inventaraufzeichnungen), Unterstützung des Sachgüterausstausches und der Betriebsabrechnung, mit der Inventarverwaltung in Zusammenhang stehende Neben- und Hilfsaufzeichnungen über Lieferanten, Anschaffungskosten sowie Verwaltung der Zuteilung von Hard- und Software an EDV-Systembenutzer.

DSFA-A06 Register, Evidenzen, Bücher**Zweck der Datenverarbeitung:**

Verarbeitung personenbezogener Daten im Rahmen von durch Unions-, Bundes- oder Landesrecht eingerichteten Registern, Evidenzen oder Büchern, sofern keine personenbezogenen Daten im Sinne der Art. 9 und 10 DSGVO verarbeitet werden.

DSFA-A07 Zugriffsverwaltung für EDV-Systeme**Zweck der Datenverarbeitung:**

Verwaltung von Benutzernamen und Passwörtern sowie Systemzugriffsprotokollierung.

DSFA-A08 Zutrittskontrollsysteme**Zweck der Datenverarbeitung:**

Kontrolle der Berechtigung des Zutritts zu Gebäuden und abgegrenzten Bereichen durch den Eigentümer oder Benutzungsberechtigten mit Hilfe von Anlagen, die personenbezogene Daten automationsunterstützt verarbeiten, wobei keine biometrischen Daten von Betroffenen verarbeitet werden. Die bloße Echtzeitwiedergabe von Gesichtsbildern ist von dieser Ausnahme umfasst.

DSFA-A09 Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung)**1. Allgemeine Voraussetzungen für die nachfolgenden Ausnahmen:****a) Räumlicher Erfassungsbereich**

Örtlichkeiten, über welche der Verantwortliche Verfügungsbefugte ist. Die Videoüberwachung darf räumlich nicht über die Liegenschaft hinausreichen, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen im Ausmaß von bis zu einem halben Meter gemessen von der Grundstücksgrenze des überwachten Objekts. Die Videoüberwachung darf überdies nicht an Orten betrieben werden, welche den höchstpersönlichen Lebensbereich von Personen darstellen.

b) Speicherdauer

Aufgenommene personenbezogene Daten sind vom Verantwortlichen spätestens nach 72 Stunden zu löschen, es sei denn eine längere Speicherdauer wurde in einem Gesetz, durch einen behördlichen Rechtsakt, in einer Betriebsvereinbarung oder mit Zustimmung der Personalvertretung ausdrücklich festgelegt.

c) Kennzeichnung

Voraussetzung für die Ausnahme ist die geeignete Kennzeichnung der Bildverarbeitung durch den Verantwortlichen. Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen.

2. Zweck der Datenverarbeitung:**A. Einfamilienhaus samt Grundstück, eigene Wohnung**

Bild- und Akustikverarbeitungen, welche dem vorbeugenden Schutz von Personen oder Sachen auf privaten, zu Wohnzwecken dienenden Liegenschaften, die ausschließlich vom Verantwortlichen und von allen im gemeinsamen Haushalt lebenden Nutzungsberechtigten genutzt werden, dienen. Voraussetzung ist die Einwilligung aller Nutzungsberechtigten.

B. Allgemein zugängliche Örtlichkeiten, die dem Hausrecht des Verantwortlichen unterliegen

Bild- und Akustikverarbeitungen, welche für den vorbeugenden Schutz von Personen oder Sachen an allgemein zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials erforderlich sind und kein gelinderes geeignetes Mittel zur Verfügung steht. In Fällen, in denen Arbeitnehmervertretungen zu bilden sind, ist das Vorliegen einer gültigen Betriebsvereinbarung oder einer gültigen Zustimmung der Personalvertretung, welche die Durchführung der Videoüberwachung regeln, Voraussetzung.

Keine Anwendung findet diese Ausnahme auf Örtlichkeiten, welche aufgrund eines bestehenden Kontrahierungszwanges oder aufgrund des öffentlichen Interesses von jedermann betreten werden dürfen.

DSFA-A10 Bild- und Akustikdatenverarbeitung in Echtzeit

1. Allgemeine Voraussetzungen für die nachfolgende Ausnahme:

a) Räumlicher Erfassungsbereich

Örtlichkeiten, über welche der Verantwortliche verfügungsbefugt ist. Die Bilddatenverarbeitung darf räumlich nicht darüber hinausreichen, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen im Ausmaß von bis zu einem halben Meter. Die Bild- und Akustikdatenverarbeitung darf überdies nicht an Orten betrieben werden, welche den höchstpersönlichen Lebensbereich von Personen darstellen.

b) Kennzeichnung

Voraussetzung für die Ausnahme ist die geeignete Kennzeichnung der Bildverarbeitung durch den Verantwortlichen. Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen.

2. Zweck der Datenverarbeitung:

Bild- und Akustikübertragungen ohne Aufzeichnung.

DSFA-A11 Bild- und Akustikverarbeitungen zu Dokumentationszwecken

Zweck der Datenverarbeitung:

Bild- und Akustikverarbeitungen, welche ausschließlich ein Dokumentationsinteresse verfolgen, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist. Strafrechtliche, verwaltungsstrafrechtliche oder zivilrechtliche Zwecke dürfen im Rahmen dieser Ausnahme nicht verfolgt werden.

DSFA-A12 Patienten-/Klienten-/Kundenverwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdiensteanbieter und Apotheken

Zweck der Datenverarbeitung:

Patientenverwaltung und Honorarabrechnung von einzelnen Ärzten, Zahnärzten und Dentisten sowie Patienten-/Klientenverwaltung und Honorarabrechnung anderer freiberuflich oder gewerblich einzeln tätiger Gesundheitsdiensteanbieter und Apotheken.

DSFA-A13 Rechts- und Beratungsberufe

Zweck der Datenverarbeitung:

Datenverarbeitung von rechtsberatenden und unternehmensberatenden Berufen, wie einzelne Rechtsanwälte, Notare, Patentanwälte, Wirtschaftstreuhänder, Steuerberater und Unternehmensberater im Rahmen ihrer Berufsausübung.

DSFA-A14 Archivierung, wissenschaftliche Forschung und Statistik

Zweck der Datenverarbeitung:

Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke aufgrund besonderer gesetzlicher Vorschriften oder mit Einwilligung der betroffenen Person.

DSFA-A15 Unterstützungsbekundungen

Zweck der Datenverarbeitung:

Verarbeitung personenbezogener Daten im Rahmen von Bürgerinitiativen, Petitionslisten oder Unterschriftensammlungen durch die Organisatoren.

DSFA-A16 Haushaltsführung der Gebietskörperschaften und sonstigen juristischen Personen öffentlichen Rechts

Zweck der Datenverarbeitung:

Erstellung von Voranschlägen, Finanzbuchführung, Zahlungsverkehr, Erstellung von Berichten, Betriebsabrechnungen, Neben- und Hilfsbuchführungen und Auswertung der Daten zur Budgetkontrolle, zu strategischem Controlling und zur Liquiditätssteuerung, Abschlussrechnungen, Jahresabschlüsse sowie Abschlussprüfungen und Rechnungsprüfungen.

DSFA-A17 Öffentliche Abgabenverwaltung**Zweck der Datenverarbeitung:**

Vorschreibung, Einhebung und Abrechnung von öffentlich-rechtlich geregelten Abgaben und Gebühren durch Bund, Länder, Gemeinden, Gemeindeverbände und sonstige Körperschaften des öffentlichen Rechts sowie deren Kontrolle.

DSFA-A18 Förderverwaltung**Zweck der Datenverarbeitung:**

Verarbeitung personenbezogener Daten durch Fördergeber und auszahlende Stellen im Rahmen der Abwicklung öffentlicher Förderungen, sofern keine personenbezogenen Daten im Sinne der Art. 9 und 10 DSGVO verarbeitet werden.

DSFA-A19 Öffentlichkeitsarbeit und Informationstätigkeit durch öffentliche Funktionsträger und deren Geschäftsapparate**Zweck der Datenverarbeitung:**

Verarbeitung von Daten Anfragender im Rahmen des Auskunftspflichtgesetzes, der Öffentlichkeitsarbeit und Informationstätigkeit, einschließlich automationsunterstützt erstellter und aufbewahrter Textdokumente in diesen Angelegenheiten;

Verarbeitung von Daten zu informierender Personen, sofern aufgrund einer Vielzahl von Anfragen zu einem bestimmten Thema ein allgemeines Bedürfnis an Informationen besteht.

DSFA-A20 Aktenverwaltung (Büroautomation) und Verfahrensführung**Zweck der Datenverarbeitung:**


Formale Behandlung der vom Verantwortlichen zu besorgenden Geschäftsfälle (einschließlich der Aufbewahrung der bei dieser Tätigkeit angefallenen Dokumente, Abrechnung von Gebühren, Organisation von Großverfahren).

DSFA-A21 Organisation von Veranstaltungen**Zweck der Datenverarbeitung:**

Datenverarbeitung zur Abhaltung von Veranstaltungen im öffentlichen und privaten Bereich, wie Einladung und Registrierung der Teilnehmer, Organisation von Reisen und Aufhalten, Versorgung der Teilnehmer und Kommunikation vor und nach der Veranstaltung, Abrechnung von Geldleistungen (Honorare, Ersatz für Reisekosten), Abwicklung von Kulturprogrammen, Übermittlung von Unterlagen sowie Anfertigung von im Zusammenhang mit der Veranstaltung stehenden Bild- und Akkustikaufnahmen.

DSFA-A22 Preise und Ehrungen**Zweck der Datenverarbeitung:**

Datenverarbeitung zur Verleihung von Preisen und Ehrenzeichen oder ähnlicher Auszeichnungen, einschließlich der damit verbundenen Vorprüfungen.

| | | |
|--|-----------------|--|
|  | Unterzeichner | serialNumber=1026761,CN=Bundeskazleramt,C=AT |
| | Datum/Zeit | 2018-05-25T10:57:18+02:00 |
| | Prüfinformation | Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bka.gv.at/verifizierung |
| | Hinweis | Dieses Dokument wurde amtssigniert. |

15 Text der Datenschutz-Folgenabschätzung-Verordnung

BUNDESGESETZBLATT

FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2018

Ausgegeben am 9. November 2018

Teil II

278. Verordnung: **Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V)**

278. Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V)

Auf Grund des § 21 Abs. 2 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 24/2018, wird verordnet:

Geltungsbereich

§ 1. Die Bestimmungen dieser Verordnung gelten für die Datenschutz-Folgenabschätzung, die gemäß Art. 35 Abs. 1 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, im Folgenden: DSGVO), ABl. Nr. L 119 vom 4.5.2016 S. 1, vom Verantwortlichen durchzuführen ist.

Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist

§ 2. (1) Sofern die Verarbeitung rechtmäßig im Sinne der Art. 6, Art. 9 und 10 DSGVO erfolgt und keine Datenverarbeitung gemäß der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl. II Nr. 108/2018, vorliegt, ist nach Maßgabe der folgenden Bestimmungen jedenfalls eine Datenschutz-Folgenabschätzung durchzuführen.

(2) Eine Datenschutz-Folgenabschätzung ist durch den Verantwortlichen durchzuführen, wenn zumindest ein in Z 1 bis Z 6 genanntes Kriterium erfüllt ist:

1. Verarbeitungen, die eine Bewertung oder Einstufung natürlicher Personen – einschließlich des Erstellens von Profilen und Prognosen – umfasst für Zwecke, welche die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben und Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen und ausschließlich auf einer automatisierten Verarbeitung beruhen und negative rechtliche, physische oder finanzielle Auswirkungen haben können.
2. Verarbeitungen von Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von natürlichen Personen dienen und von Dritten dazu genutzt werden können, automatisierte Entscheidungsfindungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen.
3. Verarbeitungsvorgänge, welche die Beobachtung, Überwachung oder Kontrolle von betroffenen Personen insbesondere mittels Bild- und damit verbundenen Akustikdatenverarbeitungen zum Ziel haben und
 - a) über Netzwerke erfasste Daten betreffen oder auf eine systematische, umfangreiche Überwachung öffentlich zugänglicher Bereiche abzielen,
 - b) öffentliche Orte, die gemäß § 27 Abs. 2 Sicherheitspolizeigesetz (SPG), BGBl. Nr. 566/1991, von einem nicht von vornherein bestimmten Personenkreis betreten werden können, erfassen,
 - c) Straßen mit öffentlichem Verkehr, die gemäß § 1 Straßenverkehrsordnung 1960 (StVO 1960), BGBl. Nr. 159/1960, von jedermann unter den gleichen Bedingungen benützt werden können, erfassen,
 - d) Örtlichkeiten, welche aufgrund eines Kontrahierungszwanges von jedermann betreten werden dürfen, erfassen,
 - e) Örtlichkeiten, welche aufgrund des öffentlichen Interesses von jedermann betreten werden dürfen, erfassen,

- f) Bildverarbeitungen unter Einsatz von mobilen Kameras zum Zweck der Vorbeugung oder Abwehr gefährlicher Angriffe oder krimineller Verbindungen im öffentlichen und nichtöffentlichen Raum umfassen,
 - g) Bild- und Akustikverarbeitungen umfassen, die dem vorbeugenden Schutz von Personen oder Sachen auf privaten, zu Wohnzwecken dienenden Liegenschaften dienen, die nicht ausschließlich vom Verantwortlichen und von allen im gemeinsamen Haushalt lebenden Nutzungsberechtigten genutzt werden, oder
 - h) Kirchen, Gebetshäuser, soweit sie nicht bereits von lit. b und lit. e erfasst sind, und andere Einrichtungen, die der Religionsausübung in der Gemeinschaft dienen, erfassen.
4. Verarbeitungen von Daten unter Nutzung oder Anwendung neuer bzw. neuartiger Technologien oder organisatorischer Lösungen, welche die Abschätzung der Auswirkungen auf die betroffenen Personen und die gesellschaftlichen Folgen erschweren, insbesondere durch den Einsatz von künstlicher Intelligenz und die Verarbeitung biometrischer Daten, sofern die Verarbeitung nicht die bloße Echtzeitwiedergabe von Gesichtsbildern betrifft.
 5. Zusammenführung und/oder Abgleich von Datensätzen aus zwei oder mehreren Verarbeitungen, die zu unterschiedlichen Zwecken und/oder von verschiedenen Verantwortlichen durchgeführt wurden, im Rahmen einer Datenverarbeitung, die über die von einer betroffenen Person üblicherweise zu erwartenden Verarbeitungen hinausgeht, sofern durch die Anwendung von Algorithmen Entscheidungen getroffen werden können, welche die betroffene Person in erheblicher Weise beeinträchtigen.
 6. Verarbeitungsvorgänge im höchstpersönlichen Bereich von Personen, auch wenn die Verarbeitung auf einer Einwilligung beruht.

Im Zusammenhang mit Beschäftigungsverhältnissen gilt dies nicht, wenn eine Betriebsvereinbarung oder Zustimmung der Personalvertretung vorliegt. Als systematische Überwachung sind jene Vorgänge zu verstehen, die im Rahmen eines Systems oder vorab festgelegt, organisiert und methodisch erfolgen.

(3) Eine Datenschutz-Folgenabschätzung ist durch den Verantwortlichen durchzuführen, wenn ein Verarbeitungsvorgang zwei oder mehr der nachstehenden Kriterien erfüllt:

1. Umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO,
2. umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO,
3. Erfassung von Standortdaten im Sinne des § 92 Abs. 3 Z 6 Telekommunikationsgesetz 2003 (TKG 2003), BGBl. I. Nr. 70/2003, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben,
4. Verarbeitung von Daten schutzbedürftiger betroffener Personen, wie unmündige Minderjährige, Arbeitnehmer, Patienten, psychisch Kranker und Asylwerber, wobei Abs. 2 letzter Satz sinngemäß anzuwenden ist, oder
5. Zusammenführung und/oder Abgleich von Datensätzen aus zwei oder mehreren Verarbeitungen, die zu unterschiedlichen Zwecken und/oder von verschiedenen Verantwortlichen durchgeführt wurden, im Rahmen einer Datenverarbeitung, die über die von einer betroffenen Person üblicherweise zu erwartenden Verarbeitungen hinausgeht, sofern diese für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei der betroffenen Person erhoben wurden.

Personenbezogene Bezeichnungen

§ 3. Bei den in dieser Verordnung verwendeten personenbezogenen Bezeichnungen gilt die gewählte Form für alle Geschlechter.


Verweisungen

§ 4. Verweisungen in dieser Verordnung auf andere Bundesgesetze oder auf Verordnungen sind als Verweisungen auf die jeweils geltende Fassung zu verstehen.

Inkrafttreten

§ 5. Diese Verordnung tritt mit Ablauf des Tages der Kundmachung im Bundesgesetzblatt in Kraft.

Jelinek

| | | |
|--|-----------------|--|
|  | Unterzeichner | serialNumber=932783133,CN=Bundeskanzleramt,C=AT |
| | Datum/Zeit | 2018-11-09T10:54:00+01:00 |
| | Prüfinformation | Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bka.gv.at/verifizierung |
| | Hinweis | Dieses Dokument wurde amtssigniert. |

