DIE EUROPÄISCHE DATENSCHUTZ-GRUNDVERORDNUNG

aus Arbeitnehmer:innensicht

Aktualisierte Auflage
mit Rechtssprechung

gpa
MEINE GEWERKSCHAFT

IMPRESSUM:
Herausgeber: Gewerkschaft GPA, 1030 Wien, Alfred-Dallinger-Platz 1
Redaktion: Clara Fritsch, Gewerkschaft GPA – Abteilung Arbeit & Technik
Layout: Christina Schier, Gewerkschaft GPA – Abteilung Organisierung und Marketing
Bilder/Fotos: iStock, Edgar Ketzer
ÖGB ZVR-Nr.: 576439352

Stand: Mai 2024

Aus der Broschürenserie **GUTE ARBEIT!**

GUTE ARBEIT!

AUTORIN

© Edgar Ketzer

Mag.ª Clara Fritsch

ist Soziologin und arbeitet in der Abteilung Arbeit & Technik der Gewerkschaft GPA. Sie ist Expertin zu den Themen Kontrolle am Arbeitsplatz und Beschäftigten-Datenschutz. Sie berät zur Gestaltung von Betriebsvereinbarungen.

VORWORT

© MichaelMazohl

VORWORT

Am 25. Mai 2018 erhielt die EU ein neues Datenschutzregime: die Verordnung 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, kurz: Europäische Datenschutzgrundverordnung (DSGVO). Damit wurde die in die Jahre gekommene Richtlinie von 1995 nach mehr als zwanzig Jahren abgelöst und die EU-weite Datenschutzgesetzgebung an die Veränderungen und Herausforderungen einer datenbasierten (Arbeits-)Welt angepasst.
Die DSGVO wurde acht Jahre lang zwischen Europäischer Kommission, EU-Parlament und EU-Rat ausgehandelt. Die DSGVO muss den Spagat zwischen dem Schutz natürlicher Personen und dem freien digitalen Markt der EU bewältigen. Es sollen sowohl die Interessen der einzelnen Bürger:innen als auch die Interessen der datenverarbeitenden Unternehmen unter einen Hut gebracht werden. Abgesehen von diesem weiten Interessen-Spektrum, versucht die Verordnung grundrechtliche Regelungen für ganz Europa festzulegen und dabei möglichst konkret zu sein.
Wie das in der betriebsrätlichen Praxis umgesetzt werden kann, zeigt diese Broschüre.

Einige Elemente sind neu zur DSGVO hinzugekommen (z. B. Marktortprinzip, betriebliche Datenschutzbeauftragte, Datenschutzfolgenabschätzung, Recht auf Datenübertragbarkeit, Datenschutz im Beschäftigungsverhältnis). Einige sind adaptiert und aktualisiert worden (z. B. höhere und einheitliche Bußgelder, Verfahrensverzeichnis, Datensparsamkeit, Missbrauchsmeldung). Und Einiges ist beim Alten geblieben (z. B. Grundsätze, Auskunftsrechte). In dieser Broschüre sind die verschiedenen Punkte einfach verständlich erklärt.

Seit die DSGVO in Kraft getreten ist hat sie Wirkung gezeigt. Nicht nur innerhalb der Mitgliedsländer ist die vormals eher belächelte Gesetzesmaterie „Datenschutz" zu einem wesentlichen Regulativ geworden, auch über die Grenzen der EU hinaus versuchen Staaten, ihre Datenschutzregelungen an das Europäische Schutzniveau anzupassen (z. B. Schweiz, Argentinien, Japan und auch die USA versuchen es immer wieder). Um den Schutz der personenbezogenen Daten im Betrieb gewährleisten zu können, muss man die gesetzlichen Voraussetzungen kennen, die DSGVO aus Sicht der Arbeitnehmer:innen kennenlernen. Dabei soll diese Broschüre helfen.

Die Broschüre vermittelt, wie die DSGVO für den Beschäftigtendatenschutz nützlich sein kann und wie man der DSGVO gerecht wird. Sie enthält die wichtigsten Inhalte der DSGVO aus Arbeitnehmer:innen-Sicht.

Die tägliche Beratungsarbeit der Gewerkschaft GPA zeigt, dass der Schutz der Privatsphäre ein immer wichtigeres Gut der Arbeitnehmer:innen ist. Betriebsrät:innen sind zunehmend darum bemüht, die Privatsphäre am Arbeitsplatz zu schützen mit dem Ziel: Weg von dem oder der gläsernen Arbeitnehmer:in hin zu einem Bestimmer oder einer Bestimmerin über die eigenen Daten. Am Weg dahin ist diese Broschüre eine hilfreiche Begleitung.

Barbara Teiber, MA
Vorsitzende

INHALT

INHALT

ÜBERSICHT FAQs

Wertvolle Tipps

FAQs

DSGVO

GRUNDLAGEN

WAS BEI DER DATENVERWENDUNG BERÜCKSICHTIGT WERDEN MUSS.

PERSONENBEZOGENE DATEN IM UNTERNEHMEN – WORUM GEHT'S?

Artikel 4, Ziffer 1 und Artikel 9, Erwägungsgründe 26, 27, 30, 31 DSGVO

Alles, was eindeutig einer Person zugeordnet wird – oder werden kann – ist ein personenbezogenes Datum (also „Klassiker" wie Name, Adresse, Telefonnummer, Geburtsdatum etc.). In der DSGVO ist die Definition breit gefasst, sodass explizit Kennnummern (z. B. Personalnummer), Online-Kennungen (z. B. IP-Adresse) und Standortdaten (z. B. GPS) dazuzählen.

Gilt die DSGVO auch bei Akten in Papierform oder Blättern im Hängeordner?

JA, auch die „nichtautomatisierte Verarbeitung personenbezogener Daten in einem Dateisystem" (z. B. ein Personalverwaltungsakt) unterliegt der DSGVO. „Analoge Daten" unterliegen der DSGVO. Der Ordner mit der Aufschrift „Diverses", in dem seit Jahren unsortiert Telefonnotizen landen, der Ordner „Privat" oder die lose Sammlung von Visitenkarten zählen allerdings nicht dazu, weil sie nicht systematisch geordnet sind bzw. weil sie einzig privaten Zwecken dienen.

Außerdem gibt es **„besondere Kategorien personenbezogener Daten"**. Diese müssen noch strenger geschützt werden.

Artikel 9, Erwägungsgründe 51–56 DSGVO

Die besonderen Kategorien personenbezogener Daten sind abschließend definiert, das heißt es gibt darüber hinaus keine anderen besonderen Kategorien. Auch wenn in Österreich landläufig finanzielle Angaben (z. B. Einkommen, Kontostand) als „sensibel" bezeichnet werden, so entspricht das nicht der gesetzlichen Definition. Es handelt sich um jene Daten, bei denen eine Diskriminierung vorliegen könnte:

- Gewerkschaftszugehörigkeit und politische Meinung,
- biometrische und genetische Daten,
- Daten über die ethnische oder rassische Herkunft,
- Gesundheitsdaten,
- Daten zum Sexualleben und
- religiöse oder weltanschauliche Überzeugungen.

Diese besonderen Kategorien personenbezogener Daten unterliegen einem besonderen Schutz und **dürfen nicht verwendet werden** – außer

- die betroffenen Personen haben ausdrücklich und freiwillig zugestimmt,
- die Verwendung ist gesetzlich geregelt (z. B. Bankwesengesetz),
- die Verwendung geschieht im Sinne der öffentlichen Gesundheit (z. B. Epidemiegesetz) bzw. der Gesundheitsvorsorge,
- es handelt sich um die Verwaltung von Gesundheitssystemen (z. B. Sozialversicherungsgesetz),
- die Datenverwendung ist arbeitsmedizinisch für die Beurteilung der Arbeitsfähigkeit erforderlich (z. B. Arbeitnehmer:innenschutzgesetz),
- es ist lebenswichtig.

(Es gibt noch weitere Ausnahmen, die allerdings für den Beschäftigtendatenschutz weniger wichtig sind.)

Darf der/die Arbeitgeber:in meine Gesundheitsdaten wissen?

Nur, wenn es ein Gesetz vorsieht. Wenn beispielsweise ein ärztliches Gutachten über das Vorliegen einer Berufserkrankung oder für Gesundheitsberufe ein Gesundheitszeugnis benötigt wird. Bei einem Krankenstand beispielsweise ist Beginn und Ende ausreichend und eine Diagnose geht den/die Arbeitgeber:in nichts an.

HANDELNDE PERSONEN IN DER DSGVO – EIN KLEINES „WHO IS WHO"

Artikel 4, Ziffer 1–9 DSGVO

Die **Betroffenen** sind diejenigen, deren personenbezogene Daten verarbeitet werden und die geschützt werden sollen, aus der Perspektive der Arbeitnehmer:innen: sie selbst.

Diejenigen, welche die Datenverarbeitungen durchführen, die also personenbezogene Daten erheben, auswerten, speichern etc. heißen **„Verantwortliche"**. Ihnen fällt die Aufgabe zu, die Vorgaben der DSGVO zu erfüllen.

Sub-Unternehmen, die personenbezogene Daten für andere Unternehmen verarbeiten, heißen **„Auftragsverarbeiter"**. Sie sind von den Verantwortlichen beauftragt, personenbezogene Daten zu verarbeiten (z. B. externe Lohnverrechnung).

Die **Datenschutzbehörde** ist nun für den gesamten EU-Raum hinsichtlich ihrer Aufgaben und Befugnisse einheitlich geregelt. (Manche verwenden noch immer die bis 2022 in Österreich gütige Bezeichnung „Datenschutzkommission".) In der DSGVO findet man sie unter der Bezeichnung „unabhängige Aufsichtsbehörde". Die Behörde hat seit dem 25. Mai 2018 unter anderem auch die Aufgabe, Geldbußen bei Verletzung der DSGVO zu verhängen (vgl. Kapitel „Strafen", S. 21).

Die **Arbeitnehmer:innenvertretung**, also Gewerkschaften und Betriebsräte sind in der DSGVO nicht namentlich erwähnt. Ihre Rechte finden sich – nach wie vor – im Arbeitsverfassungsgesetz wieder. Einzige Ausnahme bildet der Beschäftigtendatenschutz in Artikel 88 und Erwägungsgrund 155, wo festgehalten ist, dass in Kollektivvereinbarungen – also auch Betriebsvereinbarungen – spezifische Regelungen getroffen werden können (vgl. Kapitel „Rechte des Betriebsrats", S. 24). Eine Rolle spielt die Interessenvertretung der Arbeitnehmer:innen noch bei der Datenschutzfolgenabschätzung, wo sie beragt werden soll (vgl. Kapitel „DSFA", S. 14)

GRUNDRECHT AUF DATENSCHUTZ

Artikel 1, Erwägungsgrund 1 DSGVO

In der DSGVO ist – wie auch in Artikel 8 der Europäischen Grundrechtecharta (GRC) – festgelegt, dass jedermann das Recht auf den Schutz seiner/ihrer personenbezogenen Daten hat. Neben den Grundrechten auf freie Meinungsäußerung sowie auf die Achtung des Privat- und Familienlebens existiert also auch das Grundrecht, die eigenen Daten vor dem Zugriff staatlicher, aber auch privater Stellen zu schützen. EU-Bürger:innen können sich darauf berufen, dass sie ihre Daten nicht jedermann zugänglich machen müssen. In Deutschland hat sich dafür der aus dem so genannten „Volkszählungsurteil" des Bundesverfassungsgerichts von 1983 stammende Begriff **„informationelle Selbstbestimmung"** durchgesetzt. Es sollen die Menschen selbst bestimmen, welche Informationen über ihre Person wem, wie, wo, wann zugänglich gemacht werden. Zugleich soll die DSGVO aber auch sicherstellen, dass der freie Datentransfer innerhalb der Europäischen Union nicht beeinträchtigt wird.

MARKTORTPRINZIP

Artikel 3, Erwägungsgründe 22–25 DSGVO

Das Marktortprinzip ist eine – an das Wettbewerbsrecht angelehnte – neue Errungenschaft. Nun unterliegt jede Geschäftstätigkeit auf dem EU-Gebiet der DSGVO. Das bedeutet, dass auch nicht in der EU ansässige Unternehmen (z. B. Anbieter:innen von digitalen Dienstleistungen, Hersteller:innen von Apps, Plattformen zur digitalen Arbeitsvermittlung etc.) sich an die DSGVO halten müssen. Es besteht also eine Ortsunabhängigkeit

bezüglich der Niederlassung oder des Hauptsitzes des/der Verantwortlichen. Kurz: Wer also Waren und/oder Dienstleistungen der Datenverarbeitung in der EU verkauft, anbietet, betreibt oder auch nur erforscht, unterliegt der DSGVO.

Unternehmen müssen die DSGVO unabhängig davon einhalten, welche Art von Dienstleistungen oder Produkten konkret angeboten werden. Es ist egal, ob Unternehmen eine Ware oder Dienstleistung verkaufen oder „gratis" zur Verfügung stellen und es ist auch egal, ob sie ihre Produkte Erwachsenen oder Kindern anbieten. Die Betroffenen müssen sich nur innerhalb der EU aufhalten. Auch wenn „nur" das Verhalten von Personen innerhalb der EU beobachtet wird (z. B. Verkehrsstau, Nutzungsdauer einer Smartphone-App etc.), ist die DSGVO zu befolgen.

Ein nicht in der EU ansässiges Unternehmen, das in der EU Geschäfte betreibt, muss eine:n Vertreter:in in der EU benennen. Diese Vertreter:innen sind die Ansprechpartner:innen für die nationalen Datenschutzbehörden und EU-Bürger:innen bei Fragen zur gesetzeskonformen Verwendung personenbezogener Daten durch das jeweilige Unternehmen.

Artikel 27, Erwägungsgrund 80 DSGVO

Müssen sich Betriebe, die nicht aus der EU sind, an die DSGVO halten?

JA, wenn sie hier Waren und/oder Dienstleistungen anbieten. Selbst wenn sie „nur" Daten sammeln oder „nur" das Verhalten von Menschen in der EU beobachten, müssen sie die Grundprinzipien einhalten und die Grundrechte der Menschen wahren, egal ob sie im EU-Raum über eine reale Niederlassung verfügen oder nicht. Diese Verpflichtung ist auch unter dem Titel „Marktortprinzip" bekannt und stößt vor allem bei us-amerikanischen Unternehmen auf wenig Begeisterung.

GRUNDSÄTZE DER DATENVERARBEITUNG

Artikel 5 Abs 2 DSGVO

Bei jeder Datenverwendung muss sich der/die Verantwortliche an die Grundsätze der DSGVO halten. Eine Nicht-Einhaltung stellt einen Verstoß gegen die DSGVO dar.

ZWECKBINDUNG

Das für die Datenverwendung im Arbeitsverhältnis wohl wichtigste Grundprinzip ist die Zweckbindung. Jede Datenverwendung muss einen rechtmäßigen Zweck verfolgen. Es muss klar sein, wozu personenbezogene Daten verwendet werden. Der/die Verantwortliche muss die Frage beantworten können, wozu eine Datenverarbeitung dient. Ein solcher Zweck muss **festgelegt, eindeutig und rechtmäßig** sein. Eine allgemeine Formulierung wie „zur Verbesserung der internen Prozesse" ist eher nicht ausreichend.

DATENMINIMIERUNG UND SPEICHERBEGRENZUNG

Personenbezogene Daten sollen so sparsam wie möglich verwendet werden. Eine fixe Aufbewahrungspflicht gibt es laut DSGVO nicht und sie wäre auch wenig hilfreich, da die DSGVO unterschiedlichste Datenkategorien und Datenverwendungen regelt – also „technikneutral" ist – und man nicht alle über einen Kamm scheren kann.
Um festzustellen, wie lange Daten gespeichert werden dürfen, ist es erforderlich, den Zweck für die Datenverwendung zu kennen. Falls es rechtliche Vorgaben für die Datenspeicherung gibt, sind diese einzuhalten und stellen somit den Zweck dar (z. B. um dem Finanzamt eine Steuerüberprüfung zu ermöglichen, müssen dafür relevante Daten sieben Jahre aufbewahrt werden (§ 132 Abs 1 Bundesabgabenordnung); Akten zu Krankengeschichten müssen zehn Jahre aufbewahrt werden (§ 51 Abs 3 Ärztegesetz); Gewährleistungsfristen erfordern, dass Rechnungen aufgehoben werden etc.). Das Prinzip der Datenminimierung hängt also eng mit jenem der Zweckbindung sowie der Rechtmäßigkeit zusammen. In der DSGVO ist der Grundsatz der Datenminimierung stark verankert. Die vorgesehene Speicherdauer muss nämlich bei der Auskunft an die Betroffenen (vgl. Kapitel

„Betroffenenrechte – was steht dem und der Einzelnen zu?“, S.12) und im Verzeichnis der Verarbeitungstätigkeiten (vgl. Kapitel „Verzeichnis der Verarbeitungstätigkeiten“, S. 14) angegeben werden.

RICHTIGKEIT

Die verwendeten personenbezogenen Daten müssen richtig und aktuell sein. Natürlich hängt die Richtigkeit und Aktualität davon ab, für welchen Zweck die Daten verwendet werden, z. B. wird ein Bildband zum 100. Jubiläum eines Unternehmens zwangsläufig keine aktuellen personenbezogenen Daten umfassen.

TRANSPARENZ

Ein weiterer Grundsatz lautet, dass die Betroffenen immer nachvollziehen können müssen, was mit ihren personenbezogenen Daten geschieht. Dieser Grundsatz findet sich in den ausführlichen Auskunfts- und Informationspflichten wieder (siehe Artikel 12 ff DSGVO).

INTEGRITÄT UND VERTRAULICHKEIT

Der Grundsatz der Integrität und Vertraulichkeit bezieht sich vorwiegend auf die Datensicherheit (englisch „safety and security“). Damit Vertrauen entsteht – wie es ausdrücklich eine der Intentionen des Europäischen Gesetzgebers ist – müssen Daten gut vor unbefugtem Zugriff oder sonstigen Schäden geschützt sein. Im Abschnitt der DSGVO zu Datenschutz durch Technik spiegelt sich dieser Grundsatz wider (vgl. Kapitel „Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen“ sowie „Technische und organisatorische Maßnahmen" (TOM), S. 21).

RECHENSCHAFTSPFLICHT

Dieser Grundsatz war in der EU-Datenschutz-Richtlinie von 1995 noch nicht enthalten. Das Hinzufügen dieses Prinzips führt dazu, dass Verantwortliche ihr datenschutzrechtliches Handeln belegen, aufzeichnen, und festhalten müssen, um sich bei allfälligen Unklarheiten rechtfertigen zu können. Rechenschaftspflicht bedeutet also, dass Verantwortliche nachweisen müssen, dass bei Datenverwendungen die Grundsätze eingehalten wurden. Hier wird der Verantwortliche im wahrsten Sinn des Wortes in die Pflicht genommen. Das kann in einigen Unternehmen zu einem richtiggehenden Kulturwandel führen, in anderen zu „Bürokratiemonstern“ und „administrativen Hürden“.

RECHTMÄSSIGKEIT

Artikel 6, Erwägungsgründe 39–45

Datenverwendungen brauchen immer eine rechtliche Grundlage. Die DSGVO zählt auf, was als eine solche gilt:

- die Einwilligung einer betroffenen Person,
- Die Erfüllung eines Vertrages,
- eine rechtliche Verpflichtung (z. B. die Pflicht zur Aufzeichnung der Arbeitszeit gemäß Arbeitszeitgesetz),
- lebenswichtige Interessen erfordern die Datenverarbeitung,
- das öffentliche Interesse erfordert die Datenverwendung,

... und es kann auch „die Verarbeitung zur Wahrung berechtigter Interessen der Verantwortlichen oder eines Dritten“ eine legale Grundlage zur Datenverarbeitung darstellen. Diese schwammige Formulierung wird in der betrieblichen Praxis wohl eine deutliche Ausformulierung brauchen. Der Verantwortliche wird erklären müssen, was denn seine berechtigten Interessen sind und diese müssen dann wiederum mit den Interessen der Beschäftigten abgewogen werden.

GRUNDPRINZIPIEN DER DSGVO

BETROFFENENRECHTE – WAS STEHT ALLEN ZU?

Artikel 12–20, Erwägungsgründe 60–64

Eines der wichtigsten Rechte ist für die Betroffenen das **Lösch- und Berichtigungsrecht**. Sollten personenbezogene Daten nicht mehr erforderlich sein, müssen sie gelöscht werden. Dies wird auch das „Recht auf vergessen werden" genannt. Sollten personenbezogene Daten unrichtig sein, müssen sie richtiggestellt werden (siehe Artikel 16–18 DSGVO).
Das **Recht auf Datenportabilität** schafft die Möglichkeit, die eigenen Daten von einem Verantwortlichen zum nächsten in digitaler Form „mitzunehmen" (siehe Artikel 20 DSGVO).
Auch ein Recht auf Einschränkung der Verarbeitung wurde geschaffen. Sollte es zu Streitigkeiten darüber kommen, ob personenbezogene Daten richtig verwendet wurden, ob sie noch benötigt werden oder nicht, dann kann statt einer kompletten Löschung auch eine „Einschränkung" verlangt werden, wodurch die Daten quasi unzugänglich gemacht werden (siehe Artikel 18 DSGVO).

Das **Informationsrecht** nimmt Verantwortliche in die Pflicht, die Betroffenen über eine Datenverwendung ausführlich zu **informieren**. Die Information muss **verständlich, präzise und leicht zugänglich** vermittelt werden. Die Information kann elektronisch, schriftlich oder auf ausdrücklichen Wunsch der Betroffenen, auch mündlich gegeben werden (siehe Artikel 12 DSGVO).

Die Antwortfrist auf allfällige Fragen der Betroffenen beträgt einen Monat (siehe Artikel 12 Abs 3 DSGVO).

Folgende Inhalte müssen bei der Information der Betroffenen enthalten sein (siehe Artikel 13 DSGVO):

- Name und Kontaktdaten der Verantwortlichen sowie einer oder eines – allfällig vorhandenen – betrieblichen Datenschutzbeauftragten. Wer ist zuständig? An wen kann ich mich wenden?
- Zweck der Datenverarbeitung. Wozu werden die personenbezogenen Daten der Beschäftigten überhaupt verarbeitet?
- Gegebenenfalls Empfänger:innen oder Empfängerkreise. An wen werden personenbezogene Daten der Beschäftigten weitergeleitet? Beispielsweise an die Konzernzentrale/ein Sub-Unternehmen?
- Speicherdauer. Wie lange werden die Daten aufgehoben?
- Rechtliche Grundlagen. Was berechtigt den/die Verantwortlichen die personenbezogenen Daten zu verarbeiten? Gesetz/Einwilligung/Vertrag/lebenswichtige oder öffentliche Interessen?
- Hinweis auf die Betroffenenrechte, also auf das Recht auf Auskunft, Berichtigung oder Einschränkung der Verarbeitung (siehe Artikel 18 DSGVO), Löschung, Datenübertragbarkeit (siehe Artikel 13 Abs 2 lit b DSGVO) sowie das Recht eine einmal gegebene Einwilligung zu widerrufen und Beschwerde bei einer Behörde einzulegen (siehe Artikel 15 Abs 1 lit f DSGVO). Welche Rechte habe ich?
- Sollten die personenbezogenen Daten für profiling oder eine „automatisierte Einzelentscheidung" verwendet werden (siehe Exkurs Profiling, S. 13), muss über die involvierte Logik, über die Tragweite und über die angestrebten Auswirkungen informiert werden. Werden meine Daten ausschließlich automationsunterstützt verarbeitet? (Berechnet z. B. ein Programm, ob ich mich für einen bestimmten Arbeitsplatz eigne?) Wenn ja, was sind die erhofften oder geplanten Auswirkungen? Welche Tragweite kann das für mich haben? Was ist die dahinterliegende Logik? Welche Entscheidungskriterien werden herangezogen? Welche Analysen werden gemacht? Kann ich durch die automatisierte Einzelentscheidung einen Anspruch verlieren, z. B. bei der Bewerbung nicht diskriminiert zu werden?

Wenn die Daten nicht bei den Betroffenen selbst erhoben wurden (sondern z. B. von Dritten zugekauft), muss zusätzlich darüber informiert werden, welche Kategorien personenbezogener Daten verwendet werden und woher die Daten kommen. Woher hat der/die Arbeitgeber:in die Daten der Beschäftigten? Wurden Soziale Netzwerke durchforstet, was vermutlich aufgrund einer Verletzung der Privatsphäre problematisch wäre.
Außerdem haben alle Betroffenen ein **Auskunftsrecht**. Gegenüber der Informationspflicht, die den Verantwortlichen zukommt, ist das Auskunftsrecht von den Betroffenen aktiv einzufordern. Jede:r Arbeitnehmer:in und auch der Betriebsrat/die Betriebsrätin sind Betroffene, wenn ihre personenbezogenen Daten verarbeitet werden. Das Auskunftsrecht beinhaltet die oben angeführten Punkte. Der Betriebsrat kann sich diese Auflistung zu Nutze machen, indem er bei der Geschäftsführung nachfragt, wie Datenverwendungen konkret gehandhabt werden.
Der Betriebsrat kann gleichzeitig selbst Verantwortlicher sein. Dann muss er selbst den betroffenen Arbeitnehmer:innen Auskunft erteilen und die Punkte beantworten können (siehe Kapitel Daten im Betriebsratsbüro, S. 28).

Was mache ich, wenn der/die Arbeitgeber:in meine Anfragen einfach ignoriert?

Keine Auskunft zu bekommen, ist strafbar. Sollte das der Fall sein, ist eine Beschwerde auf Verletzung des Auskunftsrechts bei der Datenschutzbehörde einzubringen. Die Österreichische Datenschutzbehörde hat für solche Fälle eigens ein Dokument auf ihre Website gestellt.

Muss der oder die Verantwortliche zu jeder Frage Auskunft erteilen?

NEIN. Wenn das Begehren „exzessiv" ist kann der/ die Verantwortliche die Auskunft zu Recht unterlassen. Das ist dann der Fall, wenn eine übermäßig detaillierte Auskunft verlangt wird (z. B. die täglich versandten Emails), wenn sehr häufige Anfragen gestellt werden (z. B. einmal pro Woche) oder wenn bei vielen unterschiedlichen Verantwortlichen ein und die selbe Anfrage gestellt wird.

EXKURS: PROFILING

Artikel 4 Abs 4 (Definition), Artikel 22 und Erwägungsgründe 71–72 DSGVO

Unter „profiling" versteht man die Auswertung von personenbezogenen Daten, um die Persönlichkeit zu **analysieren und** zu **prognostizieren**. Die Arbeitsleistung, die wirtschaftliche Lage, die Zuverlässigkeit, persönliche Vorlieben oder Interessen, u.s.w. können in Profile von Arbeitnehmer:innen einfließen.). Wenn solche Analysen ausschließlich von Maschinen vorgenommen werden, also ausschließlich auf Algorithmen basieren, dann handelt es sich um eine so genannte „automatisierte Entscheidung" (Englisch spricht man von „automated desicion making – ADM"). Und wenn eine solche Auswertung dann als Grundlage für **„erheblich beeinträchtigende Entscheidungen"** im Einzelfall verwendet wird, ist das verboten.
In der DSGVO mehr Gewicht, indem erstens die Formulierung klarer gefasst wurde, zweitens der „automatisierten Einzelentscheidung" ein eigener Artikel gewidmet und drittens ein Verstoß mit höheren Sanktionen belegt wurde.
In welchen Fällen konkret eine „erhebliche Beeinträchtigung" vorliegt, wird wohl erst vor Gerichten und Behörden ausgestritten und damit definiert werden müssen. Ist die Ablehnung eines Bewerbers/einer Bewerberin eine „erhebliche Entscheidung"? Ist die Auszahlung einer Prämie aufgrund von rein algorithmisch ausgewerteten Kategorien eine „erhebliche Entscheidung"? Derzeit herrscht ein wahrer Hype rund um algorithmenbasierte Entscheidungs„hilfen", auch „Künstliche Intelligenz" genannt. Durch KI-Anwendungen werden Bewerber:innen vorab sortiert, Fahrtrouten erstellt, Teams optimiert, Weiterbildungsangebote kreiert, Protokolle zusammengefasst u.s.w. Die Bedeutung dieses Profiling-Verbots kann angesicht des grassierenedn Einsatzes von KI gar nicht hoch genug geschätzt werden.
Zum Thema Profiling gibt ein EuGH-Urteil von 2023 Aufschluss (siehe S. 32).

WESENTLICHE INHALTE – WAS DEM BETRIEBS-RAT HILFT

VERZEICHNIS DER VERARBEITUNGS-TÄTIGKEITEN (VVZ)

Artikel 30, Erwägungsgrund 82 DSGVO

Die DSGVO schreibt vor, dass innerbetrieblich eine Übersicht darüber zu führen ist, wer für die Datenverarbeitung verantwortlich ist, welche Datenverarbeitungen gemacht werden, welchem Verwendungszweck die Datenverarbeitung dient und an welche Empfängerkreise eventuell Daten weitergeleitet werden.

Unternehmen, die weniger als 250 Mitarbeiter:innen beschäftigen, müssen kein Verarbeitungsverzeichnis führen. Sollten sie allerdings besondere Kategorien von Daten verarbeiten (siehe Kapitel Personenbezogene Daten im Unternehmen), müssen sie trotzdem ein Verzeichnis führen. Dasselbe gilt, wenn Daten über **strafrechtliche Verurteilungen**, **biometrische Daten** oder **personenbezogene Daten in großer Zahl** verarbeitet werden. Sollte die Datenschutz-Folgenabschätzung (siehe Kapitel „Datenschutz-Folgenabschätzung“; S. 14) zu einem positiven Ergebnis kommen oder erfolgt die Datenverwendung regelmäßig (im Verordnungstext steht: „nicht nur gelegentlich“), ist ebenfalls ein Verzeichnis zu führen.

Das Verzeichnis ist auf Verlangen der Aufsichtsbehörde vorzuzeigen.

Auch Auftragsdatenverarbeitende, also allfällig beauftragte Unternehmen, müssen ein Verarbeitungsverzeichnis führen.

Muss der Betriebsrat für sich selbst auch ein Verarbeitungsverzeichnis führen?

JA, wenn im Betriebsrat eigene Datenverwendungen durchgeführt werden, muss auch ein Betriebsrat der Datenschutzbehörde auf Verlangen ein Verarbeitungsverzeichnis vorweisen können. Wenn der Betriebsrat also z. B. in eigenen Systemen die Apothekenbestellung verwaltet, wenn er Daten über Angehörige speichert, um Geburtenbeihilfen auszuzahlen (z. B. Excel-Listen) oder Ähnliches, dann muss im Betriebsrat-Büro ein Verarbeitungsverzeichnis vorliegen, in dem diese Verwendungen angeführt sind.

DATENSCHUTZ-FOLGENABSCHÄTZUNG (DSFA)

Artikel 35f und Erwägungsgründe 89–96

DSFA bedeutet, dass die Auswirkungen bestimmter Datenverwendungen vorab genauer geprüft werden müssen. Seit Inkrafttreten der DSGVO im Mai 2018 müssen die Risiken vom Verantwortlichen selbst, also **innerhalb des Betriebes**, abgeschätzt werden. Die DSFA soll das Risiko für die Betroffenen, dass ihre Grundrechte eingeschränkt werden, prüfen und falls eines besteht, so gering als nur irgendwie möglich halten.

Bei welchen Datenverarbeitungen muss eine Folgenabschätzung durchgeführt werden?

- bei großem Risiko für die Grundfreiheiten der Betroffenen (z. B. Eingriffe in die Privatsphäre durch permanentes GPS-Tracking der Arbeitnehmer:innen);
- bei der systematischen und umfassenden Bewertung persönlicher Aspekte von Personen (z. B. profiling, automatisierte (Leistungs-)Bewertung, die dann für schwerwiegende Entscheidungen genutzt werden (Was genau „umfassend" oder „schwerwiegend" bedeutet, wird wohl durch die Urteile von Gerichten noch näher zu definieren sein.);
- bei der umfangreichen Verwendung besonderer Datenkategorien (besondere Datenkategorien sind Gewerkschaftszugehörigkeit, politische Meinung, biometrische und genetische Daten sowie Daten über die ethnische oder rassische Herkunft, Gesundheitsdaten oder Daten zum Sexualleben; was genau „umfangreich" bedeutet, wird wohl durch die Auslegung der DSGVO noch näher zu definieren sein);
- bei der systematischen und umfassenden Überwachung öffentlicher Bereiche (z. B. Videokameras im öffentlichen Raum).

Die Datenschutzbehörde hat eine Verordnung über jene Verarbeitungsvorgänge erlassen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, die DSFA-V. Darin ist beispielsweise festgehalten, dass insbesondere für den Einsatz von **künstlicher Intelligenz** und die Verarbeitung **biometrischer Daten** eine DSFA vorgenommen werden muss.

Man spricht dabei von einer „Blacklist", die festlegt, für welche Datenverarbeitungen eine Folgenabschätzung durchgeführt werden muss, und einer sogenannten **„Whitelist"**, wenn keine DSFA erforderlich ist, was beispielsweise bei der „klassischen" Personalverwaltung der Fall ist. Die Liste jener Datenverarbeitungen, die in Österreich auch ohne Folgenabschätzung betrieben werden dürfen, trägt den etwas sperrigen Namen **„Datenschutz-Folgenabschätzung-Ausnahmen-Verordnung" (DSFA-AV)**. Die DSFA muss nicht gemacht werden bei typischen betrieblichen Datenverarbeitungen wie Buchführung, Rechnungswesen, Personalverwaltung, Berechtigungsverwaltung, Zutrittskontrollsystemen, Videoüberwachung öffentlich zugänglicher Bereiche oder beim Organisieren von Veranstaltungen.

Diese Datenverwendungen bedürfen keiner DSFA möglicherweise aber trotzdem einer BV. Die „Befreiung" von einer DSFA ist nicht zu verwechseln mit der Verpflichtung – soweit personenbezogene Daten der Beschäftigten verwendet werden oder Kontrollen der Beschäftigten ermöglicht werden – eine Betriebsvereinbarung abzuschließen.

Die österreichische Datenschutzbehörde erkannt, dass die Betriebsvereinbarung hier eine Rolle spielt und schreibt in ihrer Verordnung zur DSFA: „Im Zusammenhang mit Beschäftigungsverhältnissen gilt dies [also die Verpflichtung zur Folgenabschätzung] nicht, wenn eine Betriebsvereinbarung oder Zustimmung der Personalvertretung vorliegt." (§ 2 DSFA-V). Die Betriebsvereinbarung wird also als Ersatz einer DSFA gesehen. Hier könnte ein Missverständnis entstehen, denn umgekehrt ist das keinesfalls möglich; eine Datenschutz-Folgenabschätzung kann eine nach dem Arbeitsverfassungsgesetz erforderliche Betriebsvereinbarung nicht ersetzen!! Vielmehr wurde klargestellt: **Die Rechte des Betriebsrates nach dem Arbeitsverfassungsgesetz sind Bestandteil der DSGVO.** Indem das ArbVG der EU-Kommission als wesentlich für den Beschäftigtendatenschutz gemeldet wurde (in der EU heißt es „notifiziert" gem Artikel 88 Abs 3 DSGVO).

Wenn die Arbeitgeberseite keine DSFA machen muss, muss dann trotzdem eine BV abgeschlossen werden?

KOMMT DRAUF AN. Es handelt sich um zwei voneinander unabhängige Fragen. Ob eine DSFA gemacht werden muss, hängt von der DSGVO und der Ausnahmen-Verordnung ab. Ob eine BV abgeschlossen werden muss, liegt im ArbVG begründet. Wenn beispielsweise in einem Unternehmen die Videokameras den Eingangsbereich erfassen, braucht es keine DSFA, sehr wohl aber eine BV.

Ein Betriebsrat sollte keiner Betriebsvereinbarung zustimmen, die eine DSFA ersetzen soll. Vorab muss immer vom Verantwortlichen geklärt werden, welche Risiken mit der eingesetzten Anwendung und Technologie verbunden sind und welche Maßnahmen zum Schutz der Beschäftigten ergriffen werden.

Ist ein:e Datenschutzbeauftragte:r im Betrieb vorhanden, muss er/sie bei der Datenschutz-Folgenabschätzung mit an Bord geholt werden. Vor allem müssen aber die Betroffenen oder ihre Interessenvertretung, also der Betriebsrat, nach ihrer Meinung gefragt werden (Artikel 35 Abs 9 DSGVO).
Sollte ein Risiko festgestellt werden, muss auch die Behörde konsultiert werden, die dann ihrerseits binnen acht Wochen Empfehlungen zur Eindämmung des Risikos abgeben muss.

Die genaue Vorgehensweise wie eine Datenschutzfolgenabschätzung durchgeführt werden soll, wie die Rolle des Betriebsrates dabei aussieht und wie ein Schwellenwert bestimmt werden kann, ab dem eine DSFA erforderlich ist, dazu hat die Gewerkschaft GPA ein eigenes Dokument zusmmenstellt. Dieses erhalten GPA-Betriebsrät:innen bei den betriebsbetreuenden Kolleg:innen.

DATENTRANSFER IN LÄNDER AUSSERHALB DER EU (DRITTSTAATEN)

In allen EU-Mitgliedsländern muss die DSGVO eingehalten werden. Alle Mitgliedsländer haben dasselbe Datenschutzniveau. Somit bedarf es innerhalb der EU keiner weiteren besonderen Regelungen für Datentransfers. Bei Ländern, die keine EU-Mitglieder sind (sogenannte Drittstaaten) bedarf es allerdings ergänzender Maßnahmen, damit personenbezogene Daten rechtmäßig durch die Welt „segeln" können.

Gibt es in der DSGVO ein Privileg für Konzerne, damit diese Datentransfers einfacher durchführen können?

JEIN, es wurden mit der DSGVO mehrere Möglichkeiten geschaffen, die den internationalen Datentransfer innerhalb des Konzerns erleichtern sollen (siehe nachfolgende Kapitel). Es gibt aber keine generelle „Freigabe" für Konzerne, sodass diese die personenbezogenen Daten der Arbeitnehmer:innen nur unter bestimmten Bedingungen verwenden dürfen.

Angemessenheitsbeschluss

Artikel 45 DSGVO

Drittstaaten müssen beweisen, dass personenbezogene Daten bei ihnen genauso gut geschützt sind wie innerhalb der EU. Dazu wird zwischen dem Drittstaat und der EU-Kommission verhandelt. Der Drittstaat muss seinen Datenschutz so anpassen, dass die grundlegenden Regeln dieselben sind wie in der EU. Kriterien für ein angemessenes Schutzniveau sind z. B. ob Betroffenen der Zugang zur Rechtsprechung möglich ist, ob Behörden für den Datenschutz bestehen und Ähnliches. Wurde das Datenschutzniveau im Drittstaat dann von der EU-Kommission als angemessen bewertet, ist der Drittstaat einem EU-Mitgliedsstaat gleichgestellt. Derzeit gilt ein Angemessenheitsbeschluss für Andorra, Argentinien, Färöer-Inseln, Guernsey, Insel Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay. Japan und die Republik Korea sind als letzte auf der Liste hinzugekommen. Dem Vereinigten Königreich wird seit Juni 2021 ebenfalls ein angemessenes Datenschutzniveau attestiert, ausgenommen sind Datenverwendungen zum Zweck der Einwanderungskontrolle. Gültig ist der Beschluss bis 2025.

Auftragsdatenverarbeitung

Artikel 28f DSGVO

Nach wie vor können Datenverarbeitungen bei einem oder einer Sub-Unternehmer:in in Auftrag gegeben werden. Wenn dieses Unternehmen nun in einem Nicht-EU-Staat beheimatet ist, handelt es sich um Datenübermittlung in einen Drittstaat. Ein solcher Datentransfer muss – wie alle anderen auch – mit den entsprechenden Verträgen abgesichert werden (in der alten Datenschutz-Richtlinie hießen diese „Dienstleisterverträge"). In einem solchen Vertrag muss festgelegt sein: Gegenstand und Dauer der Datenverarbeitung, Art und Zweck der Verarbeitung, die Kreise betroffener Personen sowie die Pflichten und Rechte des/der Verantwortlichen. Der/Die Auftragsverarbeiter:in muss außerdem technisch und administrativ (z. B. technisch durch eine Firewall und organisatorisch durch Zutrittsregelungen) den Schutz der personenbezogenen Daten garantieren.

Standard-Vertragsklauseln (SVK), Standard Contractual Clauses (SCC)

Artikel 46 Abs 2 lit c DSGVO

Aufgrund dieser von der EU-Kommission ausgearbeiteten Vertragsmuster für EU-Drittstaaten wurden bislang die meisten Datentransfers rechtlich abgesichert. Die Standardvertragsklauseln sind einfache, im Netz abrufbare Muster-Verträge, die dann nur noch fertig ausgefüllt, allfällig ein wenig an die betrieblichen Bedürfnisse angepasst und unterschrieben werden müssen, und schon kann es losgehen mit der Datenübermittlung.

Exkurs:USA

Vor dem Hintergrund eines Urteils des Europäischen Gerichtshofes , wonach das mit den USA vereinbarte „Privacy Shield" nicht rechtmäßig ist (auch bekannt unter dem Namen „Schrems II"), wurde der Datentransfer in die USA seit 2021 mit eigenen Standardvertragsklauseln seitens der EU-Kommission geregelt. Für einen Datentransfer mit US-amerikanischen Unternehmen, die Daten von EU-Bürger:innen verarbeiten, muss ein Unternehmen prüfen, ob ein angemessenes Schutzniveau vorliegt.

Branchen- oder konzernweite Verhaltensrichtlinien

Artikel 42 und 47 DSGVO

Interne Datenschutzvorschriften können für einen Konzern (in der DSGVO heißt es „Unternehmensgruppe") oder ganze Branchen (in der DSGVO heißt es „Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben") ausverhandelt werden. Eine solche Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausübt, kann sich also zusammenschließen, gemeinsame Regeln ausarbeiten und diese dann von der Datenschutzbehörde genehmigen lassen. In diesen Datenschutzvorschriften müssen die Zweckbindung, Speicherfristen, Technikgestaltung, Rechtsgrundlagen etc. geregelt werden. Diese Richtlinien – so sie von der Datenschutzbehörde genehmigt werden – sind dann eine rechtmäßige Grundlage für Datentransfers in Drittländer.
Die österreichische Datenschutzbehörde hat einige datenschutzrechtliche Verhaltensrichtlinien genehmigt, wobei die Richtlinien der Berufsvereinigung der Arbeitgeber:innen privater Bildungseinrichtungen

waren 2019 eine der ersten. Mittlerweile folgten weitere, beispielsweise der Code Of Conduct der Internet Service Provider Austria, des Vereins der E-Wirtschaft bezüglich Smart-Meter oder auch der Fachverband der Versicherungsmakler.
Es ist ratsam, dass sich Betriebsrätinnen oder Betriebsräte bei der Erstellung solcher Richtlinien einbringen. Im ersten Entwurf der DSGVO war eine solche Mitbestimmung seitens der Betriebsräte noch enthalten, diese ging im Laufe des Verhandlungsprozesses aber leider verloren.

Datenschutzvorschriften für Konzerne

Artikel 46 Abs 2 lit b und Artikel 47 DSGVO

Datenschutzvorschriften werden in der Regel unternehmensintern und einseitig von der Geschäftsführung festgelegt. Die Datenschutzbehörde muss diese Vorschriften genehmigen und danach darf das Unternehmen den Datentransfer starten. Eigentlich sind diese – auch **„Binding Corporate Rules"** genannten – Vorschriften von Vorteil für Unternehmen, weil diese dann nicht mit jedem oder jeder einzelnen Geschäftspartner:in eigene Verträge zum Datenschutz abschließen müssen.

Zertifizierungen

Artikel 42 DSGVO

Neu ist, dass es Zertifizierungen für Unternehmen gibt, auf deren Basis der Datentransfer in Drittstaaten rechtlich möglich ist. Dazu ernennt die Datenschutzbehörde eigene Stellen (= Akkreditierung), die dann ihrerseits die Unternehmen prüfen und ihnen gegebenenfalls das positive Prüfungsergebnis bescheinigen. Eine solche Zertifizierungsstelle muss unparteiisch und unabhängig sein. Wie genau eine solche Zertifizierungsstelle aussehen muss, hat die Datenschutzbehörde im Februar 2021 in einer eigenen Verordnung festgelegt (Verordnung über die Anforderungen an die Akkreditierung einer Zertifizierungsstelle; ZeStAkk-V). In Österreich gibt es derzeit die Zertifizierungsstelle „Certification and Information Security Services GmbH" (CIS).
Die Prüfung eines Unternehmens erfolgt in der Regel auf Basis der ISO-Norm 27001, die den internationalen Prüfstandard für Datenschutzzertifikate darstellt. Bei diesem EU-„Datenschutzsiegel" könnte man salopp auch von einem „Datenschutz-TÜV-Pickerl" sprechen.

Behördliche Dokumente und Verwaltungsvereinbarungen

Behörden und öffentliche Stellen können Dokumente erstellen, die als Rechtsgrundlage für den Datentransfer zu Behörden in Dritt-Staaten dienen (Artikel 46 Abs 2 lit a DSGVO) oder auch „Verwaltungsvereinbarungen" mit den jeweiligen Empfänger:innen abschließen (Artikel 46 Abs 3 DSGVO). Diese Verträge müssen von der Datenschutzbehörde genehmigt werden.

BETRIEBLICHE:R DATENSCHUTZBEAUFTRAGTE:R

Artikel 37–39 und Erwägungsgrund 97 DSGVO

Deutschland hatte als einziges EU-Mitglied in seinem Bundesdatenschutzgesetz (BDSG) bereits 1977 den betrieblichen Datenschutzbeauftragten eingeführt. Im sogenannten „Ulmer Urteil" wurden die Kompetenzen des/der betrieblichen Datenschutzbeauftragten 1990 für Deutschland festgeschrieben. In Österreich gab es immer wieder Versuche ebenfalls eine:n verpflichtende:n betriebliche:n Datenschutzbeauftragte:n einzuführen, die aber regelmäßig mit dem Argument, dies wäre für Betriebe ein zu großer bürokratischer Aufwand, nicht umgesetzt wurden. Auch auf europäischer Ebene verlief die Etablierung des/der betrieblichen Datenschutzbeauftragten nicht ganz reibungslos.

Ein:e betriebliche:r Datenschutzbeauftragte:r muss unbedingt ernannt werden, wenn:

- es sich um eine Behörde handelt (mit Ausnahme von Gerichten)
- die Kerntätigkeit eine umfangreiche, regelmäßige und systematische Datenverarbeitung ist (z. B. Videoüberwachung im öffentlichen Raum)
- die Kerntätigkeit die Datenverarbeitung besonderer Kategorien personenbezogener Daten umfasst (z. B. Spital)

Zu den Aufgaben eines/einer betrieblichen Datenschutzbeauftragten zählen die **Kontrolle**, ob die DSGVO eingehalten wird, die Beratung des Managements, aber auch die **Schulung und Information** der Beschäftigten sowie der Kund:innen. Der/die betriebliche Datenschutzbeauftragte ist die Schnittstelle zur Aufsichtsbehörde. Der Name der/des Datenschutzbeauftragten muss der Behörde bekannt gegeben werden.

Betriebliche Datenschutzbeauftragte sind allerdings nicht diejenigen, die für sämtliche Verstöße gegen die DSGVO haften. Sie haben nämlich keine Durchsetzungsmacht, sollte der Verantwortliche die Empfehlungen nicht umsetzen.

Haftet der/die betriebliche Datenschutzbeauftragte, falls Bußgelder verhängt werden?

NEIN, der/die betriebliche Datenschutzbeauftragte kann nicht bestimmen, wie das Unternehmen mit personenbezogenen Daten umgeht. Er/sie kann beraten, überwachen, schulen, mit der Datenschutz-Behörde zusammenarbeiten und Ähnliches. Daher haftet er/sie auch nicht – außer er/sie vernachlässigt seine/ihre Pflichten, überschreitet seine/ihre Aufgabenbereiche, verletzt selbst Datenschutzbestimmungen, oder Ähnliches.

Betriebliche Datenschutzbeauftragte mit Gewerkschaftsmitgliedschaft genießen umfassende Versicherungsleistungen aus dem ÖGB-Berufs- und Rechtsschutzpaket. Sollte ein Gewerkschaftsmitglied in Ausübung der Aufgaben als betriebliche:r Datenschutzbeauftragte:r also mit einer Haftungsklage bedroht sein, sollte er/sie sich umgehend an den Rechtsschutz der Gewerkschaft GPA wenden.

Der/die betriebliche Datenschutzbeauftragte (mitunter auch „Privacy Officer" genannt) ist weisungsungebunden und hat einen gewissen Kündigungsschutz. Er/Sie darf auch nicht abberufen oder benachteiligt werden, bloß weil er/sie die gesetzlich vorgegebenen Aufgaben erfüllt. Einem Konzern mit mehreren Niederlassungen in der EU steht es frei auch nur eine Person in der Hauptniederlassung ernennen – vorausgesetzt diese kann ihre Aufgaben tatsächlich erfüllen, was schon allein sprachlich eine Herausforderung sein könnte.

Ein:e betriebliche:r Datenschutzbeauftragte:r muss über die notwendige Sachkenntnis im Datenschutz und über Berufserfahrung verfügen. Die meisten Ausbildungsstellen bieten in etwa einwöchige Kurse ab etwa 2.000 Euro aufwärts an und halten sich bei ihrem Curriculum an die ISO 17024. Billigere Ausbildungsangebote mit zweitägigen „Crash-Kursen" gilt es eher zu vermeiden.

Mitunter werden Betriebsrät:innen auch zum oder zur betrieblichen Datenschutzbeauftragten ernannt. Seitens der Gewerkschaft GPA wird davon abgeraten, da zwangsläufig Rollenkonflikte entstehen da der Betriebsrat von der Belegschaft gewählt wird, der betriebliche Datenschutzbeauftragte hingegen von der Unternehmensleitung bestellt wird.

Kann ein Betriebsrat auch betrieblicher Datenschutzbeauftragter sein?

NEIN, sagen das Bundesarbeitsgericht Dresden sowie das Landesgericht Sachsen, woraufhin die Frage dem Europäischen Gerichtshof zur Entscheidung vorgelegt wird. Der sagt 2023 auch „eher nein", weil er durch die Kombination der beiden Funktionen durchaus einen potenziellen Interessenkonflikt sieht und gibt die Entscheidung an das Landesgericht zurück. Es bleibt spannend.

Muss der Betriebsrat dem/der betrieblichen Datenschutzbeauftragten die Datenverarbeitungen des Betriebsrates offenlegen?

NEIN, der Betriebsrat ist ein eigenständiges, weisungsungebundenes Gremium, das die Interessen der Arbeitnehmer:innen vertritt. Daher ist ein:e von dem/der Arbeitgeber:in bestellte:r betriebliche:r Datenschutzbeauftragte:r nicht berechtigt, die Datenverarbeitungen des Betriebsrats zu kontrollieren.

BESCHÄFTIGTENDATENSCHUTZ

Artikel 88 und Erwägungsgrund 155 DSGVO

Die DSGVO behandelt den Datenschutz am Arbeitsplatz in einem eigenen Artikel. Zwar gab es seit 2000 immer wieder Stimmen in Europa, die für einen eigenständigen Arbeitnehmer:innen-Datenschutz plädierten (z. B. 2001 von der Artikel-29-Datenschutzgruppe oder 2015 vom Europarat), doch erfolgreich war man damit leider nie. Die DSGVO stellt nun klar, dass die Verarbeitung von Beschäftigtendaten nicht unter „ferner-liefen" abzuhandeln ist, sondern eine spezielle Art der Datenverwendung darstellt.

Die DSGVO legt im Artikel 88 fest, dass die EU-Mitgliedstaaten auf nationaler Ebene spezifischere Regelungen für den Beschäftigten-Datenschutz schaffen können. Es handelt sich um eine sogenannte **„Öffnungsklausel"**. Der österreichische Gesetzgeber hat diese Möglichkeit genutzt und die Mitbestimmungs-, Beratungs- und Informationsrechte des Betriebsrats aus dem Arbeitsverfassungsgesetz (ArbVG) an die EU-Kommission gemeldet. (Es handelt sich dabei um eine sogenannte **„Notifizierung"**.)

Die im Arbeitsverfassungsgesetz verankerten Mitbestimmungsrechte des Betriebsrats sind Bestandteil der DSGVO.

Die DSGVO eröffnet die Möglichkeit kollektive Vereinbarungen (also Kollektivverträge und Betriebsvereinbarungen) abzuschließen, welche die Datenverarbeitung im Beschäftigungskontext regeln. In der DSGVO ist angeführt, welche Themen konkret in einer solchen kollektiven Vereinbarung geregelt werden können (z. B. im Zusammenhang mit Einstellung oder Beendigung des Arbeitsverhältnisses, zur Erfüllung des Arbeitsvertrags, zu Gesundheit und Sicherheit am Arbeitsplatz, bei der Planung und Organisation der Arbeit, etc.). Es steht also ein weites Spektrum zur Verfügung, innerhalb dessen sich der Betriebsrat betätigen kann (vgl. Kapitel Rechte des Betriebsrats, S. 24).
Der Artikel 88 zieht einen Standard ein, der dem Beschäftigtendatenschutz mehr Gewicht als bisher verleiht.

Muss selbst dann eine Betriebsvereinbarung abgeschlossen werden wenn man sich ohnehin an die DSGVO hält?
Oder anders gefragt: Kann die Einhaltung der DSGVO den Abschluss einer Betriebsvereinbarung ersetzen?

NEIN, die allfällig bestehende Verpflichtung eine Betriebsvereinbarung gemäß §§ 96-97 Arbeitsverfassungsgesetz abzuschließen, bleibt wie sie ist.

DATENSCHUTZ DURCH TECHNIK UND DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

Artikel 25 und Erwägungsgrund 78 DSGVO

Generell ist die DSGVO technikneutral. Das heißt, die Vorgaben sind einzuhalten, egal welche Technik zum Einsatz kommt. Egal ob Chats oder Text-Dokumente, Bilddaten oder Tonaufnahmen, Log-files oder Standorterfassung, sie alle unterliegen der DSGVO – außer sie erfolgen zu rein privaten Zwecken oder zur Aufdeckung von Straftaten (vgl. Artikel 2 Abs 2 DSGVO). Dieses ausgesprochen vielseitige Anwendungsgebiet überblicken und kontrollieren zu können, ist eine Herausforderung, die mit Hilfe technischer Vorgaben bewältigt werden soll. Durch „Datenschutzfreundliche Voreinstellungen" sollen eben diese technischen Aspekte adäquat berücksichtigt werden.
Zu den Pflichten des Verantwortlichen zählt es, für Datenschutz durch datenschutzfreundliche Voreinstellungen zu sorgen. Das bedeutet, dass die Technik von vornherein so gestaltet sein muss, dass die Privatsphäre der Nutzer:innen möglichst wenig beeinträchtigt wird. Technische Produkte, Smartphones, Apps, Spiele oder Software zur Personalverwaltung, sie alle sollen schon durch ihre Programmierung die Betroffenen möglichst gut schützen. Dieser Ansatz wird auch „Datenschutz durch Technik" genannt (oder englisch **„Privacy by design"**). Zusätzlich muss die Möglichkeit vorhanden sein, dass die Betroffenen selbst diejenigen Einstellungen vornehmen können, die sie schützen. Dieser Ansatz wird auch „Datenschutz durch datenschutzfreundliche Voreinstellungen" (oder englisch **„Privacy by default"**) genannt.

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

Artikel 24 und 25, Erwägungsgründe 74–78 sowie Artikel 32, Erwägungsgrund 83 DSGVO

In der DSGVO wurde versucht technikneutral zu bleiben (also alle technischen Anwendungsmöglichkeiten einheitlich zu berücksichtigen) und gleichzeitig auch einen Technikansatz zur Datensicherheit einzubauen. Zur Konkretisierung, was unter den Grundprinzipien Rechenschaftspflicht, Vertraulichkeit und Rechtmäßigkeit zu verstehen ist, wurde in der DSGVO festgelegt, dass technische und organisatorische Maßnahmen zu treffen sind.

Geeignete technische und organisatorische Maßnahmen müssen dem Stand der Technik entsprechen, es müssen aber auch die Kosten berücksichtigt werden. Die Verantwortlichen – also die Arbeitgeber:innen – müssen die Risiken für Datenmissbrauch herausfinden und dann Maßnahmen umsetzen, die diesen Risiken entgegenwirken.

Konkret können das beispielsweise sein:

- möglichst kurze Speicherfristen festsetzen
- ausschließlich jene Daten verwenden, die für die jeweiligen Zwecke wirklich erforderlich sind
- Pseudonymisierung einführen
- Systeme sicherer und belastbarer gestalten
- Daten nach einem Zwischenfall schnell wieder verfügbar machen
- Systeme vor Zugriff von unberechtigten Personen schützen
- Regelmäßige Evaluierung, Datenschutz-Audit durchführen
- Verschlüsselung verwenden, Datenschutz-Policy einführen und Beschäftigte unterweisen.

Der/Die Verantwortliche muss nachweisen können, dass angemessene Schutzmaßnahmen getroffen wurden. Dazu können Verantwortliche auch Verhaltensregeln von der Datenschutzbehörde genehmigen lassen (vgl. Artikel 40 DSGVO) oder sich einem von der Datenschutzbehörde genehmigten Zertifizierungsverfahren unterziehen (vgl. Artikel 42 DSGVO und Kapitel „Verhaltensrichtlinien“, Seite 17).

GELDBUSSEN

Artikel 82ff und Erwägungsgründe 146–151 DSGVO

Die DSGVO schreibt Bußgelder vor. Nachdem diese auch in Prozent des weltweiten jährlichen Unternehmensumsatzes verhängt werden können (vergleichbar mit Strafen aus dem EU-Wettbewerbsrecht), kommen weitaus höhere Summen zustande als bisher bei Verstößen gegen Datenschutzrecht ausgesprochen wurden.

Auftragsverarbeiter:innen werden ebenfalls in die Pflicht genommen und können für materielle (z. B. Geschäftsentgang) und immaterielle Schäden (z. B. Identitätsdiebstahl, Rufschädigung, etc.) ebenso belangt werden wie der/die Verantwortliche selbst.
Die Bußgelder können ein Höchstausmaß von **20 Millionen Euro oder vier Prozent des weltweiten Umsatzes** betragen und müssen wirksam, verhältnismäßig und abschreckend sein. Bei der Festlegung der Strafhöhe müssen folgende Aspekte berücksichtigt werden:

- Art, Schwere und Dauer des Verstoßes (hat man dem Datenmissbrauch mehrere Monate nichts entgegengesetzt, wird das Bußgeld wohl höher angesetzt werden)
- frühere Verstöße (gab es bereits einschlägige frühere Verstöße, wird das Bußgeld wohl höher sein)
- fahrlässiges oder vorsätzliches Verhalten (wurde „nur“ fahrlässig jedoch ohne Vorsatz gehandelt, wird das Bußgeld wohl niedriger sein)
- Datenarten (bei besonderen Datenkategorien wie beispielswese der Gewerkschaftszugehörigkeit wird das Bußgeld wohl höher sein)
- Anzahl der Betroffenen (bei einer großen Menge Betroffener wird das Bußgeld wohl höher sein)
- Maßnahmen zur Abhilfe (wenn sofort Abhilfe-Maßnahmen getroffen wurden, wird das Bußgeld wohl niedriger sein)
- Zusammenarbeit mit der Behörde (wenn die Behörde sofort involviert wurde, wird das Bußgeld wohl niedriger sein)
- interne Richtlinien (wenn interne Richtlinien zur Datenverarbeitung existieren und im Großen und Ganzen eingehalten wurden, wird das Bußgeld wohl niedriger sein)
- Sicherheitsmaßnahmen (wenn angemessene technische Maßnehmen gem. Artikel 32 DSGVO implementiert wurden, wird das Bußgeld wohl niedriger sein).

Es bleiben die datenschutzrechtlichen Tatbestände aus dem Strafrecht weiterhin aufrecht (z. B. Verletzungen der Privatsphäre und bestimmter Berufsgeheimnisse §§ 118 ff StGB).

EINWILLIGUNG UND BEWEISLASTUMKEHR

Artikel 7, Erwägungsgründe 32–33 und 42–44

Eine Rechtsgrundlage für eine Datenverwendung kann ist die Einwilligung seitens der Betroffenen (siehe S.11, Kapitel Rechtmäßigkeit). Zur Stärkung der individuellen Rechte ist die Einwilligung der Betroffenen streng definiert. Sie muss **freiwillig und eindeutig** sein, für einen **bestimmten** Fall erfolgen (es darf also keine Pauschal- oder Blanko-Unterschrift zu „irgendwie eh Allem" sein) und die Betroffenen müssen **über die Tragweite informiert** sein.
Sollten Unklarheiten auftreten, ob die Einwilligung tatsächlich erfolgt ist, muss der/die Verantwortliche beweisen, dass er/sie eine Einwilligung zur Datenverwendung erhalten hat. Relevant für die betriebliche Praxis wird das bei Daten im Betriebsratsbüro sein, wo sich der Betriebsrat fragen muss, ob es für Datenverwendungen, die über die aus dem ArbVG resultierenden Rechte und Pflichten hinausgehen, Einwilligungen der Beschäftigten vorliegen (z. B. Geburtstagslisten, Medikamentenbestellungen; siehe „Kapitel Daten im Betriebsratsbüro", S. 28).

Generell ist die Freiwilligkeit einer Einwilligung im Arbeitsverhältnis aufgrund des Machtungleichgewichts zwischen Arbeitgeber:innen und Arbeitnehmer:innen aber grundsätzlich zu hinterfragen. Das Kriterium „Freiwilligkeit" ist wesentlich, um eine Einwilligung als Rechtsgrundlage für Datenverarbeitungen heranziehen zu können. Nachdem echte Freiwilligkeit im Arbeitsverhältnis kaum zutreffen kann, ist in der Regel eine andere Rechtsgrundlage heranzuziehen (z. B. gesetzliche Verpflichtung).

VERTRETUNG VON BETROFFENEN UND NON-PROFIT-ORGANISATIONEN

Artikel 80 und Erwägungsgrund 142 DSGVO

Betroffene können sich mit ihren Anliegen und Beschwerden an Vereinigungen und Organisationen wenden, die den Datenschutz zu ihren Hauptanliegen zählen. Es müssen allerdings Vereine ohne Gewinnerzielungsabsicht sein (so genannte „Non-Profit-Organisationen", NPOs) und diese können dann im Auftrag aller Betroffenen, die sich gemeldet haben, den Fall vor die Datenschutzbehörde (DSB) oder vor Gericht bringen. Es werden dabei aber immer nur individuelle Rechte von den NPOs vertreten und leider keine kollektiven. Man könnte bei dieser Bestimmung daher von einer **„Verbandsklage light"** sprechen.

Eigentlich hätte man sich seitens der Interessenvertretung der Arbeitnehmer:innen das Recht auf eine richtige Verbandsklage gewünscht, bei der die Interessenvertretung von sich aus aktiv werden und Missstände anklagen kann (wie z. B. im Konsumentenschutzgesetz).

ONE-STOP-SHOP

Artikel 56, 60–67, 77 und Erwägungsgründe 130–141 DSGVO

Dieser Begriff soll verdeutlichen, dass die DSGVO eine für alle Mitgliedstaaten einheitliche Abwicklung in Datenschutzangelegenheiten vorsieht. Die EU-Bürger:innen werden nicht mehr von einer Aufsichtsbehörde zur nächsten geschickt, sondern „ein Stop" soll ausreichen. So muss beispielsweise eine Beschwerde wegen mangelnder Auskunft – auch wenn es ein Unternehmen im Ausland betrifft – nur bei jener Behörde gestellt werden, wo der oder die Betroffene wohnt. Um eine solche Beschwerde länderübergreifend zu bearbeiten, müssen sich die Behörden in Folge EU-intern koordinieren.

Das Prinzip des „One-stop-shop" findet sich auch bei der Ernennung des/der betrieblichen Datenschutzbeauftragten wieder (vgl. Kapitel „Betriebliche:r Datenschutzbeauftragte:r", S. 18), wo es ausreicht, wenn eine Unternehmensgruppe eine:n betriebliche:n Datenschutzbeauftragte:n an einem Ort ernennt (vgl. Artikel 37 Abs 2 DSGVO).

BENACHRICHTIGUNG BEI DATENSCHUTZ-VERLETZUNG

Artikel 33f DSGVO

Im Englischen wird eine solche Information **„Data-Breach-Notification"** genannt. Die Benachrichtigungspflicht für Verantwortliche ist ein Beispiel dafür wie Transparenz, Betroffenenrechte und informationelle Selbstbestimmung gestärkt werden.

Sollte bei einer Datenverarbeitung ein Missgeschick passieren (z. B. Daten von Girokonten in falsche Hände geraten, Patient:innendaten auf dem Postweg verloren gehen, sämtliche Mitgliederdaten auf der Website offen liegen etc.), so muss dies der Datenschutzbehörde gemeldet werden. Sollte ein „hohes Risiko" für die Betroffenen bestehen (wenn z. B. personenbezogene Gesundheitsdaten öffentlich werden), müssen sie über die Datenschutzverletzung informiert werden. Wäre eine individuelle Benachrichtigung zu aufwendig, kann stattdessen auch eine öffentliche Bekanntmachung vorgenommen werden.

Bei der Meldung an die Behörde bzw. der Information an die Betroffenen muss angegeben werden, was passiert ist, um welche Datenarten es sich handelt, wie viele betroffen sind, Name und Kontaktdaten des Verantwortlichen, was die Auswirkungen sein werden und welche Gegenmaßnahmen getroffen wurden.

DIE DATENSCHUTZBEHÖRDE (DSB)

Artikel 55–59, Erwägungsgründe 122–128 DSGVO

Jeder EU-Mitgliedsstaat hat eine **nationale Aufsichtsbehörde**, welche die Einhaltung des Datenschutzrechts kontrolliert. Vor Inkrafttreten der DSGVO hatten diese Behörden EU-weit unterschiedliche Aufgaben und Funktionen. Die einen durften beispielsweise Bußgelder selbst verhängen (z. B. deutsche Landesdatenschutzbeauftragte), andere nicht (z. B. Österreich). In der DSGVO sind die Datenschutzbehörden (DSB) nun einheitlich geregelt. Allerdings sind nach wie vor nationale Sonderregelungen möglich (sogenannte „Öffnungsklausel").

Die Aufgaben der Datenschutzbehörde sind:

- Aufklärung und Sensibilisierung der Öffentlichkeit
- Beratung von Parlament und Regierung
- Beantwortung von Anfragen der Betroffenen
- Beschwerden entgegennehmen und untersuchen
- Datenschutzüberprüfungen durchführen
- Verantwortliche auf vermutliche Datenschutzverstöße hinweisen
- Verantwortliche wegen Datenschutzverstößen
  - verwarnen
  - zurechtweisen
  - Fristen zur Beseitigung des Verstoßes setzen
  - Geldbußen verhängen (vgl. Kapitel Strafen)
- Liste jener Datenverarbeitungen erstellen, für die eine Datenschutz-Folgenabschätzung erforderlich ist (vgl. Kapitel „Datenschutz-Folgenabschätzung", S. 14)
- Verhaltensregeln/Binding Corporate Rules/Zertifizierungen (z. B. für Datenübermittlung in Drittländer) prüfen und genehmigen sowie Akkreditierungsstellen für die Zertifizierung benennen (vgl. Kapitel „Datentransfer in Drittstaaten", S. 16)
- Verzeichnis von Verstößen gegen die DSGVO führen
- Tätigkeitsbericht erstellen

ZUSAMMENARBEIT DER BEHÖRDEN

Artikel 60–67 und Erwägungsgründe 130–140 DSGVO

Es wird in der DSGVO betont, dass die nationalen Datenschutzbehörden untereinander zusammenarbeiten müssen, sei es bei der Information der Betroffenen, bei der Entscheidungsfindung im Zuge eines Verfahrens oder auch bei der Durchführung von Untersuchungen. Es wird also auf eine kohärente Auslegung der DSGVO über die Landesgrenzen hinweg viel Wert gelegt und die nationalen Datenschutzbehörden müssen für Einheitlichkeit sorgen. Der **Kohärenz** ist ein eigenes Kapitel der DSGVO gewidmet, in dem sämtliche Fristen und Modalitäten für die Zusammenarbeit – besonders bei gemeinsamen Beschlüssen – beschrieben sind.

RECHTE DES BETRIEBSRATS

Die DSGVO beinhaltet erstmalig auch einen Artikel zum Beschäftigtendatenschutz (Artikel 88 DSGVO). Dies ist durchaus als Errungenschaft im Sinne der Arbeitnehmer:innen zu qualifizieren, da dieser Bereich der Datenverarbeitung damit als ein besonderer bestätigt wird, der nicht wie alle anderen abgehandelt werden kann. Allerdings ist der Artikel „Datenverarbeitung im Beschäftigungskontext" eher bescheiden geblieben, wenn es um die konkreten Ausführungen geht – von einer Mitbestimmung der betrieblichen Interessenvertretung ganz zu schweigen.

Im Wesentlichen besagt Artikel 88 DSGVO, dass die Mitgliedsstaaten diese Datenverarbeitung national regeln können. Es steht im Erwägungsgrund 155 der DSGVO: „Im Recht der Mitgliedstaaten oder in Kollektivvereinbarungen (einschließlich ‚Betriebsvereinbarungen') können spezifische Vorschriften für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorgesehen werden (...)". Somit ist gesichert, dass die bestehenden Regelungen aufrecht bleiben und auch in Zukunft in der Betriebsvereinbarung oder im Kollektivvertrag der Beschäftigtendatenschutz vereinbart werden muss und kann. Dies ist außerdem dadurch sichergestellt, dass das Arbeitsverfassungsgesetz (ArbVG) als Teil der DSGVO an die EU-Kommission gemeldet wurde.

Dem Betriebsrat steht ein ganzes „Werkzeuglager" auf Basis des ArbVG zur Verfügung, um den Beschäftigten – bildlich gesprochen – Schutzvorrichtungen zu bauen, also sie vor übermäßiger Kontrolle zu bewahren und ihre Grundrechte auf Privatsphäre, Meinungsfreiheit aber auch den Schutz personenbezogener Daten zu gewährleisten.

Ein kurzer Überblick über die Werkzeuge der Betriebsratsarbeit:

- Allgemeines Überwachungsrecht (§ 89 ArbVG)
- Allgemeines Recht auf Anhörung und Intervention (§ 90 ArbVG)
- Informationspflicht des/der Betriebsinhaber:in (§ 91 ArbVG, insb. Abs 2)
- Allgemeines Beratungsrecht (§ 92 ArbVG)
- Mitwirkungsrechte
  - Zustimmungspflichtige Maßnahmen, d.h. die Maßnahme ist ohne Zustimmung des Betriebsrats nicht rechtswirksam, sogenannte „notwendige" Betriebsvereinbarung (§ 96 ArbVG)
    - Betriebliche Disziplinarordnung (wenn z. B. die Verhaltensrichtlinie mit Sanktionen zur Disziplinarordnung ausgebaut wird; § 96 Abs 1 Z 1 ArbVG)
    - Personalfragebögen (wenn nicht nur allg. Angaben abgefragt werden; § 96 Abs 1 Z 2 ArbVG)
    - Kontrollmaßnahme (wenn sie die Menschenwürde berührt; § 96 Abs 1 Z 3 ArbVG)
  - durch die Schlichtungsstelle ersetzbare Zustimmung des Betriebsrates, d. h. auch diese Maßnahmen oder Systeme sind ohne eine Zustimmung seitens des Betriebsrats/der Schlichtungsstelle nicht rechtswirksam (§ 96a ArbVG)

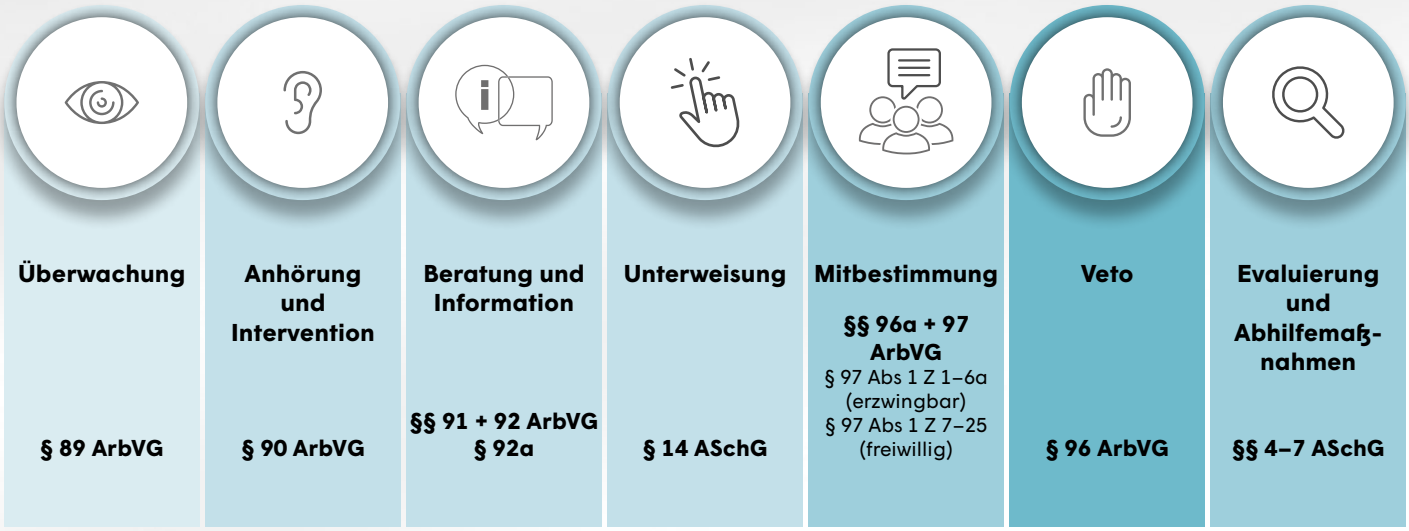
  - Systeme mit personenbezogenen ArbeitnehmerInnen-Daten (§ 96a Abs 1 Z 1 ArbVG)
  - Beurteilungssysteme (§ 96a Abs 1 Z 2 ArbVG)
- vor der Schlichtungsstelle erzwingbare Betriebsvereinbarungen
  - Ordnungsvorschriften (§ 97 Abs 1 Z 1 ArbVG)
  - Nutzung der Betriebsmittel (§ 97 Abs 1 Z 6 ArbVG)
- „Freiwillige" Betriebsvereinbarung, d. h. die Schlichtungsstelle hat hier keine Befugnis, Betriebsinhaber:in und Betriebsrat müssen sich einigen (§ 97 Abs 1 Z 7-27 ArbVG)
  - Menschengerechte Arbeitsgestaltung (§ 97 Abs 1 Z 9 ArbVG)
  - Leistungs- und erfolgsbezogene Prämien (§ 97 Abs 1 Z 16 ArbVG)
  - Maßnahmen zur Sicherung der Arbeitsmittel und Gegenstände, die dem/der
  - Arbeitnehmer:in gehören (§ 97 Abs 1 Z 17 ArbVG)
  - Betriebliche Bildungsmaßnahmen (§ 97 Abs 1 Z 19 ArbVG)

Kurze Erläuterungen zu den Rechten des Betriebsrats: Da wäre zuerst einmal das **allgemeine Überwachungsrecht** (§ 89 ArbVG): Der Betriebsrat hat die Einhaltung jener Rechtsvorschriften zu überwachen, die die Beschäftigten betreffen. Dazu zählen zweifellos auch die DSGVO und das DSG.

Das **allgemeine Interventionsrecht** (§ 90 ArbVG) beinhaltet das Recht, Vorschläge zu machen, wie die Arbeitssituation der Beschäftigten verbessert werden kann. Diese Vorschläge des Betriebsrates muss sich der oder die BetriebsinhaberIn zumindest anhören. Der Betriebsrat kann demnach vorschlagen, wie man Datenschutzmaßnahmen im Betrieb gestalten sollte, welche Ansprechpartner:innen zur Verfügung stehen sollten, wie in Verdachtsfällen auf missbräuchliche Datenverwendung vorgegangen werden sollte etc.

Es besteht weiters ein **allgemeines Informationsrecht** (§ 91 Abs 2 ArbVG). Seit 1986 umfasst dieses Informationsrecht ausdrücklich, dass der/die Betriebsinhaber:in „Mitteilung zu machen (hat), welche Arten von personenbezogenen Arbeitnehmerdaten er automationsunterstützt aufzeichnet und welche Verarbeitungen und Übermittlungen er vorsieht." Die Begriffe „personenbezogene Daten", „Datenverarbeitungen" und „Übermittlungen" sowie „automationsunterstützt" entsprechen denen der DSGVO und des DSG. Es war dem Gesetzgeber offensichtlich bewusst, dass konkrete Angaben zu Datenverarbeitungen spezielle Informationen erfordern, die ohne explizites Nachfragen des Betriebsrates von dem/der Arbeitgeber:in selbsttätig bereitgestellt werden müssen. Es handelt sich also um eine sogenannte „Bringschuld" des Arbeitgebers oder der Arbeitgeberin. Dass derartige Informationen in einer digitalisierten

INSTRUMENTE DES BETRIEBSRATS



Gewerkschaft GPA

Arbeitswelt ganz wesentlich sein werden, kann als weise Voraussicht des Gesetzgebers interpretiert werden.

Das **Beratungsrecht** des Betriebsrates besteht allgemein in sozialer, personeller, wirtschaftlicher und – hier wird es bezüglich Beschäftigten-Datenschutz interessant – **technischer Hinsicht** (§ 92 ArbVG). Also kann der Betriebsrat eine Beratung darüber verlangen, welche Technik zukünftig im Betrieb eingesetzt werden soll, welche Auswirkungen diese haben wird, wer davon betroffen sein wird etc.

Das wohl stärkste „Arbeitsgerät" im „Werkzeugkoffer" ist auch in datenschutzrechtlichen Angelegenheiten das **Vetorecht** des Betriebsrates bei bestimmten Maßnahmen (§ 96 Abs 1 Z 2 und 3 ArbVG). Der Betriebsrat kann davon Gebrauch machen, wenn umfassende Personalfragebögen eingesetzt werden, die nichts mit der direkten Verwendung und Qualifikation der Beschäftigten zu tun haben. Spätestens wenn die Unternehmensführung eine Kontrollmaßnahme anordnet, welche die Menschenwürde berührt (beispielsweise permanente Videoüberwachung, Tastatur-Anschlags-Protokolle oder Ortung), wird das betriebsrätliche Veto bedeutsam werden.
Die **Mitbestimmungspflicht** des Betriebsrates kommt auch dann zum Tragen, wenn *„Systeme zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen"* eingesetzt werden (§ 96a ArbVG) – also in der heutigen digitalen Arbeitsrealität sehr häufig.

Bei Beurteilungssystemen, die mehr als die betriebliche Verwendung umfassen (z. B. Persönlichkeitsprofile, psychologische Tests), muss das Mitbestimmungsrecht des Betriebsrates berücksichtigt werden (§ 96a Abs 1 Z 2 ArVG). Derartige Systeme müssen mit einer Betriebsvereinbarung geregelt werden; ohne entsprechende Betriebsvereinbarung sind sie nicht legal. Sollte man innerbetrieblich bei diesen Verhandlungen auf keinen grünen Zweig kommen, ist der Weg zur Schlichtungsstelle möglich.

Keine Mitbestimmungspflicht nach § 96a Absatz 1 Ziffer 1 ArbVG besteht dann, wenn ausschließlich gesetzliche Pflichten mit der Datenverwendung erfüllt werden.

Muss selbst dann eine Betriebsvereinbarung abgeschlossen werden, wenn die Datenverwendung zum Vorteil der Arbeitnehmer:innen erfolgt, z. B. damit Prämien ausgezahlt werden können?

JA, eine Betriebsvereinbarung ist unabhängig davon abzuschließen, wer von der Datenverwendung profitiert. Schließlich könnte sonst das Grundrecht auf Datenschutz gegen etwaige finanzielle – oder andere – Vorteile „verkauft" werden. Die Verpflichtung zum Abschluss einer Betriebsvereinbarung ist vielmehr davon abhängig, was ein System kann, d.h. die „objektive Eignung" zur Kontrolle ist ausschlaggebend, und nicht, ob jemand dadurch einen – angeblichen – Vorteil hat.

Im Zusammenhang mit dem Beschäftigtendatenschutz sind weiters erzwingbare Betriebsvereinbarungen in der Praxis abzuschließen, welche die zweckentsprechende **Benutzung von Betriebsmitteln** regeln (z. B. Laptop, Smartphone etc. – vgl. § 97 Abs 1 Z 6 ArbVG).

Bei **allgemeinen Ordnungsvorschriften** kann der Betriebsrat eine Betriebsvereinbarung erzwingen (z. B. zu IT-Richtlinien oder Compliance-Regeln – vgl. § 97 Abs 1 Z 1 ArbVG). Maßnahmen zur **menschengerechten Arbeitsgestaltung** können mit einer Betriebsvereinbarung geregelt werden (z. B. gegen Arbeitsverdichtung durch permanente Erreichbarkeit, für die Trennung von Arbeitszeit und Freizeit etc. – vgl. § 97 Abs 1 Z 9 ArbVG). Während sich die DSGVO dem Schutz personenbezogener Daten widmet, ist das Arbeitnehmer:innenschutzgesetz (ASchG) für den Schutz der Gesundheit zuständig. Diese beiden Ziele haben gemeinsam, dass sie eine regelmäßige Beobachtung und Anpassung des Ist-Stands erfordern. In der DSGVO ist das die Datenschutzfolgenabschätzung (siehe S. 14) im ASchG ist das die Evaluierung gesundheitlicher Risiken am Arbeitsplatz (§ 4 ff ASchG).
Der Betriebsrat hat also zwei gesetzliche Grundlagen, auf die er sich berufen kann, um eine **Evaluierung** gemeinsam mit der Unternehmensleitung zu vereinbaren.

Wie kann ich als Betriebsrat das alles überhaupt kontrollieren?

Für den Betriebsrat bietet die DSGVO zwar viele Ansatzpunkte, aber kaum konkrete Handlungsvorgaben. Die Rechte des Betriebsrates sind im Arbeitsverfassungsgesetz (ArbVG) festgelegt. Dort sind die betriebsrätlichen Rechte auf Beratung (§ 92 ArbVG), Information (§ 91 ArbVG) und Mitbestimmung (§ 96, 96a und 97 ArbVG) verankert. Die DSGVO regelt im Artikel 88, dass es einen eigenen Beschäftigtendatenschutz geben kann, dass dazu Kollektivvereinbarungen und Betriebsvereinbarungen abgeschlossen werden können und schlägt vor, in welchen Bereichen kollektive Regelungen getroffen werden können (z. B. Überwachung, Gesundheit und Sicherheit am Arbeitsplatz, Einstellung, Planung und Organisation der Arbeit etc.). Der Betriebsrat legt am besten seine Kontrollrechte in der Betriebsvereinbarung mittels technischer und organisatorischer Maßnahmen (TOM) fest.

Mit zunehmender technischer Entwicklung, zunehmender Geschwindigkeit der Updates, zunehmendem Datenverkehr zwischen allen Beteiligten steigt die Gefahr für missbräuchliche Datenverwendungen. Die Kontrollmöglichkeiten sind eine häufig vorgebrachte Frage. Die Kontrolle des Beschäftigtendatenschutzes ist ein hoher Anspruch an die Betriebsratsarbeit. Man wird von keinem Betriebsrat erwarten können, dass er sämtliche digitalen Systeme am Arbeitsplatz, von der Videokamera über die Firmenhandys bis hin zu den Apps von Microsoft 365 als Anwender:in und Administrator:in beherrscht und daher in jedem Detail kontrollieren kann. Mit einem solchen Perfektionsanspruch ist niemandem geholfen. Eine einhundertprozentige Kontrolle kann es weder auf Arbeitgeberseite geben, noch kann eine solche realistischer Weise vom Betriebsrat erwartet werden. Rechtliches Regelwerk, wie Gesetze und Betriebsvereinbarungen sind dazu da, den Datenverkehr zu regeln und sollten daher unbedingt auch genutzt werden.
Der Gegenentwurf wäre allerdings, dass sich niemand damit beschäftigt, was mit den personenbezogenen Daten der Beschäftigten passiert, zu welchen Unternehmen sie weitergeleitet werden, was gesammelt wird, wie lange gespeichert wird, welche Auswertungen der/die Arbeitgeber:in macht ... Einen solchen „Normalzustand" gilt es zu vermeiden und stattdessen eine möglichst gute Datenschutzkultur im Betrieb zu etablieren.

Das kann gelingen, indem der BR eine oder mehrere Optionen nutzt:

- Übersicht über Auswertungen
- eigene Berechtigung für die Software
- regelmäßige Routinekontrollen
- Einsicht in die Ergebnisse von Überwachung der Beschäftigten.

Es bestehen gute rechtliche Regelungen wie Beschäftigten-Datenschutz aussehen soll, diese müssen in die Praxis umgesetzt werden. Wenn der Betriebsrat oder die Betriebsrätin seine/ihre Rechte in Anspruch nimmt, Informationen einfordert, mitbestimmt und gegebenenfalls das Vetorecht nutzt, dann kann die Privatsphäre der Arbeitnehmer:innen am Arbeitsplatz geschützt werden.

DATEN IM BÜRO DES BETRIEBSRATS

Sollte der Betriebsrat selbst Datenverwendungen durchführen, also personenbezogene Daten der Beschäftigten verarbeiten, dann ist er **Verantwortlicher** im Sinne der DSGVO. Verbreitet sind im Betriebsratsbüro personenbezogene Datenverarbeitungen beispielsweise bei Geburtstagslisten, Apothekenbestellungen, Rabatt- und Gutschein-Aktionen, Betriebsausflugsorganisation oder Zuschüssen zu besonderen Anlässen wie Geburten oder Eheschließungen. Wenn betriebsratsseitig aber lediglich mitliest (z. B. in der SAP-Personalverwaltung) oder wenn er ausschließlich gesetzlich vorgegebene Pflichten erfüllt (z. B. Kontrolle, ob Arbeitnehmer:innen richtig eingestuft wurden), dann ist er kein Verantwortlicher im Sinne der DSGVO.

Wenn es also im Betriebsratsbüro eigene, von dem/der Arbeitgeber:in unabhängige Akten, Excel-Listen, Datenbanken oder Ähnliches gibt, dann treffen auch den Betriebsrat datenschutzrechtliche Pflichten. Dazu zählt, dass ein Verarbeitungsverzeichnis angelegt werden muss (siehe Kapitel „Verzeichnis der Verarbeitungstätigkeiten", S. 14), dass Auskünfte an die Betroffenen erteilt werden müssen (siehe Kapitel Betroffenenrechte) und dass allfällige Folgenabschätzungen (siehe Kapitel „Datenschutz-Folgenabschätzung" (DSFA), S. 14) durchgeführt werden müssen.

Anders formuliert, der Betriebsrat muss sich fragen:

- Gehen meine Datenverwendungen über gesetzliche Pflichten hinaus?
- Habe ich eigene Datenverwendungen, die unabhängig vom Arbeitgeber/der Arbeitgeberin sind?

Werden diese Fragen mit „JA" beantwortet, so müssen die Pflichten der Verantwortlichen auch vom Betriebsrat eingehalten werden.

Muss sich der Betriebsrat an die DSGVO halten?

JA, ganz besonders wenn er eigene Datenverwendungen durchführt, die nicht direkt aus den gesetzlichen Rechten und Pflichten des Betriebsrats resultieren. Der Betriebsrat darf für die Zwecke der Arbeitnehmer:innenvertretung bestimmte personenbezogene Daten jedenfalls verarbeiten (z. B. ist ihm/ihr Einsicht in die Arbeitszeitaufzeichnung, die Qualifikation, die Einstufung, das Gehalt etc. zu erteilen). Die Gewerkschaft GPA hat ein Dokument zu den Einsichtsrechten des Betriebsrats zusammengestellt, das bei den betriebsbetreuenden Kolleg:innen erhältlich ist.

Besitzt der Betriebsrat eigene Datenverwendungen muss er sich bei deren Verarbeitung an die Grundprinzipien des Datenschutzes halten, darf also die Daten nur für die Zwecke verwenden für die sie vorgesehen sind, muss die Daten sparsam verwenden usw.

Die Listen der Teilnehmer:innen an Betriebsausflügen, auf denen eventuell auch Angehörige namentlich

erwähnt sind, oder die vergünstigten Medikamentenbestellungen, die vielleicht namentlich an die Apotheke weitergeleitet werden, sind eigene Datenverarbeitungen und der Betriebsrat ist dafür verantwortlich, muss sich also um die Einhaltung der DSGVO im eigenen Büro kümmern (z. B. indem er ein Verfahrensverzeichnis anlegt, Aufbewahrungsfristen festlegt, personenbezogene Daten nicht weitergibt etc.).

Im Betriebsratsbüro muss dafür gesorgt sein, dass

- Auskunft über die eigenen Datenverwendungen gegeben werden kann (Verwendungszweck, Datenkategorien, Empfänger, Aufbewahrungsfristen),
- Verantwortliche genannt werden,
- Löschfristen eingehalten werden,
- allenfalls ein Verarbeitungsverzeichnis geführt wird (wenn mehr als 250 Personen betroffen sind, besondere Datenkategorien verarbeitet werden oder nicht nur gelegentlich personenbezogene Daten verarbeitet werden)

RECHTSPRECHUNG ZUR DSGVO

WAS SAGEN EUROPÄISCHER GERICHTSHOF UND DATENSCHUTZ-BEHÖRDEN

Die Europäische Datenschutzgrundverordnung (DSGVO) ist seit sechs Jahren in Kraft. Immer wieder setzen sich Gerichte und zuständige Behörden in Verfahren und Auskunftsbegehren damit auseinander oder klären generelle Fragen zur Auslegung (im Verfahren vor dem Europäischen Gerichtshof (EuGh) so genannte „Vorabentscheidungen"). So gewinnt man mit den Jahren immer klarere Einsichten, wie die DSGVO im Alltag anzuwenden ist. Ab und an betreffen diese Urteile und Entscheidungen das Arbeitsverhältnis. Einige der wichtigsten Rechtsprechungen, die das Arbeitsverhältnis und die Betriebsratsarbeit betreffenden, sind hier ausgewählt, um Betriebsrät:innen zu unterstützen, wenn sie für einen besseren Beschäftigtendatenschutz im Unternehmen argumentieren wollen.

AUSKUNFT AN DIE BETROFFENEN: MUSS DIE EMPFÄNGER BEINHALTEN

Europäischer Gerichtshof, 12. Jänner 2023, C-154/21

Der Betriebsrat oder die Betriebrätin hat durch das Arbeitsverfassungsgesetz und die Rechtsprechung garantierte Informationsrechte. Zusätzlich stehen ihm/ihr – abseits ihrer Rolle als Betriebsratsmitglied – auch als Betroffene Auskunftsrechte nach der DSGVO zu. Immer wieder wird Betriebsrät:innen – pikanter Weise unter Berufung auf „den Datenschutz" – die Auskunft verweigert und immer wieder erhalten Betroffene nur unzureichend Auskunft über die Verwendung ihrer Daten. Ein Österreicher hat sich deshalb an den EuGH gewandt.

Der Stein des Anstoßes war, dass die Verantwortliche, die Österreichische Post AG, keine Auskunft darüber geben wollte – oder nach eigener Darstellung: nicht konnte – an wen genau die personenbezogenen Daten weitergegeben worden waren. „Politische Parteien" war dem Betroffenen nicht ausreichend und er reichte Beschwerde ein, vorerst nur bei der österreichischen Datenschutzbehörde, dann auch beim EuGh.

Der EuGh stellte klar, dass eine Auskunftsbeantwortung auch Empfänger enthalten muss und nicht bloß allgemeine Angaben. Wenn die auskunftsbegehrende Person diese Angaben braucht um ihre Rechte geltend zu machen, ist der oder die Verantwortliche verpflichtet, die Identität der Empfänger:innen mitzuteilen. Es sei denn, dass es entweder nicht möglich ist, die Empfänger:innen zu identifizieren oder die Verantwortlichen nachweisen können, dass die Anträge auf Auskunft offenkundig unbegründet oder exzessiv sind.

Falls also ein:e Arbeitnehmer:in oder ein Betriebsrat/eine Betriebsrätin (in seiner/ihrer Eigenschaft als betroffene:r Arbeitnehmer:in) ein Auskunftsbegehren gegenüber dem/der Arbeitgeber:in stellt, das er oder sie braucht um damit weitere Rechte (z. B. auf Löschen der Daten) einzufordern, sind Namen und Adressen von Empfänger:innen anzugeben.

BETRIEBLICHE:R DATENSCHUTZBEAUFTRAGTE:R: PASST NICHT ZUSAMMEN MIT BETRIEBSRATSTÄTIGKEIT

Europäischer Gerichtshof, 9. Februar 2023, C-453/21

In der DSGVO ist festgelegt, dass betriebliche Datenschutzbeauftragte ihre Aufgabe weisungsfrei auszuüben haben. Betriebliche Datenschutzbeauftragte dürfen aufgrund der ordnungsgemäßen Erfüllung ihrer Aufgaben nicht abberufen oder benachteiligt werden. Allerdings ist kein genereller Kündigungsschutz für Datenschutzbeauftragte vorgesehen. Das deutsche Beschäftigtendatenschutzgesetz geht in diesem Zusammenhang jedoch noch über die Regelungen der DSGVO hinaus und besagt, dass die Abberufung von Datenschutzbeauftragten nur aus wichtigem Grund erfolgen darf.

Die X-FAB Dresden GmbH & Co. KG sah einen Interessenkonflikt gegeben, da ein Arbeitnehmer zeitgleich als Datenschutzbeauftragter und als Betriebsratsvorsitzender tätig war. Das Unternehmen sah sich aus wichtigem Grund berechtigt, den Arbeitnehmer von seiner Tätigkeit als Datenschutzbeauftragten abzuberufen. Der betroffene Arbeitnehmer konnte den wichtigen Grund nicht erkennen und klagte.

Der EuGH hatte im Rahmen eines Vorabentscheidungsersuchens insbesondere zu klären, ob eine derartige Vorschrift wie im deutschen Beschäftigtendatenschutzgesetz gegen die DSGVO verstößt und ob bei einer gleichzeitigen Tätigkeit eines Datenschutzbeauftragten als Betriebsratsvorsitzender ein Interessenkonflikt vorliegt. Zunächst entschied der EuGH, dass eine nationale Regelung, die die Abberufung eines Datenschutzbeauftragten an strengere Voraussetzungen als in der DSGVO vorgesehen knüpft, nicht gegen Unionsrecht verstößt, also grundsätzlich zulässig ist. Außerdem hielt der EuGH fest, dass durch bestimmte Aufgaben oder Pflichten, die einem Datenschutzbeauftragten zusätzlich übertragen werden, ein „Interessenkonflikt" bestehen kann (wenn dadurch die Zwecke und Mittel der Verarbeitung personenbezogener Daten bei dem Verantwortlichen oder seinem Auftragsverarbeiter bestimmt werden können). Ob die Tätigkeit als Betriebsratsvorsitzender bei gleichzeitig mit der Funktion des Datenschutzbeauftragten ausgeübt werden können oder ob das einen Interessenkonflikt darstellt, der zur Abberufung (als Datenschutzbeauftragter) berechtigt, ist jedoch im Einzelfall zu prüfen und hängt von den konkreten Umständen im Betrieb ab.

Die Gewerkschaft GPA rät daher nach wie vor davon ab, beide Funktionen unter einen Hut bringen zu wollen. Es mag verlockend erscheinen, dadurch Zugang zu speziellem Knowhow zu gelangen oder in Entscheidungen stärker eingebunden zu werden, doch beinhalten die beiden Funktionen schlicht unterschiedliche Interessen (der Betriebsrat wird von den Arbeitnehmer:innen gewählt, der Datenschutzbeauftragte wird von der Unternehmensleitung berufen) und das kann zu – unvereinbaren – Widersprüchen führen.

ENTSCHEIDUNG AUSSCHLIESSLICH AUF BASIS MASCHINELLER BERECHNUNGEN: UNTERSAGT (PROFILING-VERBOT)

Europäischer Gerichtshof, 7. Dezember 2023, C-634/21

Dass in der DSGVO ein sogenanntes „Profilingverbot" besteht (Artikel 22) ist nicht neu. Es ist untersagt, dass schwerwiegende Entscheidungen ausschließlich aufgrund maschinell berechneter Aussagen getroffen werden. Nun gibt es dazu auch Rechtsprechung des EuGH.

Ausgangspunkt war eine Beschwerde gegen die deutsche SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung, vergleichbar mit dem Kreditschutzverband von 1870 in Österreich). Eine Betroffene wollte von der Bank wissen, warum und aufgrund welcher Daten ihr Kredit abgelehnt wurde. Sie wurde von der Bank an die Kreditauskunftei verwiesen, um zu erfahren, welche Daten in die Berechnung ihrer Kreditwürdigkeit einfließen. Die SCHUFA berief sich auf das Geschäftsgeheimnis und gab nur wenige Parameter bekannt. Über den Hessischen Landesbeauftragten für Datenschutz und das Landesgericht Wiesbaden gelangte die Beschwerde schließlich zum Europäischen Gerichtshof (EuGH) nach Luxemburg.

Das Ergebnis: die Berechnung eines Scores über die Kreditwürdigkeit einer Person fällt bereits unter das Profilingverbot – auch wenn Dritte (in diesem Fall die Bank) erst darauf aufbauend die endgültige Entscheidung treffen (in diesem Fall über die Kreditvergabe). Wenn es also von dem errechneten Wahrscheinlichkeitswert maßgeblich abhängt, ob ein Vertrag mit dem oder der Betroffenen begründet, durchführt oder beendet wird.

Recherchen haben ergeben, dass jedenfalls Angaben wie Wohnort, Geburtsdatum, Handyverträge, Bankkonten oder bisherige Gewohnheiten beim Bezahlen von Rechnungen in das Ranking einbezogen werden. Der EuGh legte nun fest, dass Register-Daten, die in das Scoring einfließen (in dem Fall die des deutschen Insolvenzregisters), dann gelöscht werden, wenn auch das öffentliche Register sie löscht aus dem die Daten stammen. Löschfristen öffentlicher Daten gelten also auch für das Löschen derselben Daten bei Privaten. Wie die SCHUFA Auskunftsbegehren nun im Endeffekt beantworten muss, haben deutsche Gerichte zu entscheiden.

Im Zusammenhang mit der Arbeitswelt hat dieses Urteil wichtige Auswirkungen, denn es werden immer häufiger Profile über Arbeitnehmer:innen erstellt. Sogenannte „Künstliche Intelligenz" erstellt beispielsweise Profile über die Leistung von Beschäftigen im Außendienst aufgrund denen Boni berechnet werden. Profile aufgrund der Bildschirm-Aktivitäten versprechen herauszufinden, wie hoch die Wahrscheinlichkeit eines Verbleibs im Betrieb ist. Sollten derartige maschinell erstellte Profile, Scorings, Ratings, Rankings also Basis für erheblich beeinträchtigende Entscheidungen sein, müsste man sich die Sachlage sehr gut ansehen, ob das nicht – gemäß dem nun vorliegenden EuGh-Urteil – unzulässig wäre.

SICH AN DIE DATENSCHUTZBEHÖRDE UND EIN GERICHT WENDEN: KANN MAN MACHEN

Oberster Gerichtshof, 23. Mai 2019, 6 Ob 91/19d

Zu den Aufgaben einer nationalen Datenschutzbehörde (DSB) zählt grundsätzlich das Führen von Verfahren in Fragen des Datenschutzes. Die DSB entscheidet über Datenschutzbeschwerden von Betroffenen mit Bescheid. Dieser kann wiederum mithilfe eines Rechtsmittels an das Bundesverwaltungsgericht (BVwG) bekämpft werden. Fraglich ist, ob damit die Rechtsdurchsetzung in Datenschutzfragen vor den ordentlichen Gerichten nicht mehr möglich ist.

Der OGH hat nun festgehalten, dass für die Entscheidung über individuelle Ansprüche bei Verstößen gegen die DSGVO jedenfalls weiterhin (zumindest auch) die ordentlichen Gerichte zuständig sind. Es wird also in Fragen des Datenschutzes die Rechtsprechung der ordentlichen Gerichtsbarkeit nicht zur Gänze durch Behördenentscheidungen und verwaltungsgerichtliche Verfahren ersetzt. Dabei geht es insbesondere um Schadenersatzansprüche, die weiterhin vor den ordentlichen Gerichten geltend gemacht werden können, aber auch der (individuelle) Anspruch auf Löschung von Daten kann nicht nur vor der Datenschutzbehörde, sondern auch im gerichtlichen Verfahren geltend gemacht werden. Fallweise wird dies

als „Doppelgleisigkeit" bei der Rechtsdurchsetzung in Datenschutzfragen bezeichnet.

GPS-DATEN IM FIRMENFAHRZEUG: NUR UNTER BESTIMMTEN BEDINGUNGEN

Bundesverwaltungsgericht, 4. April 2019, W214 2207491-1/44E

Eine Gebäudeservice-Firma installierte in sämtlichen ihrer Fahrzeuge Geräte zur GPS-Datenerfassung. Das Unternehmen gab an, dass von den Fahrern eine Zustimmungserklärung vorliegt und das GPS-System zum Schutz des Eigentums (Versicherungsbonus), zur Routenplanung und -optimierung, zur Disposition der Fahrer und als Fahrtenbuch genutzt werde, nicht aber zur Mitarbeiterüberwachung. Ein Arbeitnehmer beschwerte sich dennoch bei der Behörde, da er zustimmen hätte müssen und behauptete, dass die Kolleg:innen sehr wohl kontrolliert würden – beispielsweise indem sie gefragt werden, warum sie länger an einem Ort angehalten hätten. Eine Betriebsvereinbarung dazu gibt es in dem Betrieb nicht – es gibt auch keinen Betriebsrat, der eine solche abschließen könnte.

Das Bundesverwaltungsgericht stellte fest, dass die „Zustimmung" der Beschäftigten nicht freiwillig erfolgt sein kann – und daher keine Rechtsgrundlage für das GPS-System vorliegt und erteilte dem Unternehmen einige Auflagen, die innerhalb einer Frist von sechs Monaten zu erfüllen wären damit der Einsatz der GPS-Geräte in Einklang mit der DSGVO steht:

- bei Fahrten im Privatmodus dürfen Standortdaten nur im Fall eines Diebstahles abgerufen werden;
- die Standortdaten sind nach maximal 45 Tagen zu löschen (außer es besteht eine gesetzliche Aufbewahrungspflicht);
- Arbeitszeiten und Ruhepausen dürfen nur dann mit Standortdaten abgeglichen werden, wenn fehlende oder falsche Arbeitszeit-Eintragungen vorliegen und eine Klärung beim Arbeitnehmer direkt nicht möglich ist oder eine versuchte Klärung bei diesem zu keinem klaren Ergebnis führt (selbiges gilt für die Überprüfung von Schwarzfahrten und Schwarzarbeiten);
- der Arbeitgeber muss ein angepasstes Verzeichnis der Verarbeitungstätigkeiten erstellen sowie einen angepassten Auftragsverarbeitungsvertrag und auch eine Datenschutz-Folgenabschätzung durchführen.
- Ferner müssen die Einwilligungserklärungen adaptiert werden (gem. AVRAG), wobei die Arbeitnehmer informiert werden müssen, wann Zugriff auf welche Standortdaten erfolgt.

An dieser Auflistung kann sich ein:e Betriebsrat:rätin gut orientieren, wenn sie gerade am Verhandlungstisch zu einer Betriebsvereinbarung sitzt. Eine Muster-Betriebsvereinbarung zu GPS-Datenerfassung, elektronischem Fahrtenbuch, Navigationssystem und ähnlichen Systemen können die betriebsbetreuenden Kolleg:innen der Gewerkschaft GPA zur Verfügung stellen.

HANDVENEN-SCAN ZUR BESTÄTIGUNG DER ARBEITSZEITEN: ÜBERSCHIESSEND

Datenschutzbehörde, 19. Oktober 2022 (Entscheidung D124.2941 2022-0.360.359)

Bestätigt vom Bundesverwaltungsgericht, 18. Jänner 2024 (Erkenntnis W137 2263970-1/17E)

Zum Thema Arbeitszeiterfassung mittels biometrischer Daten (z. B. Fingerprint, Handvenenscan) gibt es immer wieder Fragen, ob das zulässig sei. Nun wurde – nicht zum ersten Mal – festgestellt, dass Arbeitszeiterfassung zwar eine Verpflichtung des Arbeitgebers/ der Arbeitgeberin ist, aber nicht mittels biometrischer Merkmale vorgenommen werden darf.

Bei dem österreichischen Restaurant „Plachutta" ließ der Arbeitgeber die Beschäftigten gleichzeitig mit ihrem Arbeitsvertrag eine Einverständniserklärung zum Scannen ihres Handflächenabdrucks unterschreiben. Mit diesem Handvenenscan, wurde den Beschäftigten erklärt, erhielten sie einmal im Monat Zugang zu ihren Arbeitszeitaufzeichnung, könnten diese kontrollieren und abzeichnen.

Ein ehemaliger Koch brachte mit Hilfe der Arbeiterkammer die Angelegenheit vor die DSB. Die Behörde stellte fest, dass biometrische Daten wie der Handflächenabdruck für den Zweck der Arbeitszeiterfassung überschießend und daher nicht geeignet sind.

Die Datenschutzbehörde hielt außerdem fest, dass die Einwilligung zum Handvenenscan nicht rechtskonform

erteilt wurde. Der Arbeitnehmer musste nämlich schon bei Abschluss des Arbeitsvertrags unterschreiben, dass er für die gesamte Zeit des bestehenden Arbeitsverhältnisses die Zustimmung zum Scann erteilt hätte. Die Behörde urteilte, dass dieses Vorgehen das Recht auf Geheimhaltung besonders schutzwürdiger personenbezogener Daten verletzt hat und die Zustimmung keineswegs freiwillig erteilt werden konnte.

Außerdem wurden die neunundzwanzig unter anderem in der Küche installierten Kameras als nicht zweckdienlich beurteilt. Videokameras zum Zweck der Mitarbeiter:innen-Kontrolle untersagt das österreichische Datenschutzgesetz generell. Der Zweck Diebstahl- und Einbruchsschutz sei mit den Kameras nicht zu erfüllen – so die Behörde. Das gelindere Mittel wäre gewesen, vereinzelt Kameras in Räumen mit wertvollen Gütern zu installieren oder auf Fluchtwege zu richten. Die beiden Kameras in der Küche mussten außer Betrieb genommen werden. Eine Geldbuße wurde nicht verhängt.

Plachutta wandte sich zwar an die nächsthöhere Instanz, das Bundesverwaltungsgericht (BVwG) um den Bescheid anzufechten, das BVwG hat die Entscheidung der DSB jedoch bestätigt. Bei einer Kopplung der Einwilligung zu einer Verarbeitung vertragsunabhängiger personenbezogener Daten mit einem Vertragsschluss sei grundsätzlich davon auszugehen, dass die Erteilung der Einwilligung nicht freiwillig erfolge. Auch war in dem Fall eine „echte Wahl" nicht gegeben, sodass etwaige Ängste vor negativen Folgen ausgeschlossen oder zumindest weitgehend beseitigt gewesen wären.

Die Videokameras in der Vorbereitungsküche berühren hingegen gemäß BVwG nicht die Menschenwürde, da sich die Arbeitnehmer:innen nicht überwiegend im Blickfeld der Kamera aufhalten, Ausweichmöglichkeiten bestehen, keine sensiblen Bereiche überwacht werden und die Einsichtnahme in die Aufzeichnungen nur im Anlassfall erfolgt. Gleichzeitig ist die Kamera laut BVwG für den genannten Zweck der Diebstahlsicherung nicht erforderlich, da bereits ein Großteil der Ein- und Ausgänge videoüberwacht sind und die Kamera nur zu einem geringen Teil den allfälligen Fluchtweg nach einem Diebstahl erfasst. Es wäre ausreichend von außen, ohne Sicht in die Küche, zu filmen.

Falls Zeiterfassungssysteme oder Videokameras in einem Betrieb zum Thema werden sollten, können die betriebsbetreuenden Kolleg:innen der Gewerkschaft Gpa individuelle Beratungen sowie Muster-Betriebsvereinbarungen zur Arbeitszeiterfassung und zur Videokontrolle zur Verfügung stellen.

UMFASSENDE EINSICHT IN E-MAIL-LOGFILES: GESCHÄFTSFÜHRUNG BRAUCHT GESETZLICHE GRUNDLAGE

Datenschutzbehörde, 7. Dezember 2022, GZ: 2022-0.737.249

Die Datenschutzbehörde hat sich mit der Frage auseinandergesetzt, ob die Kontrolle der E-Mail-Protokolle von Mitarbeiter:innen zulässig ist. Aus derartigen Logfiles sind Verbindungsdaten wie Sender:innen, Empfänger:innen, Datum, Uhrzeit, Größe oder auch Betreff ersichtlich. Die Geschäftsführung hatte die Serverprotokolle aller 6.000 Angestellten auf eine spezifische Empfängerdomain hin überprüft, da die Frage im Raum stand, ob es geheime Absprachen mit Konkurrenzunternehmen gäbe.

Das Verfahren wurde auf Grund der Beschwerde dreier Angestellter eingeleitet, die sich in ihrem Grundrecht auf Geheimhaltung verletzt sahen. Die Datenschutzbehörde vertrat in ihrem noch nicht rechtskräftigen Bescheid die Ansicht, dass die Kontrollmaßnahme, die erst sechs Monate nach dem anlassgebenden Vorfall stattgefunden hat, auf Grund des fehlenden zeitlichen Konnexes und der Aktualität nicht verhältnismäßig gewesen wäre. Auch eine erforderliche Zustimmung des Betriebsrats bemängelte die DSB und stellte fest, dass der Arbeitgeber für eine solche Kontrollmaßahme eine gesetzliche Grundlage benötige. Eine gerichtliche Klärung ist jedoch noch ausständig.

Eine Unterlage zu rechtlichen Grundlagen bei Einsichtswünschen von Vorgesetzten können die betriebsbetreuenden Kolleg:innen der Gewerkschaft Gpa zur Verfügung stellen.

CHECKLISTE DSGVO

Die wichtigsten Fragen um festzustellen, ob eine Datenverwendung im Betrieb rechts-konform ist

- ☐ Wird die **Rechenschaftspflicht** eingehalten,
  d.h. sind die Verwendungsvorgänge dokumentiert, sodass bei Bedarf alles nachvollziehbar ist?

- ☐ Wofür werden die Daten verwendet (Grundsatz der **Zweckbindung**)
  d.h. gibt es einen legitimen, eindeutig festgelegten und für das Ziel geeigneten Zweck für die Datenverwendung?

- ☐ Was ist die **Rechtsgrundlage** für die Datenverwendung (Grundsatz der Rechtmäßigkeit);
  d.h. gibt es ein Gesetz, einen Vertrag, ein konkretes und wichtiges Interesse aufgrund dessen die personenbezogenen Daten verarbeitet werden?

- ☐ Sind die verwendeten Daten richtig und aktuell (Grundsatz der **Richtigkeit**)?

- ☐ Wird **Datensparsamkeit** praktiziert (Grundsatz der Datenminimierung),
  d.h. werden ausschließlich jene personenbezogenen Daten verwendet, die tatsächlich erforderlich sind um dem Zweck gerecht zu werden?

- ☐ Werden nicht mehr benötigte personenbezogene Daten wieder **gelöscht** (Grundsatz der Speicherbegrenzung)?

- ☐ Wird auf **Transparenz** geachtet,
  d.h. erhalten die Beschäftigten Informationen über sie selbst betreffende Datenverwendungen (den Verwendungszweck, die Datenkategorien, die Empfänger:innen, Löschfristen, Verantwortliche sowie ihr Beschwerderecht vor der Datenschutzbehörde) innerhalb der vorgegebenen Frist (ein Monat)?

- ☐ Wurde ein:e **Verantwortliche:r** für die Datenverwendung genannt?
  d.h. gibt es eine Ansprechperson im Betrieb für Datenschutzangelegenheiten? Gibt es eine:n **betriebliche:n Datenschutzbeauftragte:n**, der oder die für die innerbetriebliche Beratung, Unterrichtung, Überwachung, Sensibilisierung etc. bereitsteht? Gibt es Verantwortliche für die Meldung von Datenschutzverletzungen?

- ☐ Wird die Privatsphäre der Arbeitnehmer:innen durch **technische Einstellungen** geschützt?
  d.h.: gibt es ein Berechtigungskonzept, sodass die personenbezogenen Daten der Beschäftigten nur jenen zur Verfügung stehen, die sie brauchen? Sind die Einstellungen und Nutzungsbedingungen so festgelegt, dass den Arbeitnehmer:innen ein möglichst großer Spielraum zur freiwilligen und diskriminierungsfreien Verwendung der Systeme bleibt (Opt-Out-Möglichkeit)? Werden Daten – wo möglich und sinnvoll – pseudonymisiert, anonymisiert und/oder verschlüsselt?

- ☐ Sind die Software, Systeme, Programme etc. die personenbezogene Daten verwenden, ins **Verarbeitungsverzeichnis** eingetragen?

- ☐ Falls Profile von Beschäftigten erstellt werden: Wenn die persönlichen Daten der Beschäftigten erfasst werden, um deren Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel zu analysieren oder vorherzusagen unterliegt das dem **Profiling-Verbot** (Art. 22 DSGVO).
  Wurden die Beschäftigten über die **Logik** informiert, nach der die Profile erstellt werden, sowie über die angestrebten **Auswirkungen**, die mit dem Profiling erzielt werden sollen?
  Werden **schwerwiegende Entscheidungen** rein auf Basis von derartigen automationsunterstützten Berechnungen, also maschinellen Verarbeitungen, getroffen (z.B. ob jemand eine Prämie, eine freie Stelle, eine kostspielige Weiterbildung etc. erhält), wäre das nicht rechtmäßig bzw. müsste sehr genau geprüft werden, ob und wenn ja, welche Rechtsgrundlage dafür besteht.

- ☐ Falls von einer Datenverwendung ein hohes Risiko für die Beschäftigten ausgeht (z.B. ihre Privatsphäre beeinträchtigt wird) muss eine Datenschutzfolgenabschätzung vorliegen.

  - Wurden die Betroffenen, also die Beschäftigten, bzw. deren Vertretung, also der **Betriebsrat**, eingebunden (gemäß Art. 36 Abs 9 DSGVO)?

  - Ist der oder die **betriebliche Datenschutzbeauftragte** eingebunden gewesen?

  - Wurde **Abhilfe** geschaffen gegen allfällig bestehende Risiken? Wurde das **gelindeste, zum Ziel führende Mittel** eingesetzt – etwa indem Daten nicht personenbezogen, sondern pseudonymisiert oder **anonymisiert** verwendet werden?

- ☐ **Falls es sich um freiwillige Datenverwendungen handelt:** Haben die Betroffenen **eingewilligt**? Und ist die Einwilligung tatsächlich freiwillig erfolgt oder ist sie an die (Weiter-)Beschäftigung oder andere das Arbeitsverhältnis betreffende Faktoren gekoppelt? Falls letzteres der Fall wäre, wäre die Einwilligung nicht freiwillig und könnte außerdem dem „Koppelungsverbot" (Art. 7 Abs 4 DSGVO) widersprechen.

- ☐ **Falls es sich um Datentransfer in ein EU-Drittland handelt:** Wurden die Beschäftigten darüber informiert, dass ihre Daten in ein Drittland übermittelt werden und welche Sicherheiten in diesem Land für ihre Daten gibt (z. B. Angemessenheitsbeschluss der EU-Kommission, Standarddatenschutzklauseln, von der Behörde genehmigte interne Datenschutzvorschriften etc.).

Jede mit **„ja"** beantwortete Frage, bedeutet, dass die DSGVO eingehalten wird. (Außer die nach dem Profiling und die nach dem Koppelungsverbot.)

Jede mit **„nein"** beantwortete Frage, verlangt zumindest einer genauen Überprüfung.

Die konkreten, an den Betrieb angepassten Antworten auf die Fragen können als Grundlage für eine allfällig erforderliche Betriebsvereinbarung herangezogen werden. Beispielsweise kann in der Betriebsvereinbarung konkret und eindeutig festgelegt werden, für welche Zwecke die Datenverarbeitungen zu verwenden sind (z. B. interne informelle Kommunikation über Teams Chats) und damit ausgeschlossen werden, dass andere, zweckfremde Tätigkeiten mit einer App gemacht werden (z.B. offizielle Antworten an Kund:innen). Oder es könnte festgelegt werden, wie und bei wem Beschäftigte die ihnen zustehenden Auskünfte erhalten.

ANHANG: DIE DATENSCHUTZ-GRUNDVERORDNUNG

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/Erwägungsgrund (Datenschutz-Grundverordnung)

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, nach Stellungnahme des Ausschusses der Regionen, gemäß dem ordentlichen Gesetzgebungsverfahren, HABEN FOLGENDE VERORDNUNG ERLASSEN:

INHALT

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand und Ziele

[Erwägungsgründe 1–14]

(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

[Erwägungsgründe 15–21]

(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, soweit sie 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 (Erwägungsgrund) Nr. 45/2001. Die Verordnung (Erwägungsgrund) 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/Erwägungsgrund und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit der Vermittler unberührt.

Artikel 3

Räumlicher Anwendungsbereich

[Erwägungsgründe 22–25]

(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

[Erwägungsgründe 26–37]

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

[Erwägungsgrund 39]

(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");
   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

[Erwägungsgründe 40–50]

(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

[Erwägungsgründe 32–33 und 42–43]

(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

[Erwägungsgrund 38]

(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

[Erwägungsgründe 51–56]

(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 aufrecht erhalten, 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 zusammen hängende Sicherungsmaßregeln 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

[Erwägungsgrund 57]

(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

[Erwägungsgründe 58–59]

(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

[Erwägungsgrund 60]

(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

[Erwägungsgründe 61–62]

(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) alls 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

[Erwägungsgründe 63–64]

(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")

[Erwägungsgründe 65–66]

(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

[Erwägungsgrund 67]

(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

[Erwägungsgrund 68]

(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

[Erwägungsgründe 69–70]

(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/ Erwägungsgrund 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

[Erwägungsgründe 71–72]

(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

Artikel 23

Beschränkungen

[Erwägungsgrund 73]

(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

[Erwägungsgründe 74–77]

(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

[Erwägungsgrund 78]

(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

[Erwägungsgrund 79]

(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

[Erwägungsgrund 80]

(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

[Erwägungsgrund 81]

(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

a) die personenbezogenen Daten nur auf d okumentierte 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;

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;
d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
e) 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;
f) 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;
g) 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;
h) 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

[Erwägungsgrund 82]

(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

[Erwägungsgrund 83]

(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

[Erwägungsgrund 85]

(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

[Erwägungsgründe 86–88]

(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

[Erwägungsgründe 84 und 89–93]

(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 Datenschutz beauftragten, 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

[Erwägungsgründe 94–96]

(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

[Erwägungsgrund 97]

(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

[Erwägungsgründe 98–99]

(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 Streitbeilegungsverfahren 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

[Erwägungsgrund 100]

(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 (Erwägungsgrund) 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;

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 (Erwägungsgrund) 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

[Erwägungsgründe 101–102]

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

[Erwägungsgründe 103–107]

(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/Erwägungsgrund 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/Erwägungsgrund 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

[Erwägungsgründe 108–109]

(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/Erwägungsgrund 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/Erwägungsgrund 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

[Erwägungsgrund 110]

(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 Datenschutzschulungen 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

[Erwägungsgrund 115]

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 personen bezogener 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

[Erwägungsgründe 111–114]

(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

[Erwägungsgrund 116]

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

[Erwägungsgrund 117)

(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

[Erwägungsgründe 118–120]

(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

[Erwägungsgrund 121]

(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 Amtsbeziehungsweise Dienstzeit gilt diese Verschwiegenheitspflicht insbesondere für die von natürlichen Personen gemeldeten Verstößen gegen diese Verordnung.

Abschnitt 2

Zuständigkeit, Aufgaben und Befugnisse

Artikel 55

Zuständigkeit

[Erwägungsgründe 122–123]

(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

[Erwägungsgründe 124–131]

(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 grenzüber schreitende 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

[Erwägungsgründe 132–134]

(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

[Erwägungsgrund 129]

(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) wurde aus Platzgründen weggelassen und ist im Internet zu finden.

KAPITEL VIII

Rechtsbehelfe, Haftung und Sanktionen

Artikel 77

Recht auf Beschwerde bei einer Aufsichtsbehörde

[Erwägungsgründe 141]

(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

[Erwägungsgründe 143–144]

(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 Rechtbehelfs 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

[Erwägungsgrund 145]

(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.

Artikel 80

Vertretung von betroffenen Personen

[Erwägungsgrund 142]

(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 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, in ihrem Namen die in den Artikeln 77, 78 und 79 genannten Rechte wahrzunehmen und das Recht auf Schadensersatz 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

[Erwägungsgründe 144–145]

(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

[Erwägungsgründe 146–147]

(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 Schadensersatz für die betroffene Person sichergestellt ist.

(5) Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieswer 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

[Erwägungsgründe 148–151]

(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 abzuhelfen 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

[Erwägungsgründe 149 und 152]

(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

[Erwägungsgrund 153]

(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

[Erwägungsgrund 154]

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

[Erwägungsgrund 155]

(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

[Erwägungsgründe 156–163]

(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

[Erwägungsgrund 164]

(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

[Erwägungsgrund 165]

(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

[Erwägungsgründe 166–169]

(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

[Erwägungsgrund 170]

(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/Erwägungsgrund

[Erwägungsgrund 171]

(1) Die Richtlinie 95/46/Erwägungsgrund 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/Erwägungsgrund 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/Erwägungsgrund

[Erwägungsgrund 173]

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/Erwägungsgrund 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/Erwägungsgrund 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

[Erwägungsgrund 171]

(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 . . . . . Im Namen des
Europäischen Parlaments . . . . . Rates

Der Präsident . . . . . Die Präsidentin
M. SCHULZ J.A. HENNIS-PLASSCHAERT

Literatur für die Betriebsrats-Bibliothek

JA! ICH WERDE JETZT GPA-MITGLIED!

☐ Frau ☐ Herr ☐ Divers ☐ .....

Titel .....

Familienname .....

Vorname .....

Geburtsdatum

Straße/Hausnr. .....

PLZ/Wohnort .....

Telefonisch erreichbar .....

E-Mail .....

Damit wir dich bei Kollektivvertragsverhandlungen richtig informieren können, bitten wir um Angabe deines Dienstgebers und der genauen Branche.

Beschäftigt bei .....

Anschrift .....

Branche .....

Derzeitige Tätigkeit .....

Zutreffendes bitte ankreuzen:

☐ Angestellte:r ☐ Arbeiter:in ☐ Lehrling/..... Lj.

☐ Schüler:in ☐ Student:in ☐ Werkvertrag

☐ Zeitarbeitskraft ☐ freier Dienstvertrag

☐ Zweitmitgliedschaft ☐ geringfügig beschäftigt

GPA-Beitrittsmonat/-jahr: .....

Gehaltshöhe brutto .....

Der monatliche Mitgliedsbeitrag beträgt 1 % des Bruttogehalts bis zu einem Maximalbeitrag, der jährlich angepasst wird (siehe **www.gpa.at/mitgliedsbeitrag**). Der Mitgliedsbeitrag ist steuerlich absetzbar.

☐ Ich willige ein, dass ÖGB, ÖGB Verlag und/oder VÖGB mich telefonisch bzw. per elektronischer Post (§107 TKG) kontaktieren dürfen, um über Serviceleistungen, etwa Aktionen für Tickets, Bücher und Veranstaltungen zu informieren und sonstige Informationen zu übermitteln. Die Einwilligung kann jederzeit widerrufen werden.

Ich bezahle meinen Mitgliedsbeitrag durch: (Zutreffendes bitte ankreuzen)

☐ **Betriebsabzug**

Ich erkläre, dass mein Gewerkschaftsbeitrag durch meinen Arbeitgeber von meinem Gehalt/Lohn/Lehrlingseinkommen abgezogen werden kann. Ich erteile deshalb meine Einwilligung, dass meine im Zusammenhang mit der Beitragseinhebung erforderlichen personenbezogenen Daten (angegebene Daten und Gewerkschaftszugehörigkeit, Beitragsdaten, KV-Zugehörigkeit, Eintritts-/und Austrittsdaten, Karenzzeiten, Präsenz-, Ausbildungs- und Zivildienstzeiten, Pensionierung und Adressänderungen) von meinem Arbeitgeber und von der Gewerkschaft verarbeitet werden dürfen, wobei ich diese Einwilligung zum Betriebsabzug jederzeit widerrufen kann.

☐ **SEPA Lastschrift-Mandat** (Bankeinzug)

Ich ermächtige die Gewerkschaft GPA, die Zahlungen meines Mitgliedsbeitrages von meinem Konto mittels SEPA-Lastschrift einzuziehen. Zugleich weise ich mein Kreditinstitut an, die von der Gewerkschaft GPA auf mein Konto gezogene SEPA-Lastschriften einzulösen. Ich kann innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrags verlangen. Es gelten dabei die mit meinem Kreditinstitut vereinbarten Bedingungen.

Der Einzug des Mitgliedsbeitrages erfolgt jeweils zum Monatsultimo.

Wenn ich dem Betriebsabzug zugestimmt habe, diesen aber nicht mehr wünsche oder aus dem Betrieb ausscheide oder der Abzug des Mitgliedsbeitrages über den Betrieb nicht mehr möglich ist, ersuche ich die Zahlungsart ohne Rücksprache auf SEPA-Lastschrift von meinem bekannt gegebenen Konto umzustellen.

IBAN

BIC

.....
Datum/Unterschrift

Ich bestätige, nachstehende Datenschutzerklärung (auch abrufbar unter www.oegb.at/datenschutz) zur Kenntnis genommen zu haben.

.....
Datum/Unterschrift

ÖGB-ZVR-Nr.: 576439352, CID: AT48ZZZ00000006541

DATENSCHUTZINFORMATION (online unter: **www.oegb.at/datenschutz**)

Der Schutz Ihrer persönlichen Daten ist uns ein besonderes Anliegen. In dieser Datenschutzinformation informieren wir Sie über die wichtigsten Aspekte der Datenverarbeitung im Rahmen der Mitgliederverwaltung. Eine umfassende Information, wie der ÖGB/die Gewerkschaft GPA, mit Ihren personenbezogenen Daten umgeht, finden Sie unter www.oegb.at/datenschutz.

Verantwortlicher für die Verarbeitung Ihrer Daten ist der Österreichische Gewerkschaftsbund. Wir verarbeiten die von Ihnen angegebenen Daten mit hoher Vertraulichkeit, nur für Zwecke der Mitgliederverwaltung der Gewerkschaft und für die Dauer Ihrer Mitgliedschaft bzw. solange noch Ansprüche aus der Mitgliedschaft bestehen können. Rechtliche Basis der Datenverarbeitung ist Ihre Mitgliedschaft im ÖGB/in der Gewerkschaft GPA; soweit Sie dem Betriebsabzug zugestimmt haben, Ihre Einwilligung zur Verarbeitung der dafür zusätzlich erforderlichen Daten.

Die Datenverarbeitung erfolgt durch den ÖGB/die Gewerkschaft GPA selbst oder durch von diesem vertraglich beauftragte und kontrollierte Auftragsverarbeiter. Eine sonstige Weitergabe der Daten an Dritte erfolgt nicht oder nur mit Ihrer ausdrücklichen Zustimmung. Die Datenverarbeitung erfolgt ausschließlich im EU-Inland.

Ihnen stehen gegenüber dem ÖGB/der Gewerkschaft GPA in Bezug auf die Verarbeitung Ihrer personenbezogenen Daten die Rechte auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung zu. Gegen eine Ihrer Ansicht nach unzulässige Verarbeitung Ihrer Daten können Sie jederzeit eine Beschwerde an die österreichische Datenschutzbehörde (www.dsb.gv.at) als Aufsichtsstelle erheben.

Sie erreichen uns über folgende Kontaktdaten:

Gewerkschaft GPA
1030 Wien, Alfred-Dallinger-Platz 1
Tel.: +43 (0)5 0301
E-Mail: service@gpa.at

Österreichischer Gewerkschaftsbund
1020 Wien, Johann-Böhm-Platz 1
Tel.: +43 (0)1 534 44-0
E-Mail: oegb@oegb.at

Unseren Datenschutzbeauftragten erreichen Sie unter **datenschutzbeauftragter@oegb.at**.

Bitte die ausgefüllte Mitgliedsanmeldung beim Betriebsrat abgeben oder in ein frankiertes Kuvert stecken und senden an: **Gewerkschaft GPA,** Service Center, Alfred-Dallinger-Platz 1, 1030 Wien

GEWERKSCHAFT GPA
IN GANZ ÖSTERREICH

SERVICE-HOTLINE:
+43 (0)5 0301

GEWERKSCHAFT GPA
Service-Center
1030 Wien, Alfred-Dallinger-Platz 1
Tel.: +43 (0)5 0301
Fax: +43 (0)5 0301-300
E-Mail: service@gpa.at

GPA Wien
1030 Wien, Alfred-Dallinger-Platz 1

GPA Niederösterreich
3100 St. Pölten, Gewerkschaftsplatz 1

GPA Burgenland
7000 Eisenstadt, Wiener Straße 7

GPA Steiermark
8020 Graz, Karl-Morre-Straße 32

GPA Kärnten
9020 Klagenfurt, Bahnhofstraße 44/4

GPA Oberösterreich
4020 Linz, Volksgartenstraße 40

GPA Salzburg
5020 Salzburg,
Markus-Sittikus-Straße 10

GPA Tirol
6020 Innsbruck,
Südtiroler Platz 14

GPA Vorarlberg
6900 Bregenz, Reutegasse 11

www.gpa.at

GUTE ARBEIT!

mitgliedwerden.gpa.at

MEINE GEWERKSCHAFT