Der Bayerische Landesbeauftragte
für den Datenschutz

Thomas Petri | Kai Engelbrecht

Meine Daten, die Verwaltung und ich

Wegweiser durch die Welt der Datenschutz-Grundverordnung für bayerische Bürgerinnen und Bürger

Meine Daten, die Verwaltung und ich

Wegweiser durch die Welt der Datenschutz-Grundverordnung für bayerische Bürgerinnen und Bürger

von
Thomas Petri und
Kai Engelbrecht

Herausgeber:

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18
Telefon: +49 89 21 26 72-0
E-Mail: poststelle@datenschutz-bayern.de
https://www.datenschutz-bayern.de

Autoren:

Prof. Dr. Thomas Petri
Dr. Kai Engelbrecht

2. Auflage Dezember 2019

Geleitwort
des Bayerischen Landesbeauftragten
für den Datenschutz
zur 1. Auflage

München, im Juli 2019

Sehr geehrte Leserinnen und Leser,

die Datenschutz-Grundverordnung – ein bürokratisches Monster und Vorlagengeber für absurde Verwaltungsentscheidungen oder vielleicht doch eine überfällige Antwort des Europäischen Gesetzgebers auf Risiken der Digitalisierung? Beide Einschätzungen treffen möglicherweise zu, aber irgendwie auch nicht. Vielleicht liegt die Wahrheit zwischen diesen beiden Polen. In den letzten Monaten habe ich einige kluge Analysen, leider aber auch viel Unausgereiftes darüber gelesen, was das neue EU-Datenschutzrecht angeblich verlangt. Die meisten Hilfestellungen richten sich dabei an Juristinnen und Juristen, Unternehmen, Vereine und öffentliche Verwaltungen.

Was ich zumeist vermisse, sind werthaltige Informationen für Bürgerinnen und Bürger, deren Alltag nicht von einer beruflichen Beschäftigung mit dem Thema „Datenschutz" bestimmt ist. Was bringt die Datenschutz-Grundverordnung für sie, welche Betroffenenrechte gibt es und wie kann man sie zweckmäßig ausüben? Solche Informationen sind jedenfalls in Bezug auf die Betroffenenrechte gegenüber Behörden und öffentlichen Stellen rar. Dabei soll die Datenschutz-Grundverordnung das Grundrecht auf Datenschutz ausgestalten. Und das Grundrecht auf Datenschutz soll in erster Linie Ihre Freiheit gewährleisten – es dient in allererster Linie dem Schutz der Menschen, die in der Europäischen Union leben!

Natürlich: Ein EU-weit einheitlicher Datenschutz soll auch dafür sorgen, dass personenbezogene Daten leichter zwischen den Behörden und Unternehmen der Mitgliedstaaten fließen können. Im EU-Jargon nennt man das „freien Datenverkehr".

Insgesamt glaube ich persönlich, dass die Datenschutz-Grundverordnung etwas weniger strenge Voraussetzungen an die Verarbeitung personenbezogener Daten verlangt als es das bisherige deutsche Datenschutzniveau vorgesehen hat. Dafür hat das neue EU-Datenschutzrecht die Rechte der betroffenen Personen gestärkt.

Mir ist es wichtig, dass Sie als eine von Datenverarbeitung betroffene Person die Ihnen zustehenden Betroffenenrechte wirksam ausüben können. Dieses Buch soll Ihnen einen verständlichen Überblick über das neue Datenschutzrecht geben und Sie vor allem über Ihre Betroffenenrechte informieren.

Zur Veranschaulichung enthält dieses Buch viele Beispiele, insbesondere aus der Rechtsprechung. Diesen Beispielen folgt oft eine Begründung, warum ein Fall nach einer bestimmten Vorschrift zu beurteilen ist. Wenn Sie wollen, können Sie also zunächst versuchen, die Erklärung eines Beispiels selbst zu finden.

Das Buch betrifft im Grundsatz nur die Datenverarbeitung durch bayerische Behörden und sonstige öffentliche Stellen. Soweit ich aus Gründen der Verständlichkeit Beispiele wähle, die sich auf Unternehmen oder Vereine beziehen, weise ich hier ausdrücklich darauf hin, dass ich mit meinen Ausführungen keine verbindlichen Rechtsauskünfte erteilen kann und will – dies können nur die für den nicht-öffentlichen Bereich zuständigen Datenschutz-Aufsichtsbehörden. In Bayern ist dies das Bayerische Landesamt für Datenschutzaufsicht.

Tipp:

> Viele nützliche Datenschutzinformationen für Unternehmen, Vereine und freiberufliche Datenverarbeiter finden Sie unter https://www.lda.bayern.de.

Im öffentlichen Sektor sind Fragen des Datenschutzes häufig in Fachgesetzen geregelt (siehe Abschnitte 1.3 und 4.1.5). Das Buch kann die Vielfalt dieser Regelungen nicht darstellen, geht aber punktuell auf einige bedeutsame Vorschriften ein. Weitgehend ausgespart bleibt auch der Datenschutz im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz (siehe Abschnitt 3.3.3), also insbesondere die Tätigkeit der Strafverfolgungsbehörden.

Besonders wichtige Gesetze zitiere ich im Text gerne wörtlich. Meistens allerdings enthält das Buch nur Quellenhinweise. Die zitierten Vorschriften der Datenschutz-Grundverordnung (DSGVO) und des Bayerischen Datenschutzgesetzes (BayDSG) sind im Anhang abgedruckt. Sie werden mit einem Pfeil gekennzeichnet. Finden Sie einen solchen Pfeil, dann können Sie die Vorschrift in einem der Anhänge nachlesen.

Beispiel:

> → Art. 4 Nr. 1 DSGVO. Diese Vorschrift beschreibt, was die Datenschutz-Grundverordnung unter einem „personenbezogenen Datum“ versteht.

Andere Informationsquellen sind nicht unbedingt notwendig, um das im Text Gesagte zu verstehen. Sie sind für Sie aber vielleicht trotzdem interessant. Viele dieser Informationen sind im World Wide Web frei verfügbar. Im nachfolgenden Abschnitt „Zugang zu weiterführenden Informationen“ erhalten Sie Hinweise zur Recherche.

Informationen, die Sie auf den dort angegebenen Datenbanken und Internetpräsenzen abrufen können oder die sich leicht mit Hilfe der gängigen Suchmaschinen auffinden lassen, sind im Text mit eckigen Klammern gekennzeichnet.

Beispiel:

> [Europäischer Gerichtshof, Urteil vom 10. Juli 2018, C-25/17, Rn. 52 ff.]. – Der Europäische Gerichtshof ist das Gericht, das letztverbindlich über die Auslegung von EU-Recht entscheidet.

Viele der vorgestellten Entscheidungen betreffen übrigens noch die Richtlinie 95/46/EG, weil das Gericht Verarbeitungen zu beurteilen hatte, die vor dem 25. Mai 2018 und damit vor der Geltung der Datenschutz-Grundverordnung lagen. Die Richtlinie 95/46/EG war das Vorgängergesetz zur Datenschutz-Grundverordnung. Sie enthält viele Vorschriften, die nahezu wortgleich mit Vorschriften der Datenschutz-Grundverordnung sind. Die Rechtsprechung ist dann zumeist auf die heutige Rechtslage übertragbar.

Falls Sie nach der Lektüre Verständnisfragen oder Anregungen haben, würde ich mich über Ihre Rückmeldung freuen.

Mit freundlichen Grüßen

Ihr Thomas Petri
Bayerischer Landesbeauftragter
für den Datenschutz

Zugang zu weiterführenden Informationen

Da das vorliegende Buch datenschutzrechtliche Fragen behandelt, kommt es nicht ohne die Erwähnung von Vorschriften aus. Vorschriften, die mit einem Pfeil (→) versehen sind, finden Sie im Anhang. Andere Bestimmungen sind über die einschlägigen Datenbanken zugänglich. Entsprechende Links finden Sie auf

> https://www.datenschutz-bayern.de
> in der Rubrik „Recht und Normen".

Unter diesem Link steht auch eine vollständige Fassung der Datenschutz-Grundverordnung bereit.

Viele **Entscheidungen deutscher Gerichte** können bequem über ein freies Portal abgerufen werden:

> https://openjur.de

Entscheidungen des Europäischen Gerichtshofs sind in einem mehrsprachigen Portal verfügbar:

> https://curia.europa.eu

Als Suchkriterium eignet sich jeweils das Aktenzeichen, das bei den Nachweisen im Buch nach dem Entscheidungsdatum angegeben ist.

Weiterführende Informationen zum Datenschutz können Sie auf den **Internetpräsenzen der zuständigen Datenschutz-Aufsichtsbehörden** abrufen. Dort haben Sie insbesondere Zugang zu den Tätigkeitsberichten dieser Behörden, weiterhin zu Orientierungshilfen, die wichtige Fragen des Datenschutzes ausführlich behandeln. Darüber hinaus finden Sie eine Vielzahl von Arbeitspapieren. Diese Internetpräsenzen sind wie folgt erreichbar:

Bayerischer Landesbeauftragter für den Datenschutz (Datenschutz-Aufsichtsbehörde für den öffentlichen Sektor in Bayern):

> https://www.datenschutz-bayern.de

Bayerisches Landesamt für Datenschutzaufsicht (Datenschutz-Aufsichtsbehörde für den nicht-öffentlichen Sektor in Bayern):

> https://www.lda.bayern.de

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Datenschutz-Aufsichtsbehörde für die öffentlichen Stellen des Bundes):

> https://www.bfdi.bund.de

Auch die **Konferenz der Datenschutz-Aufsichtsbehörden des Bundes und der Länder** hat mittlerweile eine Internetpräsenz, auf der Orientierungshilfen, Entschließungen und Beschlüsse sowie zahlreiche weitere Materialien eingestellt sind:

> https://www.datenschutzkonferenz-online.de

Der **Europäische Datenschutzausschuss**, in dem die Datenschutz-Aufsichtsbehörden aus den Mitgliedstaaten der Europäischen Union ihre Arbeit koordinieren, bietet insbesondere mit den unionsweit einheitlichen „Leitlinien" („Guidelines") wertvolle Hilfen für das Verständnis der Datenschutz-Grundverordnung sowie der Datenschutz-Richtlinie für Polizei und Strafjustiz:

> https://edpb.europa.eu/edpb_de
> in der Rubrik „Unsere Arbeit und Hilfsmittel – Allgemeine Leitlinien".

Inhaltsverzeichnis

1 Einführung

1.1 Was ist Datenschutz?

„Datenschutz“ ist in der Umgangssprache ein facettenreicher Begriff. Man kann darunter das Anliegen verstehen, alle Informationen zu schützen, die nicht für die Allgemeinheit bestimmt sind.

Beispiele:

> Betriebs- und Geschäftsgeheimnisse, Amts- und Berufsgeheimnisse können Informationen betreffen, die als schützenswert angesehen werden.

Oft wird Datenschutz auch mit **IT-Sicherheit** gleichgesetzt. IT-Sicherheit ist ein Bereich der Informatik, der sich mit dem Schutz von IT-Systemen und den damit verarbeiteten Informationen in allen ihren Erscheinungsformen beschäftigt.

Beispiel:

> Die Abwehr von Angriffen auf Systeme oder Informationen gehört zu den klassischen Aufgaben der IT-Sicherheit.

Das EU-Datenschutzrecht definiert **Datenschutz** anders. Es meint mit Datenschutz den „Schutz von natürlichen Personen bei der Verarbeitung personenbezogener Daten.“

Das Wort „Daten“ ist begriffsverwandt mit „Information“. Datenschutzrecht soll die Rechte und Freiheiten natürlicher Personen gewährleisten, die von Datenverarbeitungen konkret betroffen sind. So heißt es in → Art. 1 DSGVO:

> „(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.“

Natürlich gibt es Überschneidungen zwischen den unterschiedlichen Datenschutz-Begriffen. Beispielsweise sind Datenschutz in unserem Sinne und die IT-Sicherheit in vielen Bereichen tatsächlich deckungsgleich. In anderen Bereichen unterscheiden sie sich allerdings grundlegend. Unterschiedlich ist vor allem das Ziel: **Beim Datenschutz steht der Schutz des Menschen vor den Risiken der Datenverarbeitung im Vordergrund, bei der IT-Sicherheit der Schutz von IT-Systemen und Infor-**

mationen. Es gibt auch im Datenschutzrecht Vorgaben, die eine angemessene Datensicherheit sicherstellen sollen und damit zur IT-Sicherheit beitragen. Umgekehrt wirken Vorgaben zur IT-Sicherheit nicht selten auch so, dass das Datenschutzniveau verbessert wird.

Beispiele:

> → Art. 25 DSGVO regelt den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, → Art. 32 DSGVO betrifft die Sicherheit der Verarbeitung aus Sicht des Datenschutzes.

Das EU-Datenschutzrecht hat mehrere Funktionen. Es soll den Menschen vor einer missbräuchlichen Verarbeitung seiner personenbezogenen Daten schützen. Ebenso wichtig ist die Gewährleistung der Privatsphäre (**„Privatleben"**, Art. 7 Charta der Grundrechte der Europäischen Union, im Folgenden: GRCh).

> Art. 7 GRCh – Achtung des Privat- und Familienlebens
> Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

In einer modernen Gesellschaft, in der ein vernetzter Datenaustausch zum Alltag gehört, genügen diese beiden Funktionen jedoch nicht. Dementsprechend sieht Art. 8 GRCh ein **Grundrecht auf Datenschutz** vor, wonach die betroffenen Personen die sie betreffenden Verarbeitungen mitgestalten können. Betroffene Personen haben also das Recht, von einer Verarbeitung sie betreffender Daten zu erfahren und auf sie einzuwirken (zu Betroffenenrechten siehe Kapitel 5).

> Art. 8 GRCh – Schutz personenbezogener Daten
> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Dieser Grundrechtsschutz wird durch die Datenschutz-Grundverordnung konkretisiert, wie Erwägungsgründe 1 bis 4 DSGVO hervorheben.

Ach, übrigens:

> Die Erwägungsgründe stehen vor den Regelungen in Art. 1 bis 99 DSGVO. Aus den Erwägungsgründen einer EU-Verordnung können zwar keine unmittelbaren Rechtsfolgen abgeleitet werden. Sie sind aber dennoch wichtig, weil sie den Vorschriftenteil aus Sicht des

Normgebers erläutern. Mit anderen Worten können die Erwägungsgründe Ihnen oftmals helfen, die einzelnen Artikel besser zu verstehen.

1.2 Warum Datenschutz?

Auf Datenschutz angesprochen, reagieren viele Menschen auch heute noch mit den Worten: „Datenschutz? Brauche ich nicht. Ich habe nichts zu verbergen." Insbesondere Sicherheitspolitiker greifen dieses **„Nichts-zu-verbergen-Argument"** gerne auf. Es gibt sogar einen Wikipedia–Eintrag dazu. Die britische Regierung soll die Vollüberwachung des öffentlichen Raums mithilfe von Videokameras so begründet haben. Das Motto dieser Kampagne lautete sinngemäß: Wenn du nichts zu verstecken hast, hast du nichts zu befürchten („If you've got nothing to hide, you've got nothing to fear").

Ein Journalist befragte daraufhin seine Leserschaft, wie sie auf die Aussage „Ich habe nichts zu verbergen" antworten würden. In einem Artikel listete er einige der Antworten auf [Daniel J. Solove, Why Privacy Matters Even if You Have „Nothing to Hide", The Chronicle of Higher Education, 15. Mai 2011 – frei ins Deutsche übersetzt]:

- „Also haben Sie zuhause keine Vorhänge?"
- „Kann ich bitte Ihre Kreditkartenabrechnung des letzten Jahres sehen?"
- „Ich habe nicht zu begründen, warum ich etwas nicht offenbare, Sie müssen begründen, warum Sie etwas wissen wollen."
- „Ich habe nichts zu verbergen, aber ich habe auch nichts, was ich Ihnen gerne zeigen möchte."
- „Wenn Sie nichts zu verbergen haben, haben Sie kein Leben."
- „Zeigen Sie mir Ihres, dann zeige ich Ihnen meines."
- „Das hat nichts damit zu tun, etwas zu verstecken, sondern es geht darum, bestimmte Dinge nicht zum Geschäft anderer zu machen."
- „Josef Stalin würde es lieben. Muss ich noch mehr dazu sagen?"

Adrian Lobe argumentierte für den Erhalt der Privatsphäre so [Adrian Lobe, Privatsphäre. Wir haben sehr wohl etwas zu verbergen! Zeit Online, 28. November 2016]:

> „Wir haben sehr wohl etwas zu verbergen: unsere Identität, Neigungen, Gefühle, Meinungen, politische Positionen, aus denen heraus erst die Inanspruchnahme von Freiheitsrechten möglich ist. Ein Staat, der die Gedanken seiner Bürger kennt, ist ein totalitärer. Deshalb ist es so gefährlich, wenn Google und Amazon nun millionenfach camouflierte Wanzen, die als ‚Assistenten' vermarktet werden, in Millionen Haushalte schleust und unsere intimsten Gespräche belauscht. Big Brother kommt im Gewand des netten Helfers daher. Wenn die Wohnung auch noch mit Google Nest ausgestattet ist, wird der Thermostat womöglich nicht nur die Raumtemperatur messen, sondern auch, ob geraucht, getrunken und gefeiert wird. Die Sensoren registrieren jede Regung. Vielleicht wird das Individuum in vorauseilendem Gehorsam sich selbst zensieren und auf bestimmte Handlungen verzichten, weil die Technik alles aufzeichnet. Das ist Kontrolle in bester Foucault'scher Manier: Der Bürger wird zum Komplizen seiner eigenen Polizeigewalt – und überwacht sich selbst."

Auf den Punkt gebracht: Die wohl wichtigste Funktion des Datenschutzes besteht darin, dem einzelnen Menschen Schutzräume zu bewahren, innerhalb derer er unbeobachtet denken und kommunizieren kann. Nicht nur für heute, sondern auch für die Zukunft.

1.3 Datenschutz durch Recht

Dieses Buch behandelt Datenschutzrecht, wie es seit Mai 2018 in der Europäischen Union, in Deutschland und damit auch in Bayern gilt. Die folgenden Kapitel befassen sich vor allem mit der **Datenschutz-Grundverordnung (DSGVO)**. Sie ist das allgemeine EU-Datenschutzgesetz und gilt in allen Mitgliedstaaten unmittelbar und allgemein.

Ach, übrigens:

Wie eine EU-Verordnung wirkt, ergibt sich aus Art. 288 Vertrag über die Arbeitsweise der Europäischen Union (AEUV). Er ist ein Teil der Grundlagenverträge zur Europäischen Union, wie sie von den EU-Mitgliedstaaten im Jahr 2007 unterzeichnet wurden. Zum Vertrag von Lissabon gehören neben dem Vertrag über die Arbeitsweise der Europäischen Union der Vertrag über die Europäische Union sowie die Charta der Grundrechte der Europäischen Union. Der Vertrag von Lissabon ist am 1. Dezember 2009 in Kraft getreten. Art. 288 Abs. 1 bis 3 AEUV lauten:

„Für die Ausübung der Zuständigkeiten der Union nehmen die Organe Verordnungen, Richtlinien, Beschlüsse, Empfehlungen und Stellungnahmen an.

Die Verordnung hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

> Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel."

Die Datenschutz-Grundverordnung enthält allerdings nicht alle Regelungen zum Datenschutz. Zunächst klammert sie selbst ausdrücklich einige Verarbeitungen aus. Beispielsweise gilt die Datenschutz-Grundverordnung nicht für die Strafverfolgungsbehörden, wenn sie versuchen, Straftaten zu bekämpfen und dabei personenbezogene Daten verarbeiten. Hierfür gibt es eine besondere EU-Richtlinie. Dieses Buch stellt einige wenige Besonderheiten dieser Richtlinie (EU) 2016/680 kurz vor. Sie wird oft auch als Datenschutz-Richtlinie für Polizei und Strafjustiz (RLDSJ) bezeichnet.

Neben dem EU-Datenschutzrecht bestehen auch weiterhin nationale **Datenschutzgesetze der Mitgliedstaaten**. In Deutschland gibt es ein Bundesdatenschutzgesetz (BDSG) und speziellere Datenschutzregelungen (etwa in der Abgabenordnung und im Zehnten Buch Sozialgesetzbuch), außerdem Landesdatenschutzgesetze (so in Bayern das → Bayerische Datenschutzgesetz – BayDSG) und auch noch spezielle Datenschutzregelungen des Landesrechts). Der größte Teil dieser nationalen Vorschriften konkretisiert Vorgaben des EU-Datenschutzrechts oder nutzt gewisse Spielräume aus, die das EU-Datenschutzrecht eröffnet. Nur sehr wenige Vorschriften regeln Fragen des Datenschutzes, soweit er nicht in den Anwendungsbereich des EU-Rechts fällt.

Beispiel:

> § 85 BDSG betrifft unter anderem Verarbeitungen im Zusammenhang mit der Landesverteidigung durch die Bundeswehr. Die Europäische Union hat nicht die Kompetenz, Fragen der militärischen Landesverteidigung von Mitgliedstaaten zu regeln.

In diesem Buch steht die Datenschutz-Grundverordnung im Vordergrund, doch kommen auch fachgesetzliche Regelungen des Bundes- wie des bayerischen Landesrechts zur Sprache.

1.4 Wichtige Begriffe (Auswahl)

Wenn Sie die Datenschutz-Grundverordnung verstehen wollen, ist es wichtig, dass Sie zentrale datenschutzrechtliche Begriffe richtig einordnen können. Deshalb werden einige wichtige Begriffe in → Art. 4 DSGVO definiert.

Tipp:

> Falls Ihnen die Bedeutung eines Begriffs unklar ist, schauen Sie in → Art. 4 DSGVO nach - vielleicht wird er dort näher erläutert!

Hier werden nur vier zentrale Datenschutzbegriffe vorab kurz vorgestellt: Was ist ein personenbezogenes Datum? Was ist unter einer Verarbeitung personenbezogener Daten zu verstehen? Was ist ein für die Verarbeitung Verantwortlicher? Und was ist eine betroffene Person?

1.4.1 Was sind „personenbezogene Daten"?

Nach → Art. 4 Nr. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf einen konkret ermittelbaren Menschen („natürliche Person") beziehen. Ermittelbar ist jemand, wenn er (oder sie) direkt oder indirekt identifiziert werden kann. Dabei sollen „alle Mittel berücksichtigt werden, die von einem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um eine natürliche Person direkt oder indirekt zu identifizieren" (Erwägungsgrund 26 Satz 3 DSGVO).

Beispiel:

> Die Höhe des Jahreseinkommens einer oder eines Beschäftigten und ihr oder sein Name sind personenbezogene Daten [Europäischer Gerichtshof, Urteil vom 20. Mai 2003, C-465/00, Rn. 64 und 90].

Vor Inkrafttreten der Datenschutz-Grundverordnung wurde lange über die Frage gestritten, unter welchen Voraussetzungen eine indirekte Identifizierbarkeit dazu führt, dass jemand ermittelbar ist.

Beispiel:

> Auf der Webseite von Bundesbehörden wird die IP-Adresse von Nutzerinnen und Nutzern erfasst. Dies erfolgt vor allem aus Gründen der IT-Sicherheit. Ist die erfasste dynamische IP-Adresse ein personenbeziehbares Datum? – Nach einem Urteil des Europäischen Gerichtshofs, das vor Geltungsbeginn der Datenschutz-Grundverordnung ergangen ist, ist in der Erfassung der IP-Adresse durch eine Bundesbehörde wohl schon eine Verarbeitung personenbezogener Daten zu sehen. Zwar kann die Nutzerin oder der Nutzer nur mithilfe von Zusatzinformationen ermittelt werden, die in der Regel beim Internetprovider gespeichert sind. Bundesbehörden verfügen aber über rechtliche Mittel, mit denen sie den Internetprovider zur Offenbarung der betreffenden Person veranlassen können, siehe [Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, Rn. 49].

Der Unionsgesetzgeber hat die im vorigen Beispiel erwähnte Entscheidung zum Anlass genommen, die Definition des personenbezogenen Datums abzuändern: Während es nach dem alten Datenschutzrecht darauf ankam, ob ein Verantwortlicher ein Mittel zur Identifizierung „vernünftigerweise" einsetzt, soll es heute entscheidend sein, ob ein Mittel „wahrscheinlich" eingesetzt wird (→ Art. 4 Nr. 1 und Erwägungsgrund 26 DSGVO).

Hintergrund für diese Änderung war eine Randbemerkung des Gerichtshofs, wonach der Einsatz eines rechtswidrigen Mittels nicht „vernünftig" im Sinne des Datenschutzrechts sei.

Vertiefung:

Früher war die Auffassung weit verbreitet, dass sogenannte **„Funktionsträgerdaten"** nicht unter das Datenschutzrecht fallen würden. Gemeint sind personenbezogene Daten, soweit sie speziell den jeweiligen Menschen in seiner Eigenschaft als Amtsträger betreffen. (Beispiel: Eine Beamtin oder ein Beamter unterschreibt einen Verwaltungsakt oder ein sonstiges amtliches Schreiben.) Normalerweise ist die Unterschrift einer Person zweifelsfrei ein personenbezogenes Datum. Gegen die Anwendung des Datenschutzrechts auf den Beispielsfall wurde früher etwa so argumentiert: Erfasst wird das Datum der Beamtin oder des Beamten nur im Hinblick auf seine dienstliche Handlung. Diese Handlung ist dem Staat zuzurechnen. Der Staat ist aber kein Mensch, sondern ein Hoheitsträger. Das könnte es rechtfertigen, auch die Daten eines Beamten oder einer Beamtin in Ausübung des Dienstes anders zu behandeln als die Daten anderer Menschen.

Ähnlich hat die Republik Österreich in einem Fall argumentiert, der jüngst vor dem Europäischen Gerichtshof verhandelt wurde. Ein Mann hatte eine Polizeiwache gefilmt und dabei die Polizisten und Polizistinnen erfasst. Der Europäische Gerichtshof hatte in diesem Fall die Frage zu beantworten, ob der Mann mit seinen Filmaufnahmen personenbezogene Daten im Sinne der Richtlinie 95/46/EG verarbeitet hat. Nach der Einschätzung Österreichs müssen Beamtinnen und Beamten, die ihren Amtspflichten nachgehen, es hinnehmen, dass sie im öffentlichen Bereich agieren und dass ihre Handlungen kritisch beobachtet werden können.

Aber: Die alte Richtlinie 95/46/EG sah eine solche Beschränkung des Datenschutzes im Hinblick auf Beamtinnen und Beamte bewusst nicht vor – die Datenschutz-Grundverordnung tut es übrigens auch nicht. Deshalb hat die für den Fall zuständige Generalanwältin in ihren Schlussanträgen empfohlen, die Richtlinie 95/46/EG auf den Fall anzuwenden [Europäischer Gerichtshof, Schlussanträge der Generalanwältin Eleanor Sharpton vom 27. September 2018, C-345/17, Rn. 29 ff.]. Im Ergebnis ist der Europäischer Gerichtshof dieser Empfehlung der Generalanwältin gefolgt [Urteil vom 19. Februar 2019, C-345/17, Rn. 44 ff.].

Ach, übrigens:

> Muss sich der Europäische Gerichtshof mit neuen Rechtsfragen befassen, bereitet eine Generalanwältin oder ein Generalanwalt die Entscheidung des Gerichtshofs vor. Diese Person verfasst eine Art Gutachten zum Fall („Schlussanträge"), um die Entscheidung des Gerichtshofs vorzubereiten.

1.4.2 Verarbeitung personenbezogener Daten

Die **Verarbeitung** personenbezogener Daten wird sehr weit verstanden. Die Datenschutz-Grundverordnung nennt so in → Art. 4 Nr. 2 DSGVO „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang […] im Zusammenhang mit personenbezogenen Daten" und fügt dann zahlreiche Erläuterungen an, was darunter zu verstehen ist.

Beispiel:

> Personenbezogene Daten umfassen auch das von einer Kamera aufgezeichnete Bild einer Person. Dementsprechend stellt eine solche Videoaufzeichnung grundsätzlich eine „Verarbeitung personenbezogener Daten" dar [Europäischer Gerichtshof, Urteil vom 11. Dezember 2014, C-212/13, Rn. 21 ff.].

Personenbezogene Daten können auch ohne technische Hilfe verarbeitet werden.

Beispiel:

> Selbst handschriftliche Notizen in einem Notizbuch können eine Verarbeitung sein, wenn für sie der Anwendungsbereich der Datenschutz-Grundverordnung eröffnet ist (ausführlich dazu in Abschnitt 3.2, der sich mit der nichtautomatisierten Verarbeitung befasst).

1.4.3 Für die Verarbeitung Verantwortlicher

Der für die Verarbeitung personenbezogener Daten **Verantwortliche** ist der zentrale Adressat von datenschutzrechtlichen Pflichten. → Art. 4 Nr. 7 DSGVO beschreibt ihn als Stelle, die über die Zwecke und Mittel einer Verarbeitung personenbezogener Daten entscheidet. Die Entscheidung kann allein getroffen werden oder gemeinsam mit anderen Stellen.

Für bayerische öffentliche Stellen sieht → Art. 3 Abs. 2 BayDSG vor, dass Verantwortlicher regelmäßig die für die Verarbeitung zuständige öffentliche Stelle ist.

Beispiel:

> Eine Gemeinde ist öffentliche Stelle im Sinn von → Art. 1 Abs. 1 BayDSG, daher Verantwortlicher für zahlreiche Verarbeitungen – von der Meldestelle über das Steueramt bis zur Bauverwaltung.

Vertiefung:

> Das Fachrecht kann besondere Regelungen enthalten. So legt § 67 Abs. 4 Zehntes Buch Sozialgesetzbuch (SGB X) fest, wer im Bereich des Sozialdatenschutzes als Verantwortlicher anzusehen ist. Aus § 67 Abs. 4 Satz 2 SGB X folgt, dass beispielsweise das Sozialamt einer Stadt ein eigenständiger Verantwortlicher ist.

Für die datenschutzrechtliche Verantwortlichkeit ist es nicht erforderlich, dass die Stelle selbst personenbezogene Daten verarbeitet. Es genügt, wenn sie aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel einer Verarbeitung mitwirkt.

1.4.4 Betroffene Person

Die betroffene Person ist das Gegenüber des Verantwortlichen. Ihre personenbezogenen Daten sind Gegenstand der Verarbeitung. Die Datenschutz-Grundverordnung führt diese „Rolle" zusammen mit der Begriffsbestimmung der personenbezogenen Daten ein (→ Art. 4 Nr. 1 DSGVO). Der betroffenen Person werden in zahlreichen Vorschriften Rechte zugeordnet (etwa in Art. 15 ff. DSGVO, siehe Abschnitte 5.4 bis 5.11). Ihr gegenüber hat der Verantwortliche Pflichten (etwa aus Art. 13 und 14 oder Art. 34 DSGVO, siehe Abschnitte 5.2 und 5.3). Zugunsten der betroffenen Person wirkt auch das Datenschutzgrundrecht, das ihr ein Abwehrrecht gegen rechtswidrige Verarbeitungen vermittelt, siehe Abschnitte 2.1 und 4.1).

2 Datenschutz als Grundrechtsschutz

„Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht." So lautet der erste Satz des ersten Erwägungsgrundes zur Datenschutz-Grundverordnung. Er verweist vor allem auf die Grundrechte, die in der Charta der Grundrechte der Europäischen Union niedergelegt sind. Diese Charta wurde im Jahr 2000 verabschiedet und gehört seit dem Vertrag von Lissabon im Jahr 2009 zum „EU-Primärrecht", also zu den Verträgen, die das rechtliche Fundament der Europäischen Union bilden.

Zuvor nahm das EU-Primärrecht auf die Grundrechte der Europäischen Menschenrechtskonvention (EMRK) Bezug sowie auf die Grundrechte, wie sie der gemeinsamen – teilweise langen – Verfassungstradition der Mitgliedstaaten entsprechen. Zur Erleichterung des Verständnisses werden nachstehend einige Grundlinien erläutert, die das Datenschutzgrundrecht nach deutschem Verständnis kennzeichnen.

2.1 Grundrechtsschutz im deutschen Verfassungsrecht

Grundrechte haben zunächst einmal die Funktion, dem einzelnen Bürger und der einzelnen Bürgerin zu helfen, Eingriffe des Staates in ihre Freiheiten abzuwehren. Kurz gefasst: Grundrechte vermitteln **Abwehrrechte** gegenüber dem Staat.

> Art. 1 Abs. 3 Grundgesetz
> Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Ein Grundrecht auf Datenschutz ist im **Grundgesetz für die Bundesrepublik Deutschland** (GG) nicht ausdrücklich vorgesehen. Dennoch ist der Datenschutz grundrechtlich verankert. Zunächst gibt es einige Grundrechte, die spezielle Fragen des Datenschutzes betreffen. Dazu zählen insbesondere das **Brief-, Post- und Fernmeldegeheimnis** aus Art. 10 GG und die Garantie der **Unverletzlichkeit der Wohnung** in Art. 13 GG. Weil sie ausdrücklich im Grundgesetz aufgeführt sind, werden sie manchmal auch als „benannte Persönlichkeitsrechte" bezeichnet.

Die Grundrechte aus Art. 10 GG schützen Kommunikationsverhältnisse, bei denen die Grundrechtsträger auf die Unterstützung Dritter angewiesen sind (beim Brief- und Postgeheimnis insbesondere auf die Post, bei der Telekommunikation insbesondere auf die Telekommunikationsanbieter). Das Grundrecht auf Unverletzlichkeit

der Wohnung aus Art. 13 GG schützt insbesondere die vertrauliche Kommunikation in der Wohnung. Die Wohnung soll dadurch als privater Rückzugsraum des Einzelnen geschützt werden.

Ansonsten wird der grundrechtlich gewährleistete Datenschutz in Deutschland zumeist aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) abgeleitet. Auch heute noch grundlegend für das Verständnis von Datenschutz ist das Volkszählungsurteil aus dem Jahr 1983 (BVerfGE 65, 1 ff. im Internet abrufbar unter http://www.servat.unibe.ch/dfr/bv065001.html).

> Das Bundesverfassungsgericht hatte in diesem Fall das Volkszählungsgesetz 1983 zu beurteilen. Volkszählungen werden durchgeführt, um eine tatsachengestützte Grundlage für politische Planungsentscheidungen zu gewinnen.
>
> Die Volkszählung 1983 war allerdings besonders. Zum ersten Mal in Deutschland wurde eine Volkszählung mithilfe der automatisierten Datenverarbeitung durchgeführt. Die erhobenen Daten sollten allerdings dem Volkszählungsgesetz zufolge nicht nur für statistische Zwecke verwendet werden. Vielmehr sollten sie beispielsweise auch dazu eingesetzt werden, um amtliche Melderegister auf ihre Richtigkeit und Vollständigkeit zu überprüfen. Das löste zahlreiche Proteste in der Bevölkerung aus.
>
> Das Bundesverfassungsgericht erklärte einige Regelungen des damaligen Volkszählungsgesetzes für verfassungswidrig. Vor allem aber leitete das Gericht aus dem allgemeinen Persönlichkeitsrecht ein **Recht auf informationelle Selbstbestimmung** ab. Hier die drei ersten Leitsätze des Urteils, welche die Reichweite des neuen Grundrechts beschreiben:
>
> „1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 Grundgesetz umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.
>
> 2. Einschränkungen dieses Rechts auf ‚informationelle Selbstbestimmung' sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.
>
> 3. Bei den verfassungsrechtlichen Anforderungen an derartige Einschränkungen ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anony-

> mer Form erhoben und verarbeitet werden, und solchen, die für statistische Zwecke bestimmt sind. Bei der Datenerhebung für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden. Der Informationserhebung und Informationsverarbeitung müssen aber innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen." [BVerfGE 65, 1 f.]

Das Volkszählungsurteil hat das allgemeine Persönlichkeitsrecht im Hinblick auf die Bedingungen der automatisierten Datenverarbeitung zu einem Recht auf informationelle Selbstbestimmung weiterentwickelt.

> „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen." [BVerfGE 65, 1/43]

Das Gericht hat freilich auch klargestellt, dass diese Befugnis nicht als uneingeschränktes Herrschaftsrecht missverstanden werden darf. **Die betroffene Person kann also nicht wie im Grundsatz hinsichtlich ihres Eigentums über ihre Daten verfügen und andere von der Datenverarbeitung nach Belieben gänzlich ausschließen.** Die hoheitliche Datenverarbeitung muss allerdings gesetzlich legitimiert sein und ist für die betroffenen Personen so transparent wie möglich zu gestalten. Auch heute noch wenden sich Bürgerinnen und Bürger an die Datenschutz-Aufsichtsbehörden, die ihr Grundrecht auf Datenschutz als eine Art Eigentum an ihren Daten (miss-)verstehen. Sie kann die Datenschutz-Aufsichtsbehörde in ihrem Anliegen oft nicht unterstützen, wenn der Gesetzgeber die Verarbeitung ihrer personenbezogenen Daten auch gegen ihren Willen ausdrücklich erlaubt.

In seiner Urteilsbegründung hat das Bundesverfassungsgericht hervorgehoben, dass es unter den Bedingungen der automatisierten Datenverarbeitung im Grundsatz **keine belanglosen personenbezogenen Daten** mehr geben könne. Um die Auswirkungen einer Datenverarbeitung für das Persönlichkeitsrecht beurteilen zu können, müsse vielmehr der konkrete **Verwendungszusammenhang** bekannt sein.

In anderen Entscheidungen hat das Bundesverfassungsgericht klargestellt, dass die Erhebung und Verwendung von Daten, die dem **Kernbereich der privaten Lebensgestaltung** zuzuordnen sind, strikt verboten ist. Der besondere Schutz dieser Daten gründet in der Menschenwürde (Art. 1 Abs. 1 GG). Die Würde des Menschen ist jedoch unantastbar – sie darf nicht beeinträchtigt werden.

Beispiel:

> Selbst zur Aufklärung eines Mordfalls dürfen Strafverfolgungsbehörden nicht ein Beichtgespräch der mutmaßlichen Täterin oder des mutmaßlichen Täters mit einer Seelsorgerin oder einem Seelsorger abhören.

Sieht man von diesen absolut geschützten Daten ab, können Eingriffe in das Recht auf informationelle Selbstbestimmung gerechtfertigt sein. Denn personenbezogene Daten „gehören" nicht nur dem betroffenen Menschen. Jeder Mensch ist Teil einer miteinander kommunizierenden Gemeinschaft. Dementsprechend sind Einschränkungen des Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse verfassungsrechtlich durchaus möglich. Dazu allerdings muss ein **hinreichend bestimmtes Gesetz** sie erlauben. Das bedeutet in erster Linie, dass der Gesetzgeber den Verwendungszweck der zu erhebenden Daten bestimmt und klar festlegt.

Die Verwaltung ist an die gesetzlich festgelegten Zwecke gebunden. Das **Zweckbindungsprinzip** ist ein zentrales Prinzip auch des einfachgesetzlichen Datenschutzrechts. Für Verwendungsbereiche mit besonderer Grundrechtsrelevanz sind bereichsspezifische Regelungen erforderlich. Das Prinzip der Zweckbindung soll sicherstellen, dass die betroffene Person zumindest grundsätzlich überschauen kann, welche sie betreffende Informationen in bestimmten Bereichen ihrer sozialen Umwelt bekannt sind. Sie soll abschätzen können, was Kommunikationspartnerinnen und Kommunikationspartner über sie wissen – und was sie mit diesem Wissen anstellen. Danach dürfen Daten im Grundsatz nur zu dem gleichen Zweck verwendet und insbesondere weitergegeben werden, zu dem sie erhoben worden sind. Nachträgliche Zweckänderungen sind zwar möglich, erfordern aber ihrerseits eine verfassungsgemäße Rechtsgrundlage.

Beispiel 1:

> Für die polizeiliche Datenverarbeitung haben die Polizeigesetze Regelungen vorzusehen, welche die polizeilichen Besonderheiten berücksichtigen. Beispielsweise sollen diese Vorschriften es der Polizei ermöglichen, Straftaten effektiv zu verhüten.

Beispiel 2:

> Das Sozialgesetzbuch enthält eine grundsätzlich abgeschlossene Regelung des Datenschutzes für den Bereich der sozialen Leistungsgewährung (siehe insbesondere §§ 67 ff. SGB X).

Die Festlegung des Verwendungszweckes ist auch notwendig, um die **Verhältnismäßigkeit** eines informationellen Grundrechtseingriffs beurteilen zu können. Der Grundsatz der Verhältnismäßigkeit besagt, dass eine hoheitliche Maßnahme einen legitimen Zweck haben und dass sie zu dessen Verfolgung geeignet, erforderlich und

angemessen sein muss. Bei der Verhältnismäßigkeit einer behördlichen Maßnahme im Gesetzesvollzug ist der „legitime Zweck" gleichbedeutend mit dem Gesetzeszweck. Die Geeignetheit, Erforderlichkeit und Angemessenheit ist also auf den Zweck der gesetzlichen Befugnis zu beziehen, auf die sich die Maßnahme stützt.

Beispiel (Fehlen von Geeignetheit und Erforderlichkeit):

> Die Aufzeichnung einer Videoüberwachungsanlage kann unter bestimmten Voraussetzungen die Aufklärung einer Straftat erleichtern. Sofern die Voraussetzungen vorliegen, ist sie zu diesem Zweck **geeignet**.
>
> Die Polizei hat mithilfe der Videoaufzeichnungen einen Straftäter überführt. Die Videoaufzeichnung war zur Ermittlung des Straftäters **erforderlich**, weil es keine ähnlich geeigneten, milderen Mittel gab, um den Straftäter ausfindig zu machen.
>
> Der Straftäter ist rechtskräftig verurteilt worden und sitzt seine Strafe ab. Jetzt ist die Aufzeichnung nicht mehr zur Aufklärung der begangenen Straftat erforderlich, weil sie ihren Zweck schon erreicht hat. Gibt es keine anderen Gründe zur Aufbewahrung der Aufzeichnung, ist sie zu löschen.

Zentraler Prüfungspunkt bei der Verhältnismäßigkeit ist oft die Angemessenheit: Die mit der Maßnahme verbundene Belastung einer betroffenen Person darf nicht außer Verhältnis zu dem angestrebten Ziel stehen. Bei der Überprüfung der Angemessenheit kommt es meist auf eine **Abwägung der widerstreitenden Rechtsgüter** (beim Datenschutzgrundrecht insbesondere: Position der betroffenen Person gegen Verarbeitungsinteresse der Behörde) an.

Greift eine Maßnahme in ein Grundrecht ein, ohne dass es hierzu eine gesetzliche Grundlage gibt, ist die Maßnahme schon deshalb rechtswidrig. Dieser **grundrechtliche Gesetzesvorbehalt** ist eine besondere Ausprägung der Gesetzmäßigkeit der Verwaltung und zählt zu den zentralen Prinzipien unseres Rechtsstaates (Art. 20 Abs. 3 GG). Die Prüfung des Verhältnismäßigkeitsgrundsatzes erübrigt sich in einem solchen Fall.

Das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG gewinnt im Verhältnis zu spezielleren Freiheitsrechten – etwa Art. 10 und 13 GG – an Bedeutung, wenn moderne Entwicklungen neue Gefährdungen für die menschliche Persönlichkeit erzeugen können.

So hat das Bundesverfassungsgericht im Jahr 2008 aus dem allgemeinen Persönlichkeitsrecht auch ein „**Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**" abgeleitet. Häufig wird dieser komplizierte Namen durch die etwas ungenauere dafür aber einfachere Kurzform „IT-Grundrecht" ersetzt. Die neue grundrechtliche Gewährleistung ist notwendig, weil

die Nutzung der modernen Informationstechnologie rapide zugenommen hat. Zugleich kann die Nutzerin oder der Nutzer wegen der technischen Komplexität oft nicht mehr selbst die Vertraulichkeit und Integrität eigener IT-Systeme (etwa des Smartphones) sicherstellen. Das Recht auf informationelle Selbstbestimmung und auch andere Persönlichkeitsrechte laufen leer, weil sie nur die Daten und ihre Kommunikation, nicht aber das IT-System schützen. Das IT-Grundrecht schließt diese Schutzlücke. Es sichert den persönlichen Bereich auch dann, wenn auf das IT-System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten.

Beispiel:

Einige Polizeigesetze und einige Verfassungsschutzgesetze sehen die Befugnis zur sogenannten **Online-Durchsuchung** vor. Bei dieser Maßnahme infiltriert die Sicherheitsbehörde das von ihr angegriffene IT-System heimlich mit Hilfe eines Spähprogramms („Staatstrojaner"), um an die auf dem IT-System gespeicherten Daten zu gelangen. Eine derartige Online-Durchsuchung ist ein schwerwiegender Eingriff in das IT-Grundrecht. Die Integrität des IT-Systems ist verletzt, und in aller Regel erkennen die Betroffenen diese verdeckte Manipulation nicht. Zugleich kann die Ermittlungsbehörde mit einem Schlag Zugriff auf einen Datenbestand erhalten, der ein aussagekräftiges Persönlichkeitsbild über die betroffene Nutzerin oder den betroffenen Nutzer zeichnet. Da heute viele mithilfe ihrer IT-Systeme auch telefonieren und E-Mails austauschen können, kann eine solche Infiltration auch die Überwachung von Telekommunikation ermöglichen. Angesichts der äußerst hohen Eingriffsintensität ist eine Online-Durchsuchung nur unter strengen Voraussetzungen verfassungskonform. Es müssen tatsächliche Anhaltspunkte für eine konkrete Gefahr für ein überragend wichtiges Rechtsgut wie Leib, Leben oder Freiheit der Person vorliegen. Die Maßnahme darf grundsätzlich nur auf richterliche Anordnung hin erfolgen, vgl. [Bundesverfassungsgericht, Urteil vom 27. Februar 2008, 1 BvR 370/07]. – Die Strafprozessordnung (StPO) hat übrigens lange Zeit keine Online-Durchsuchung vorgesehen. Da ein Grundrechtseingriff stets nur auf gesetzlicher Grundlage erlaubt sein kann, war eine Online-Durchsuchung zur Strafverfolgung in Deutschland nicht gestattet. Erst Mitte 2017 hat der Bundesgesetzgeber eine Befugnis zur Online-Durchsuchung in die Strafprozessordnung eingefügt (§ 100b StPO).

Bisher war von Risiken die Rede, die das Datenschutzgrundrecht im öffentlichen Sektor trifft. Nicht wenige Gefährdungen gehen aber von **privaten Unternehmen** aus, zumal wenn sie grenzüberschreitend agieren.

Beispiele:

Ein Arbeitgeber installiert heimlich Videokameras, mit denen er seine Beschäftigten überwacht. – Kreditinstitute und Versicherungen machen den Abschluss von Verträgen mit Verbraucherinnen und Verbrauchern oft von umfangreichen Datenerhebungen abhängig.

Wenn das Bundesverfassungsgericht in seinem für das Datenschutzrecht noch immer grundlegenden Volkszählungsurteil aus dem Jahr 1983 festhält:

> „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß" [BVerfGE 65, 1/43],

so beschreibt dieser Hinweis auch Risiken, die bei der Verarbeitung personenbezogener Daten durch Unternehmen entstehen können.

Der Staat muss Bürgerinnen und Bürger auch gegenüber Unternehmen oder anderen privaten Institutionen schützen. Bei der Ausübung dieser **grundrechtlichen Schutzpflicht** muss er einen angemessenen Ausgleich zwischen den konkurrierenden Freiheitsrechten auf Datenschutz einerseits und auf wirtschaftliche Betätigung andererseits schaffen. Dies geschieht durch einfachgesetzliche Regelungen – wie etwa die Datenschutzgesetze. Als Mindestanforderungen sind dabei insbesondere eine angemessene Zweckbindung der Datenverarbeitung, die Sicherheit der Daten und die Transparenz des Datenumgangs sicherzustellen.

Ach, übrigens:

> Die Inhalte der widerstreitenden Grundrechte sind dann im Rahmen der Auslegung des einfachen Gesetzesrechts zu berücksichtigen. Im deutschen Verfassungsrecht wird diese Wirkungsweise der Grundrechte **„mittelbare Drittwirkung von Grundrechten"** genannt.

2.2 Datenschutz im deutschen Verfassungsgefüge

Das nationale Datenschutzrecht war schon vor der Datenschutzreform 2018 auf zwei Ebenen geregelt. Der Bund hatte mit dem bis zum 24. Mai 2018 geltenden (alten) Bundesdatenschutzgesetz (BDSG-alt) eine „Vollregelung" geschaffen, die in erster Linie Verarbeitungen öffentlicher Stellen des Bundes (insbesondere also der Bundesbehörden) betraf und daneben einen Rechtsrahmen für Verarbeitungen durch nicht-öffentliche Stellen (insbesondere Unternehmen) bereithielt. Zudem hatten die Länder nach und nach Landesdatenschutzgesetze erlassen. Gegenstand dieser Regelungen waren Verarbeitungen durch die jeweiligen Landesbehörden.

Die Gesetzgeber im Bund wie in den Ländern hatten bei der Schaffung datenschutzrechtlicher Vorschriften die Vorgaben des Grundgesetzes zu beachten, insbesondere also die Weisungen, die das soeben angesprochene Recht auf informationelle

Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) für die Gesetzgebung bereithält. Von den Landesgesetzgebern konnten daneben noch entsprechende Vorgaben in den Landesverfassungen zu berücksichtigen sein.

Da ein „allgemeines" Datenschutzgesetz weder auf der Bundesebene noch auf der Länderebene der Vielfalt tatsächlich anzutreffender Verarbeitungssituationen gerecht werden konnte, bestanden neben diesen Regelungen noch bereichsspezifische Datenschutzbestimmungen. Manchmal waren dies einzelne Vorschriften in Fachgesetzen, manchmal aber auch ganze Abschnitte, die den Datenschutz für einen Lebensbereich (etwa das Sozialrecht) ganz und gar selbstständig regelten. Solche bereichsspezifischen Datenschutzbestimmungen gab es sowohl auf der Bundes- wie auf der Landesebene, dort insbesondere im Polizeirecht, im Beamtenrecht oder im Schulrecht.

Hatte eine Verwaltungsbehörde Datenschutzvorschriften anzuwenden, hatte sie zunächst zu klären, ob bereichsspezifisches Datenschutzrecht einschlägig war. Dieses hatte dann grundsätzlich Vorrang. Fehlte es an bereichsspezifischen Regelungen, konnte die Behörde auf „ihr" allgemeines Datenschutzgesetz zurückgreifen – also entweder auf das Bundes- oder das jeweilige Landesdatenschutzgesetz. Erforderlichenfalls hatte sie – etwa bei der Auslegung nicht ganz klarer Rechtsbegriffe oder bei der Ausfüllung eines gesetzlich eröffneten Entscheidungsspielraums – Stichwort: „Ermessen" – verfassungsrechtliche Vorgaben, insbesondere das Recht auf informationelle Selbstbestimmung heranzuziehen.

2.3 Datenschutz in der Welt der Datenschutz-Grundverordnung

Die in Abschnitt 2.2 kurz skizzierte, vergleichsweise übersichtliche Ordnung des Datenschutzes vor dem 25. Mai 2018 ist nun etwas komplizierter geworden. Die seit diesem Tag geltende Datenschutz-Grundverordnung hat eine umfassende Anpassungsgesetzgebung in den Mitgliedstaaten ausgelöst. In Deutschland waren sowohl auf der Bundes- wie auf der Länderebene zum einen die allgemeinen Datenschutzgesetze betroffen. Am 25. Mai 2018 sind daher auch ein neues Bundesdatenschutzgesetz sowie ein neues Bayerisches Datenschutzgesetz in Kraft getreten. Zum anderen war das bereichsspezifische Datenschutzrecht grundlegend zu überarbeiten. Diese Reform ist in Bayern weitgehend abgeschlossen.

Der bewährte Regelungsbestand konnte nur zu einem Teil beibehalten werden. Bei der Neuregelung war insbesondere zu beachten:

– Die Datenschutz-Grundverordnung versteht sich im Grundsatz als „Vollregelung", die sowohl Verarbeitungen im öffentlichen wie im nicht-öffentlichen Sektor

betrifft. Sie eröffnet den Mitgliedsstaaten (lediglich) Regelungsspielräume, die ausgefüllt werden müssen oder ausgefüllt werden können.

- Von der Datenschutz-Grundverordnung abweichende Regelungen sind nicht zulässig, es sei denn, die Datenschutz-Grundverordnung ermächtigt ausdrücklich dazu.
- Die nationalen Gesetzgeber dürfen keine „Regelungsdubletten" erzeugen – die wörtliche oder sinngemäße Wiederholung von Regelungen aus der Datenschutz-Grundverordnung ist grundsätzlich nicht zulässig.
- Die nationalen Gesetzgeber dürfen bei der Definition von Begriffen, welche die Datenschutz-Grundverordnung vorgibt (so etwa „personenbezogene Daten", „Verarbeitung", „Verantwortlicher"), nicht vom Sprachgebrauch des Unionsrechts abweichen.

Dieser Handlungsrahmen hat zur Folge, dass das nationale Recht keine „Vollregelung" des Datenschutzrechts mehr anbieten kann. Datenschutz-Grundverordnung und nationale Regelungen stehen in einem Ergänzungsverhältnis. **Bei der Rechtsanwendung in den Verwaltungsbehörden müssen Datenschutz-Grundverordnung und nationale Regelungen immer „nebeneinandergelegt" werden.** Muss eine Behörde die Bedeutung eines unklaren Rechtsbegriffs ermitteln oder einen gesetzlich eröffneten Entscheidungsspielraum ausfüllen, hat sie nun auch das EU-Datenschutzgrundrecht zu berücksichtigen.

3 Zum Anwendungsbereich des EU-Datenschutzrechts – Wann und wo gilt die Datenschutz-Grundverordnung?

Wofür und wo gilt die Datenschutz-Grundverordnung? Antwort auf diese Frage geben die Vorschriften zum sachlichen (→ Art. 2 DSGVO) und räumlichen Anwendungsbereich (→ Art. 3 DSGVO).

3.1 Automatisierte Verarbeitung personenbezogener Daten

→ Art. 2 Abs. 1 DSGVO hält zunächst fest, dass die Datenschutz-Grundverordnung für die „ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten" gilt. Im Grundsatz verfolgt die Datenschutz-Grundverordnung einen „technologieneutralen Ansatz": Der Datenschutz soll nicht von den verwendeten Techniken abhängen (Erwägungsgrund 15 DSGVO). Wer → Art. 2 Abs. 1 DSGVO liest, wird allerdings feststellen, dass die nichtautomatisierte Verarbeitung nur unter ganz bestimmten Voraussetzungen datenschutzrechtlich relevant ist. In Bezug auf die automatisierte Verarbeitung personenbezogener Daten hingegen gibt es nur einige Ausnahmefälle, in denen die Anwendung der Datenschutz-Grundverordnung nach → Art. 2 Abs. 2 DSGVO ausgeschlossen ist.

Beispiel:

> Eine automatisierte Verarbeitung personenbezogener Daten ist etwa die Videoaufzeichnung von Personen: Bei der Videoaufzeichnung werden personenbezogene Daten erhoben und gespeichert – beide Tätigkeiten sind in → Art. 4 Nr. 2 DSGVO ausdrücklich als Beispiele für die Verarbeitung personenbezogener Daten aufgeführt [siehe auch Europäischer Gerichtshof, Urteil vom 11. Dezember 2014, C-212/13, Rn. 23 f.].

3.2 Nichtautomatisierte Verarbeitung personenbezogener Daten

Die Datenschutz-Grundverordnung gilt für die nichtautomatisierte Verarbeitung personenbezogener Daten immer dann, wenn die Daten in einem „Dateisystem" gespeichert sind oder gespeichert werden sollen, → Art. 2 Abs. 1 DSGVO. Diesen Begriff erläutert → Art. 4 Nr. 6 DSGVO. Die Vorgängerregelung Art. 2 Buchst. c Richtlinie 95/46/EG verwandte noch den Begriff der „Datei", meinte damit aber das Gleiche.

Es geht dabei um eine Datensammlung, die so strukturiert ist, dass man die gespeicherten Daten leicht wiederfindet. Die Begriffe „Datei" bzw. „Dateisystem" sind weit zu verstehen.

Beispiel:

> Die Mitglieder einer Religionsgemeinschaft gehen bei ihrer Verkündigungstätigkeit von Tür zu Tür. Sie notieren dabei den Namen, die Adressen und weitere Informationen über die aufgesuchten Personen in Notizbüchern. Die Mitglieder werden von der Religionsgemeinschaft nur in bestimmten Gebieten eingesetzt. – In diesem Beispielsfall hat der Europäische Gerichtshof angenommen, dass die Sammlung personenbezogener Daten durch die Mitglieder vermutlich in einer Datei gespeichert ist. Eine Datei setzte nur eine Sammlung von Informationen voraus, die nach bestimmten Kriterien so strukturiert sind, dass sie in der Praxis zur späteren Verwendung leicht wiederauffindbar sind. Um unter diesen Begriff zu fallen, muss eine solche Sammlung nicht aus spezifischen Kartotheken oder Verzeichnissen oder anderen der Recherche dienenden Ordnungssystemen bestehen [Europäischer Gerichtshof, Urteil vom 10. Juli 2018, C-25/17, Rn. 52 ff.].

Für Verarbeitungen durch bayerische öffentliche Stellen, die nicht unter → Art. 2 Abs. 1 und 2 DSGVO fallen, hat der Landesgesetzgeber die Datenschutz-Grundverordnung in → Art. 2 Satz 1 BayDSG für anwendbar erklärt. Für die nichtautomatisierte Verarbeitung personenbezogener Daten gelten deshalb im Wesentlichen die gleichen Vorschriften wie für die automatisierte Verarbeitung (einschränkend aber → Art. 2 Satz 1 BayDSG).

3.3 Ausnahmen: Wofür die Datenschutz-Grundverordnung nicht gilt

Wenn personenbezogene Daten verarbeitet werden, gilt also in aller Regel die Datenschutz-Grundverordnung. Von dieser Regel gibt es allerdings einige Ausnahmen, die nachfolgend vorgestellt werden.

3.3.1 Ausschließlich persönliche oder familiäre Tätigkeiten

Die Datenschutz-Grundverordnung ist nicht auf die Verarbeitung personenbezogener Daten anzuwenden, soweit sie „durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten" (→ Art. 2 Abs. 2 Buchst. c DSGVO) erfolgt.

Nach der Rechtsprechung des Europäischen Gerichtshofs ist diese bereits in Art. 3 Abs. 2 2. Spiegelstrich Richtlinie 95/46/EG enthaltene Vorschrift – die sogenannte „Haushaltsausnahme" – sehr genau zu lesen: Es geht nicht darum, dass Menschen Daten für persönliche oder familiäre Zwecke verarbeiten.

Beispiel:

Frau Lindqvist arbeitete ehrenamtlich in einer schwedischen Kirchengemeinde mit. Sie hatte eine private Internetseite, auf der sie – leicht humorig – die Namen, Freizeitaktivitäten und Besonderheiten von Bekannten vorstellte, die sich ebenfalls in der Kirchengemeinde engagierten. Offenbar fanden es nicht alle ihrer Bekannten witzig, was Frau Lindqvist über sie veröffentlicht hatte. Jedenfalls wurde sie angezeigt und gegen sie ein Strafverfahren eingeleitet. In diesem Verfahren wurde der Europäische Gerichtshof angerufen. Sinngemäß richteten die schwedischen Gerichte die Frage an ihn, ob Frau Lindqvist einen schwerwiegenden Datenschutzverstoß begangen habe.

Dazu müssten die Veröffentlichungen von Frau Lindqvist zunächst einmal eine Verarbeitung personenbezogener Daten sein, auf die die Datenschutz-Grundverordnung anzuwenden ist. Der Name in Verbindung mit Freizeitaktivitäten stellt ein personenbezogenes Datum dar, weil man diese Angaben konkreten Personen zuordnen kann. Nach → Art. 4 Nr. 2 DSGVO zählen die Offenlegung, Übermittlung, Verbreitung oder andere Formen der Bereitstellung zu den Regelbeispielen der Verarbeitung. Genau das hat Frau Lindqvist gemacht [siehe auch Europäischer Gerichtshof, Urteil vom 6. November 2003, C-101/01, Rn. 25].

Dass eine Verarbeitung personenbezogener Daten erfolgt war, ist also recht eindeutig aus der Datenschutz-Grundverordnung abzuleiten. Streitig war aber, ob eine Ausnahme nach → Art. 2 Abs. 2 Buchst. c DSGVO vorlag – ob also Frau Lindqvist eine Verarbeitung personenbezogener Daten „zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten" vorgenommen hat.

Der Europäische Gerichtshof stellte dazu fest, dass Frau Lindqvist auf ihrer Webseite Angaben über andere Personen an einen unbegrenzten Personenkreis richtete. Maßgeblich sei nicht das private Motiv von Lindqvist gewesen, sondern dass die Daten an Personen und Stellen außerhalb ihrer privaten Sphäre gelangt seien. Ihre Verarbeitung überschreite deshalb den Rahmen der ausschließlich persönlichen und familiären Tätigkeit [vgl. Europäischer Gerichtshof Urteil vom 6. November 2003, C-101/01, Rn. 47].

Erwägungsgrund 18 DSGVO führt dazu jetzt aus: „Als persönliche oder familiäre Tätigkeit könnte auch das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten gelten. Diese Verordnung gilt jedoch für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen."

Nach diesem Erwägungsgrund ist nicht mehr ganz klar, wo konkret die Grenze zwischen der Verarbeitung zur Ausübung ausschließlich persönlich-familiärer Tätigkeiten und einer Verarbeitung verläuft, die nach der Datenschutz-Grundverordnung zu

beurteilen ist. Trotzdem liegt es bis auf weiteres nahe, den Maßstab des Europäischen Gerichtshofs anzuwenden, wonach eine Verarbeitung nicht mehr ausschließlich zur persönlichen oder familiären Tätigkeit erfolgt, wenn sie **außerhalb des Bereichs der privaten Sphäre** desjenigen vorgenommen wird, der die Daten verarbeitet.

Beispiel:

> Herr Ryneš wurde wiederholt von einem Unbekannten angegriffen. Daraufhin richtete er auf seinem Privatgrundstück eine Videokamera ein. Die Kamera erfasste nicht nur das eigene Grundstück, sondern auch einen Teil der angrenzenden öffentlichen Straße und den Eingang eines gegenüber liegenden Hauses. – Herr Ryneš hat die Videoüberwachung eingerichtet, allein um sich selbst vor Angriffen zu schützen. Insofern könnte man vertreten, dass die Videoüberwachung für persönlich-familiäre Zwecke erfolgte. Hierauf kommt es gemäß der Rechtsprechung des Europäischen Gerichtshofs aber nicht an. Maßgeblich ist vielmehr, ob die Verarbeitung die private Sphäre von Herrn Ryneš überschritten hat oder nicht. Die räumliche private Sphäre von Herrn Ryneš endet an den Grenzen seines Grundstücks. Soweit die Kamera auch den öffentlichen Verkehrsraum erfasst, liegt eine Verarbeitung vor, die nicht ausschließlich für private oder familiäre Tätigkeiten vorgenommen wird. Erst recht gilt dies für die Überwachung des Eingangs des Nachbarhauses (so auch [Europäischer Gerichtshof, Urteil vom 11. Dezember 2014, C-212/13, Rn. 31 und 33])

Bei der Beurteilung, ob eine Verarbeitung ausschließlich für eine persönliche oder familiäre Tätigkeit erfolgt, kommt es auf die Tätigkeit der Person an, die personenbezogene Daten verarbeitet.

Rückblick:

> Im bereits vorgestellten Fall der Verkündigungstätigkeit einer Religionsgemeinschaft (Abschnitt 3.2) werden die aufgesuchten Personen auf ihre persönlichen religiösen Überzeugungen angesprochen. Die Religionsgemeinschaft vertrat im Gerichtsverfahren wohl die Auffassung, deshalb handle es sich um eine Verarbeitung, die ausschließlich für private Tätigkeiten der besuchten Personen erfolge. Das allgemeine Datenschutzrecht finde demzufolge keine Anwendung. – Diese Auffassung beruht auf einem Missverständnis von → Art. 2 Abs. 2 Buchst. c DSGVO: Es kommt nicht darauf an, dass die Verarbeitung den persönlichen oder familiären Bereich der besuchten Personen betrifft (also derjenigen, die Betroffene einer Verarbeitung sind), sondern auf die Mitglieder der Religionsgemeinschaft (also derjenigen, die personenbezogene Daten verarbeiten). Soweit die Mitglieder der Religionsgemeinschaft fremde Personen auf deren religiöse Überzeugungen ansprechen, verlassen sie ihre eigene privaten Sphäre, die Verarbeitung fällt dann in den Anwendungsbereich der Datenschutz-Grundverordnung [Europäischer Gerichtshof, Urteil vom 10. Juli 2018, Rechtssache C 25/17, Rn. 41].

3.3.2 Tätigkeit außerhalb des Anwendungsbereichs des Unionsrechts

Die Datenschutz-Grundverordnung gilt nicht für die Verarbeitung personenbezogener Daten im Zusammenhang mit Tätigkeiten, die „nicht in den Anwendungsbereich des Unionsrechts“ fallen, → Art. 2 Abs. 2 Buchst. a DSGVO. Nach Erwägungsgrund 16 DSGVO gehört dazu insbesondere die Verarbeitung im Zusammenhang mit der nationalen Sicherheit.

Beispiel 1:

> Die Verarbeitung personenbezogener Daten im Zusammenhang mit der Landesverteidigung ist im Grundsatz nicht nach der Datenschutz-Grundverordnung zu beurteilen. Das neue Bundesdatenschutzgesetz enthält dazu mit § 85 BDSG eine Regelung.

Beispiel 2:

> Die Datensammlung durch Nachrichtendienste betrifft ebenfalls die nationale Sicherheit. Deshalb ist die Datenschutz-Grundverordnung grundsätzlich nicht auf sie anzuwenden.

Vertiefung:

> Weitere Ausnahmen lassen sich ermitteln, wenn man den Anwendungsbereich des EU-Rechts klärt. Aufschluss geben hier insbesondere der Vertrag über die Europäische Union (EUV), der Vertrag über die Arbeitsweise in der Europäischen Union und die Charta der Grundrechte der Europäischen Union. Eine Zuständigkeitsregelung, die sich auf den Anwendungsbereich der Datenschutz-Grundverordnung auswirkt, enthält etwa → Art. 4 Abs. 2 Satz 2 EUV. Danach achtet die Europäische Union die grundlegenden Funktionen der Mitgliedstaaten.

Beispiel:

> Soweit der Bundestag oder ein Landtag Kernaufgaben des Parlaments wahrnimmt, gilt die Datenschutz-Grundverordnung nicht. Anderes gilt für die Verarbeitung personenbezogener Daten, soweit die Bundestags- oder Landtagsverwaltung in Verwaltungsangelegenheiten tätig wird → Art. 1 Abs. 1 Satz 2 BayDSG. Die Durchführung von Petitionsverfahren wird der parlamentarischen Funktion des Landtags zugeordnet. Auch wenn Abgeordnete im Rahmen einer Gesetzgebungsdebatte personenbezogene Daten erörtern, findet das allgemeine Datenschutzrecht deshalb keine Anwendung.

Die Datenschutz-Grundverordnung bezieht sich außerdem nicht auf die Gemeinsame Außen- und Sicherheitspolitik (GASP) der Europäischen Union. Soweit die Mitgliedstaaten in diesem Rahmen personenbezogene Daten verarbeiten, gilt die Datenschutz-Grundverordnung dementsprechend nicht, → Art. 2 Abs. 2 Buchst. b DSGVO.

3.3.3 Bekämpfung von Straftaten durch zuständige Behörden

Die Datenschutz-Grundverordnung gilt schließlich auch dann nicht, wenn personenbezogene Daten zur Bekämpfung von Straftaten verarbeitet werden und die Verarbeitung durch die für die Bekämpfung von Straftaten zuständigen Behörden erfolgt → Art. 2 Abs. 2 Buchst. d DSGVO. Für solche Verarbeitungen gilt die Datenschutz-Richtlinie für Polizei und Strafjustiz.

Beispiel:

§ 161 Strafprozessordnung (StPO) ist eine Generalklausel im deutschen Strafverfahrensrecht, die es den Strafverfolgungsbehörden (Staatsanwaltschaft und Polizei) erlaubt, Ermittlungen zur Aufklärung und Verfolgung von Straftaten vorzunehmen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. – Hier geht es um die Ermittlung, Aufdeckung und Verfolgung von Straftaten – alles Zwecke, die in → Art. 2 Abs. 2 Buchst. d DSGVO genannt sind. Die Strafverfolgungsbehörden sind auch „zuständige Behörden". Datenverarbeitungen richten sich nach der Datenschutz-Richtlinie für Polizei und Strafjustiz und den zu ihrer Umsetzung erlassenen mitgliedstaatlichen Gesetzen. § 161 StPO ist ein Beispiel für eine solche Regelung.

Gegenbeispiel:

Bezugnehmend auf das Fallbeispiel in Abschnitt 3.3.3 nimmt Herr Ryneš eine Videoüberwachung vor, um Angriffe eines Unbekannten zu verhindern. – Die Videoüberwachung von Herrn Ryneš dient zwar der Verhütung von Angriffen eines Unbekannten. Es spricht viel dafür, dass die Verarbeitung deshalb zur „Verhütung" von Straftaten erfolgt – das ist ein Zweck, der nach → Art. 2 Abs. 2 Buchst. d DSGVO die Geltung der Datenschutz-Grundverordnung ausschließen kann. Aber: Herr Ryneš selbst ist keine „zuständige Behörde", sondern ein normaler Bürger. Seine Verarbeitung unterliegt deshalb der Datenschutz-Grundverordnung. Das gilt auch, wenn Herr Ryneš die Bildaufzeichnungen der Polizei übergibt, damit sie mögliche Straftäter verfolgen kann. Erst wenn die Polizei selbst die überlassenen Bilddaten zur Strafverfolgung verwendet (etwa im Rahmen einer Öffentlichkeitsfahndung veröffentlicht), ist ihre Verarbeitung nach → Art. 2 Abs. 2 Buchst. d DSGVO nicht nach der Datenschutz-Grundverordnung zu beurteilen.

3.4 Wo die Datenschutz-Grundverordnung gilt

Bislang wurde der sachliche Anwendungsbereich der Datenschutz-Grundverordnung behandelt. → Art. 3 DSGVO behandelt den räumlichen Anwendungsbereich, klärt also, wo die Datenschutz-Grundverordnung anzuwenden ist. Dazu gibt es insbesondere zwei wichtige Grundregeln:

Die **erste Grundregel** lautet: Soweit eine Verarbeitung personenbezogener Daten „**im Rahmen der Tätigkeiten einer Niederlassung** eines Verantwortlichen oder eines Auftragsverarbeiters **in der Union** erfolgt", gilt die Datenschutz-Grundverordnung. Dazu muss die Verarbeitung nicht in der Europäischen Union stattfinden, → Art. 3 Abs. 1 DSGVO.

Beispiel:

> Die Suchfunktion von Google wird über google.com angeboten. In einigen Mitgliedstaaten der Europäischen Union gibt es auch regionale Google-Versionen (etwa in Spanien google.es, in Deutschland google.de). Daten, die im Rahmen von Google Search erhoben werden, werden hauptsächlich von Google Inc. mit Sitz in den USA verarbeitet. Google unterhält aber in verschiedenen Mitgliedstaaten der Europäischen Union Niederlassungen, unter anderem in Spanien. Sie sollen den Verkauf von Produkten und Diensten der Onlinewerbung an Dritte und das entsprechende Marketing organisieren. – Der Europäische Gerichtshof hatte in einem spanischen Fall zu entscheiden, ob eine Verarbeitung „im Rahmen der Tätigkeiten einer Niederlassung" des Verantwortlichen Google auch dann erfolgt, wenn die Niederlassung nicht selbst personenbezogene Daten verarbeitet. Der Europäische Gerichtshof stellte fest, dass die mithilfe der Suchmaschine erfolgende Verarbeitung personenbezogener Daten vor allem dazu diene, Werbeanzeigen schalten zu können (und damit Geld zu verdienen). Wenn bei Nutzerinnen und Nutzern in Spanien spanische Werbeanzeigen geschaltet werden, erfolge deshalb die Verarbeitung personenbezogener Daten auch „im Rahmen der Tätigkeit" der spanischen Niederlassung von Google. [Europäischer Gerichtshof, Urteil vom 13. Mai 2014, C 131/12, Rn. 50 ff.]

Bereits aus der ersten Grundregel ergibt sich: Für die bayerischen Behörden und öffentlichen Stellen gilt die Datenschutz-Grundverordnung immer, wenn ihr sachlicher Anwendungsbereich eröffnet ist.

Streng genommen ist die **zweite Grundregel** für das Thema „Datenschutz bei bayerischen öffentlichen Stellen" kaum relevant. Sie wird nur der Vollständigkeit halber vorgestellt und lautet: Selbst wenn ein Verantwortlicher oder ein Auftragsverarbeiter nicht in der Europäischen Union niedergelassen ist, muss er die Datenschutz-Grundverordnung beachten, wenn er personenbezogene Daten von Menschen verarbeitet, die sich in der Europäischen Union befinden. Diese Regel gilt allerdings nur, wenn die Verarbeitung im Zusammenhang damit steht, a) betroffenen Menschen in der Europäischen Union Waren und Dienstleistungen anzubieten oder b) das Verhalten betroffener Personen in der Europäischen Union zu beobachten, soweit ihr Verhalten dort erfolgt → Art. 3 Abs. 2 DSGVO.

Beispiel:

> Ein in einem Drittland ansässiges Unternehmen unterhält eine deutschsprachige Webseite, die auf dem deutschen Markt Immobilien vermitteln soll. In diesem Zusammenhang verarbeitet das Unternehmen personenbezogene Daten der Inserentinnen und Inserenten. Die Inserate sind einen Monat lang kostenlos, danach muss dafür bezahlt werden. Zahlreiche Inserentinnen und Inserenten verlangten per E-Mail die Löschung ihrer Inserate ab diesem Zeitpunkt und gleichzeitig die Löschung der sie betreffenden personenbezogenen Daten. Das Unternehmen kam dieser Forderung nach Löschung jedoch nicht nach und stellte ihre Dienstleistungen den Betroffenen in Rechnung. Da die in Rechnung gestellten Beträge nicht bezahlt wurden, übermittelte diese Gesellschaft die personenbezogenen Daten der betroffenen Inserentinnen und Inserenten an verschiedene Inkassounternehmen. – Die Inserentinnen und Inserenten haben in dem Fall die Löschung ihrer personenbezogenen Daten verlangt und dabei einen datenschutzrechtlichen Anspruch geltend gemacht → Art. 17 Abs. 1 DSGVO. Bevor Sie jedoch einen solchen Löschanspruch überprüfen, müssen Sie klären, ob die Datenschutz-Grundverordnung überhaupt anwendbar ist. Das wäre hier zu bejahen: Das Unternehmen bietet die Dienstleistung Immobilienvermittlung Personen an, die sich in Deutschland (also in der EU) befinden. Zu diesem Zweck verarbeitet es auch personenbezogene Daten dieser Personen.

→ Art. 3 Abs. 1 und Abs. 2 DSGVO stellen also darauf ab, wo der wirtschaftliche Schwerpunkt einer Verarbeitung personenbezogener Daten liegt. Gemeinhin wird dies als **Marktortprinzip** umschrieben.

Bitte beachten Sie, dass der Anwendungsbereich nur die Frage klärt, ob die Datenschutz-Grundverordnung für einen bestimmten Sachverhalt gilt. Nicht geklärt ist damit die Rechtmäßigkeit einer Verarbeitung.

4 Datenschutzrechtliche Grundsätze

Die Datenschutz-Grundverordnung enthält einen Katalog von „Grundsätzen für die Verarbeitung personenbezogener Daten". Nach → Art. 5 Abs. 1 DSGVO sind dies:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz;
- Zweckbindung;
- Datenminimierung;
- Richtigkeit;
- Speicherbegrenzung sowie
- Integrität und Vertraulichkeit.

Vielleicht fragen Sie sich: Was ist mit so allgemein gehaltenen Grundsätzen anzufangen – und was habe ich als Bürgerin oder Bürger davon? Nun – mit den datenschutzrechtlichen Grundsätzen aus → Art. 5 Abs. 1 DSGVO allein lassen sich in aller Regel keine konkreten Fälle lösen. Dafür werden spezifische Vorschriften benötigt, solche nämlich, die in einer bestimmten Lebenssituation sagen, was zu tun oder zu unterlassen ist. Solche Vorschriften hält das Datenschutzrecht auch bereit; was Ihre Rechte betrifft, werden Sie einige davon in Abschnitt 5 näher kennenlernen.

Gleichwohl sind die datenschutzrechtlichen Grundsätze alles andere als überflüssig. Sie umschreiben wichtige Teilgehalte des in Art. 8 GRCh gewährleisteten Datenschutzgrundrechts und leisten damit einen Beitrag, diese Position für die Rechtsanwendung nutzbar zu machen. Die datenschutzrechtlichen Grundsätze bringen auch anschaulich den „Geist der Datenschutz-Grundverordnung" zum Ausdruck: Das Grundanliegen allen Datenschutzrechts liegt in erster Linie darin, die Rechte und Freiheiten natürlicher Personen zu sichern, und nicht darin, die Interessen der Verantwortlichen durchzusetzen. Schließlich geben die datenschutzrechtlichen Grundsätze Verständnisleitlinien vor, wenn bei der Anwendung von Datenschutzrecht Auslegungs- oder Entscheidungsspielräume bestehen.

Beispiel:

> Eine Behörde fragt sich bei der Anwendung von → Art. 4 Abs. 1 BayDSG, ob eine bestimmte Datenerhebung „zur Erfüllung einer ihr obliegenden Aufgabe erforderlich" ist. – Der Grundsatz der Datenminimierung (→ Art. 5 Abs. 1 Buchst. c DSGVO) fordert, dass sich die Behörde von dem verfolgten Zweck leiten lassen soll. Nicht erforderlich ist dann die Erhebung von Daten, „die man vielleicht einmal gebrauchen kann". Die Behörde wird also

> nur Daten erheben, die sie benötigt, um eine konkrete Entscheidung verantwortlich treffen zu können.

Vor diesem Hintergrund lohnt es sich, die datenschutzrechtlichen Grundsätze näher kennenzulernen. Für eilige Leserinnen und Leser sei Abschnitt 4.1 besonders hervorgehoben.

4.1 Rechtmäßigkeit

Nach → Art. 5 Abs. 1 Buchst. a DSGVO müssen personenbezogene Daten „auf rechtmäßige Weise" verarbeitet werden. Aber was heißt „auf rechtmäßige Weise"?

Nach Art. 8 Abs. 2 Satz 1 GRCh dürfen personenbezogene Daten „nur mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden." Diese grundrechtliche Vorgabe beschreibt ein datenschutzrechtliches **„Verbot mit Erlaubnisvorbehalt"**: Kann die Verarbeitung nicht auf eine legitime Verarbeitungsgrundlage gestützt werden, ist sie rechtswidrig. Das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt wird vor allem in → Art. 6 DSGVO konkretisiert. Diese Vorschrift sieht vor, dass eine Verarbeitung nur rechtmäßig ist, wenn mindestens eine Bedingung aus → Art. 6 Abs. 1 UAbs. 1 Buchst. a bis f DSGVO erfüllt ist. Diese Bedingungen werden in den nachfolgenden Abschnitten 4.1.1 bis 4.1.6 vorgestellt.

Nach Erwägungsgrund 39 DSGVO sollen auch „die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein". Daraus ist abzuleiten, dass eine Verarbeitung stets einen eindeutigen und rechtmäßigen Zweck voraussetzt. Verarbeitet ein Verantwortlicher personenbezogene Daten ohne Zweckbestimmung, ist die Verarbeitung schon deshalb rechtswidrig.

4.1.1 Einwilligung

Nach → Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO kann eine Verarbeitung rechtmäßig sein, wenn die betroffene Person ihre Einwilligung in die sie betreffende Verarbeitung erteilt hat. Was eine Einwilligung ist, erläutert → Art. 4 Nr. 11 DSGVO. Beide Vorschriften müssen also zusammen gelesen werden.

Für eine wirksame Einwilligung müssen nach → Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO und → Art. 4 Nr. 11 DSGVO zumindest die folgenden Merkmale erfüllt sein:

- unmissverständlich abgegebene Willensbekundung (→ Art. 4 Nr. 11 DSGVO);
- konkreter Zweckbezug (→ Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO);
- konkreter Verarbeitungsbezug (→ Art. 4 Nr. 11 DSGVO);

- Freiwilligkeit (→ Art. 4 Nr. 11 DSGVO);
- Informiertheit (→ Art. 4 Nr. 11 DSGVO).

Vertiefung:

> In der Literatur wird teilweise zwischen begrifflichen Merkmalen der Einwilligung und Wirksamkeitsvoraussetzungen unterschieden. Diesem etwas komplizierten Ansatz folgt der vorliegende Text nicht. Fehlt eines der fünf Merkmale, kann eine Erklärung, die als Einwilligung „daherkommt", die in → Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO angeordnete Rechtswirkung nicht entfalten.

Unmissverständlich abgegebene Willensbekundung ▪ Die Einwilligung setzt zunächst eine unmissverständlich abgegebene Willensbekundung voraus, mit der eine betroffene Person zu verstehen gibt, dass sie mit einer Verarbeitung der sie betreffenden Daten einverstanden ist. Eine solche Willensbekundung kann eine Erklärung sein. Sie kann aber auch in einer „sonstigen eindeutigen bestätigenden Handlung" der betroffenen Person bestehen, die verdeutlicht, dass sie mit der Verarbeitung einverstanden ist.

Beispiel:

> Hinter einem klar formulierten Einwilligungstext befindet sich ein sogenanntes „Opt-In"-Kästchen. Nur wenn die Nutzenden dieses Kästchen anklicken, wird eine Einwilligung unterstellt.

Gegenbeispiel:

> Die Webseite eines Anbieters enthält einen Text, wonach die Nutzenden mit der Verwendung von Cookies durch den Anbieter einverstanden sind. Darunter befindet sich ein vorangekreuztes Kästchen, das man durch Anklicken auskreuzen kann (sog. „Opt-out"). – Das Nichtauskreuzen eines vorangekreuzten Kästchens signalisiert nicht eindeutig ein Einverständnis: Die betroffene Person muss aktiv werden, wenn sie eine – ihr zunächst „untergeschobene" – Erklärung (doch) nicht abgeben möchte (näher [Europäischer Gerichtshof, Urteil vom 1. Oktober 2019, C-673/17, Rn. 61 ff.]).

Konkreter Zweckbezug und konkreter Verarbeitungsbezug ▪ Eine Einwilligung muss sich weiterhin auf einen bestimmten Zweck beziehen. Damit sind die Verarbeitungszwecke im Sinne von → Art. 5 Abs. 1 Buchst. b DSGVO gemeint. Mehrere Verarbeitungszwecke können erfasst sein, wenn für alle Verarbeitungszwecke eine Einwilligung gegeben wird (vgl. Erwägungsgrund 32 DSGVO). Außerdem müssen die Verarbeitungen absehbar sein, für welche die Einwilligung als Rechtsgrundlage herangezogen werden soll. Eine „Blanko-Einwilligung" sieht die Datenschutz-Grundverordnung nicht vor.

Beispiel:

> Die betroffene Person willigt darin ein, dass der Verantwortliche ihre personenbezogenen Daten zu den Zwecken der Direktwerbung und der Bonitätsbeurteilung verarbeitet. – Die Einwilligung bezieht sich damit auf zwei Zwecke, die beide hinreichend bestimmt sein müssen.

Gegenbeispiel:

> Die betroffene Person soll darin einwilligen, dass der Verantwortliche X. „die personenbezogenen Daten an seine Vertragspartnerinnen und Vertragspartner weitergeben kann". Wer dies ist, bleibt ungewiss. – Hier soll die betroffene Person eine Pauschaleinwilligung erteilen: Geklärt ist nur, dass die Daten weitergegeben werden sollen. Es wird aber nicht näher erläutert, welche Vertragspartnerinnen und Vertragspartner der X. hat sowie zu welchem Zweck die Daten weitergegeben und gegebenenfalls weiterverarbeitet werden sollen. Insbesondere erfährt die betroffene Person auch nicht, ob ihre Einwilligung Datenweitergaben ins Nicht-EU-Ausland rechtfertigen soll. Die Einwilligung gegenüber X. wäre unwirksam. Steht keine andere Rechtsgrundlage zur Verfügung, sind die Verarbeitungen bei X. rechtswidrig. Von einer schlampig formulierten Einwilligung hat X. also nichts.

Tipp:

> Eine Einwilligungserklärung muss den Verarbeitungszweck immer aussagekräftig beschreiben. Schauen Sie sich Einwilligungen, die Ihnen vorgelegt werden, genau an. Die vom Gesetz verlangte Transparenz dürfen Sie auch einfordern!

Freiwilligkeit ▪ Eine wirksame Einwilligung muss zudem freiwillig erteilt sein. Erwägungsgrund 42 DSGVO führt dazu am Ende aus: „Es sollte nur dann davon ausgegangen werden, dass sie [die betroffene Person] ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden."

Beispiel:

> Eine Behörde will auf ihrer Webseite alle Beschäftigten vorstellen. Dazu sollen jeweils Portraitfoto, Name, Telefonnummer und die dienstliche E-Mail-Adresse veröffentlicht werden. Der Dienstherr verlangt von seinen Beschäftigten, dass sie in diese Veröffentlichung einwilligen. – Die Freiwilligkeit einer solchen „Einwilligung" ist zumindest zweifelhaft. Erfahrungsgemäß machen viele Beschäftigte mit, weil sie nicht als „Spielverderberinnen" oder „Spielverderber" dastehen wollen. Das erzeugt bei den kritischeren Kolleginnen und Kollegen einen gewissen Gruppendruck, den Vorgesetzte mitunter auf mehr oder minder subtile Art verstärken. Aus Furcht vor Nachteilen willigen dann auch einige ein, die das „eigentlich" gar nicht wollen.

Vertiefung:

Das Problem der Freiwilligkeit von Einwilligungen im Beschäftigungsverhältnis wird beispielsweise in → § 26 Abs. 2 BDSG berücksichtigt. Diese Vorschrift gilt zwar nicht für die bayerischen öffentlichen Stellen. Sie gibt aber wertvolle Hinweise, wann Freiwilligkeit auch in solchen Konstellationen angenommen werden kann.

Nach § 26 Abs. 2 BDSG ist „bei der Beurteilung der Freiwilligkeit insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen."

Nach § 26 Abs. 2 Satz 2 BDSG kann die Einwilligung einer beschäftigten Person insbesondere dann freiwillig sein, wenn sich für sie ein rechtlicher oder wirtschaftlicher Vorteil ergibt. Ähnliches gilt für Verarbeitungen, bei denen der Arbeitgeber und die beschäftigte Person gleichgelagerte Interessen verfolgen. Verallgemeinert gesprochen liegt ein Indiz für die fehlende Freiwilligkeit einer Einwilligungserklärung vor, wenn zwischen dem Verantwortlichen und der betroffenen Person ein klares Ungleichgewicht besteht (Erwägungsgrund 43 DGSVO).

Tipp:

Ihr Arbeitgeber oder Dienstherr verlangt Ihnen eine Einwilligung für eine Verarbeitung ab, mit der Sie eigentlich nicht einverstanden sind – und Sie trauen sich nicht, „nein" zu sagen, weil Sie Nachteile befürchten? Dann können Sie sich vertraulich an die behördliche Datenschutzbeauftragte, den betrieblichen Datenschutzbeauftragten oder an die zuständige Personalvertretung wenden (Betriebsrat/Personalrat). Insbesondere wenn Sie dort kein Gehör finden, können Sie auch den Rat der zuständigen Datenschutz-Aufsichtsbehörde suchen (siehe Abschnitt 6.4).

Im öffentlichen Bereich bestehen oftmals Ansprüche auf Genehmigung, auf Gewährung bestimmter Leistungen oder auf Zugang zu öffentlichen Einrichtungen. Solche Ansprüche sind häufig gesetzlich näher ausgestaltet. Die zuständige Stelle darf die Leistung, den Zugang oder die Teilnahme grundsätzlich nicht von einer Einwilligung in Datenumgänge abhängig machen, die über den Zweck der Verfahrensdurchführung hinausreichen.

Beispiel:

Eine Bauaufsichtsbehörde verlangt von Bauwerberinnen und Bauwerbern neben dem Bauantrag eine Einwilligung in Datenverarbeitungen, die auch Übermittlungen ins Nicht-EU-Ausland einschließen. – Hinsichtlich eines genehmigungsfähigen Bauantrags besteht ein Genehmigungsanspruch. Die Durchführung des Genehmigungsverfahrens darf nicht von der Einwilligung abhängig gemacht werden, die nicht freiwillig erteilt und deshalb nicht wirksam wäre.

Gegenbeispiel:

> Ein kommunales Theater hat in seinen Geschäftsbedingungen festgelegt, dass Karten an der Vorverkaufs- oder Abendkasse gegen Barzahlung erworben werden können; wird der Kauf auf Rechnung gewünscht, werden die Karten nach Überweisung des Rechnungsbetrags zugesandt. In diesem Fall müssen Erwerberinnen oder Erwerber Name und Anschrift angeben und in die Verarbeitung für die Abwicklung des Kartenkaufs einwilligen. – Für die Freiwilligkeit der Einwilligung spricht, dass die Option des Barkaufs angeboten wird. „Preis" der Anonymität ist hier der Gang zur entsprechenden Kasse.

Informiertheit ▪ Die Einwilligung muss schließlich informiert erteilt sein. Die betroffene Person muss wissen, dass und in welchem Umfang sie eine Rechtsgrundlage für eine Verarbeitung des Verantwortlichen schafft. Sie muss dazu mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen.

Nachweisbarkeit ▪ Im Übrigen sieht → Art. 7 Abs. 1 DSGVO vor, dass der Verantwortliche nachweisen können muss, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. → Art. 7 Abs. 1 DSGVO gestaltet die Rechenschaftspflicht nach → Art. 5 Abs. 2 DSGVO in Bezug auf die Einwilligung näher aus.

Eine naheliegende Möglichkeit, die Rechenschaftspflicht des → Art. 7 Abs. 1 DSGVO zu erfüllen, besteht darin, dass der Verantwortliche bei den betroffenen Personen schriftliche Einwilligungserklärungen einholt. Wenn die betroffene Person schriftlich einwilligen soll, muss der Verantwortliche auch → Art. 7 Abs. 2 DSGVO beachten. Wird die datenschutzrechtliche Einwilligung mit anderen Erklärungen verbunden, muss sie deutlich von diesen anderen Erklärungen zu unterscheiden sein. Zudem muss „das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" erfolgen, → Art. 7 Abs. 2 Satz 1 DSGVO.

Beispiel:

> Die datenschutzrechtliche Einwilligungserklärung darf nicht in umfangreichen Allgemeinen Geschäftsbedingungen „versteckt" werden.

Nach → Art. 7 Abs. 2 Satz 2 DSGVO dürfen Teile der Einwilligungserklärung nicht gegen die Datenschutz-Grundverordnung verstoßen – sonst sind sie nicht verbindlich.

Beispiel:

> Die registrierten Nutzenden einer Webseite werden gebeten, sich damit einverstanden zu erklären, dass der Anbieter zu Werbezwecken einen Cookie auf dem jeweiligen IT-System der Nutzenden ablegt. Nähere Informationen hierzu werden gegeben. Außerdem sollen

> sie zustimmen, dass Nutzerdaten an Vertragspartnerinnen oder Vertragspartner des Anbieters weitergeleitet werden. Die Vertragspartner und der Weiterleitungszweck werden nicht beschrieben. – Der erste Teil der erbetenen Erklärung betrifft eine Verarbeitung des Anbieters. Sie gibt Informationen über dessen Identität, Mittel und Zwecke der Verarbeitung. Ganz anders ist der zweite Teil der Einwilligung zu bewerten: Die Nutzenden erhalten weder eine aussagekräftige Information über die Datenempfänger noch Kenntnis über die Verarbeitungszwecke. Während der erste Teil der Einwilligung wirksam ist, ist der zweite Teil unwirksam. Das heißt: Bei der Weiterleitung der Daten an Vertragspartnerinnen oder Vertragspartner kann sich der verantwortliche Anbieter nicht auf eine wirksame Einwilligung stützen. Gibt es keine andere Rechtsgrundlage für die Datenweiterleitung, ist sie rechtswidrig.

Widerruflichkeit ▪ Die betroffene Person kann ihre Einwilligung jederzeit **frei widerrufen**. Dann entfällt die Einwilligung als Rechtsgrundlage für die Verarbeitung. Nach → Art. 7 Abs. 3 Satz 2 DSGVO entfällt die Rechtfertigungswirkung der Einwilligung ab dem Zeitpunkt des erfolgten Widerrufs. Davor erfolgte Verarbeitungen sind also noch von der Einwilligung gedeckt. Der Verantwortliche hat die betroffene Person über das Recht auf Widerruf und seine Wirkungen zu unterrichten, bevor sie die Einwilligung erteilt.

4.1.2 Verarbeitung zur Durchführung eines Vertrags mit der betroffenen Person

Schließt ein Verantwortlicher mit einer betroffenen Person einen **Vertrag** ab, so verfolgen beide gleichgerichtete Interessen: Der eine Vertragspartner will beispielsweise eine Dienstleistung anbieten, der andere möchte sie in Anspruch nehmen. Das erklärte Interesse beider Vertragspartner ist dann darauf gerichtet, dass eine ganz bestimmte Dienstleistung erbracht (und meistens auch irgendwie entlohnt) wird. Erfolgt der Vertragsschluss unter fairen Bedingungen, hat er in Bezug auf die betroffene Person gewisse Ähnlichkeiten mit der Einwilligung: In beiden Fällen steht ein Willensakt der betroffenen Person im Raum. Außerdem können in einem Vertrag Vorkehrungen zum Schutz der Rechte und Freiheiten des Empfängers einer Dienstleistung getroffen werden.

Vor diesem Hintergrund sieht → Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO als zweiten möglichen Rechtfertigungsgrund einer Verarbeitung die Erforderlichkeit zur Durchführung eines Vertrags des Verantwortlichen mit der betroffenen Person vor.

Beispiel:

> Eine Kundin bestellt bei einem städtischen Theater Eintrittskarten, die sie nach Hause gesandt haben will. – Um seine Vertragspflicht (Zusendung der Eintrittskarten) erfüllen zu

können, benötigt das Theater Angaben, wohin die Eintrittskarten geliefert werden sollen, damit sie die Kundin erreichen. Meistens wird Lieferort die Wohnadresse der Kundin sein – oder ein anderer Ort, zu dem die Kundin einen Bezug hat. Die Wohnadresse ist zweifelsohne ein personenbezogenes Datum im Sinne des → Art. 4 Nr. 1 DSGVO. Die Verarbeitung dieser Angabe ist erforderlich, damit das Theater seine Vertragspflicht erfüllen kann.

Zulässig kann eine Verarbeitung auch sein, wenn sie zur Durchführung von **„vorvertraglichen Maßnahmen“** erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. „Auf Anfrage der betroffenen Person“ bedeutet, dass die Initiative zum geplanten Vertragsabschluss von der betroffenen Person gekommen sein muss.

Beispiel:

Eine Kundin erteilt der Stadtwerke A. GmbH eine Abbuchungsermächtigung. – Um die Abbuchungen durchführen zu können, muss die Stadtwerke A. GmbH Kontodaten der Kundin verarbeiten. Auch diese Verarbeitung kann im Grundsatz auf → Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO gestützt werden.

Gegenbeispiel:

Um ihre Kundschaft stärker an sich zu binden, schreiben die Stadtwerke A. GmbH ihre Kundschaft direkt an und bieten auf die jeweilige Person zugeschnittene Angebote für den öffentlichen Personennahverkehr an. – Hier geht die Initiative von der Stadtwerke A. GmbH aus. Sie kann ihre Verarbeitung nicht auf → Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO stützen. Das bedeutet aber nicht zwangsläufig, dass das Anschreiben datenschutzrechtswidrig ist. In Betracht kommt insbesondere eine Verarbeitung auf Grundlage einer Einwilligung nach → Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO.

4.1.3 Verarbeitung zur Erfüllung rechtlicher Verpflichtungen

→ Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO sieht einen Verarbeitungsgrund für Fälle vor, in denen die Verarbeitung „zur Erfüllung einer rechtlichen Verpflichtung erforderlich [ist], der der Verantwortliche unterliegt.“ Erfasst sind nur Verpflichtungen, die in Rechtsvorschriften des Unionsrechts oder des nationalen Rechts angeordnet sind (insbesondere in Parlamentsgesetzen, Rechtsverordnungen oder Satzungen sowie in Verordnungen des Unionsrechts). Eine Rechtsvorschrift aus dem Nicht-EU-Ausland genügt nicht, wie → Art. 6 Abs. 3 UAbs.1 DSGVO zeigt.

Beispiel:

Eine Staatsanwaltschaft erhebt gegen einen Beamten Anklage bei einem Strafgericht. Nach § 49 Beamtenstatusgesetz (BeamtStG) ist die Anklageschrift mit Begründung an den Dienstvorgesetzten zu übersenden. Diese Übermittlungspflicht soll es dem Dienstherrn ermöglichen zu prüfen, ob auch disziplinarische Schritte gegen den Beamten angezeigt sind.

Verarbeitungen nach → Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO sind besonders bei Unternehmen häufig, weil diese – etwa im Steuerrecht – zahlreichen gesetzlichen Mitteilungspflichten ausgesetzt sind. Sie kommen – wie → Art. 6 Abs. 3 UAbs. 1 DSGVO erkennen lässt – jedoch auch bei öffentlichen Stellen vor (siehe das Beispiel). Hier ist die Abgrenzung zu → Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO fließend.

4.1.4 Schutz lebenswichtiger Interessen

Eine Verarbeitung personenbezogener Daten kann auf → Art. 6 Abs.1 UAbs. 1 Buchst. d DSGVO gestützt werden, wenn sie erforderlich ist, um lebenswichtige Interessen von Menschen zu schützen. „Lebenswichtige Interessen" schließen jedenfalls das Leben und die körperliche Unversehrtheit mit ein, wie sich aus Erwägungsgrund 112 DSGVO ergibt. Nach Erwägungsgrund 46 DSGVO soll der Schutz lebenswichtiger Interessen nur dann Verarbeitungsgrundlage sein, wenn eine andere offensichtlich nicht in Betracht kommt. Umstritten ist, ob → Art. 6 Abs. 1 UAbs. 1 Buchst. d DSGVO auch nicht anzuwenden ist, wenn der Verantwortliche die Einwilligung der betroffenen Person einholen kann.

Bayerische öffentliche Stellen können in diesem Zusammenhang regelmäßig auf gesetzliche Verarbeitungsbefugnisse (→ Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO) zurückgreifen.

Beispiel:

> Erwägungsgrund 46 nennt als Anwendungsfall von → Art. 6 Abs. 1 UAbs. 1 Buchst. d DSGVO die Überwachung von Epidemien. Die insofern relevanten Datenumgänge sind in §§ 6 ff. Infektionsschutzgesetz sowie Art. 30 ff. Gesundheitsdienst- und Verbraucherschutzgesetz umfassend geregelt, siehe dazu auch Bayerischer Landesbeauftragter für den Datenschutz, 27. Tätigkeitsbericht 2016, Nr. 7.4.2 (im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Tätigkeitsberichte").

4.1.5 Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe

Die Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe setzt zunächst eine besondere Rechtsgrundlage voraus → Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 DSGVO. Diese Vorschrift „trägt" die Verarbeitung also nicht allein, es kommt vielmehr darauf an, dass der Unionsgesetzgeber oder ein nationaler Gesetzgeber die Verarbeitung im Einzelnen regelt, → Art. 6 Abs. 3 UAbs. 1 DSGVO.

Die nach → Art. 6 Abs. 3 UAbs. 1 DSGVO zu schaffende besondere Rechtsgrundlage wird üblicherweise als **Befugnisnorm** bezeichnet. Solche Vorschriften sind daran zu erkennen, dass sie einer öffentlichen Stelle unter konkreten Voraussetzungen be-

stimmte Verarbeitungen personenbezogener Daten erlauben. Bayerische öffentliche Stellen verarbeiten personenbezogene Daten in der Regel aufgrund von spezifischen bundes- oder landesrechtlichen Befugnisnormen.

Beispiel:

Art. 85 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) gibt bayerischen öffentlichen Schulen verschiedene Befugnisse, personenbezogene Daten über ihre Schülerinnen und Schüler, die Erziehungsberechtigten (Eltern), Lehrkräfte und sonstigen Beschäftigten zu verarbeiten. Detailregelungen zu dem – datenschutzrechtlich besonders sensiblen – Umgang mit Schülerunterlagen finden sich in §§ 37 ff. Bayerische Schulordnung. Siehe dazu ausführlich Bayerischer Landesbeauftragter für den Datenschutz, 27. Tätigkeitsbericht 2016, Nr. 10.1, im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Tätigkeitsberichte".

Gibt es fachrechtliche Verarbeitungsbefugnisse wie aus Art. 85 BayEUG, dann gelten sie und nicht das allgemeine Datenschutzrecht. Diesen Vorrang des speziellen Datenschutzrechts vor dem allgemeinen Datenschutz stellt → Art. 1 Abs. 5 BayDSG ausdrücklich klar.

Fehlt es allerdings an einer fachspezifischen Befugnis, können bayerische öffentliche Stellen Verarbeitungen je nach Lage des Einzelfalls auch auf die **allgemeinen Rechtsgrundlagen** in → Art. 4 BayDSG und → Art. 5 BayDSG stützen.

Beispiel:

Zu den öffentlichen Aufgaben einer Gemeinde gehören auch gewisse Repräsentationsveranstaltungen. Will der Oberbürgermeister einer kreisfreien Stadt Neubürger zu einem Empfang einladen, kann die dazu erforderliche Verarbeitung von → Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO, → Art. 4 Abs. 1 BayDSG gedeckt sein, siehe näher Bayerischer Landesbeauftragter für den Datenschutz, Einladungen zu Veranstaltungen durch bayerische Kommunen, Aktuelle Kurz-Information 10, unter Nr. 1 a), im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen".

In der Regel sind es Behörden und andere öffentliche Stellen, die personenbezogene Daten zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe verarbeiten. Seltener werden Private mit der Erfüllung öffentlicher Aufgaben betraut. Dann gelten sie als öffentliche Stellen, → Art. 1 Abs. 4 BayDSG.

Ach, übrigens:

Auch öffentliche Stellen des Bundes können eine allgemeine Befugnisnorm (Generalklausel) heranziehen, wenn eine fachspezifische Verarbeitungsgrundlage fehlt, → § 3 BDSG.

4.1.6 Verarbeitung auf Grundlage eines berechtigten Verarbeitungsinteresses

→ Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO erlaubt die Verarbeitung auf der Grundlage einer Abwägung von berechtigten Verarbeitungsinteressen des Verantwortlichen mit entgegenstehenden Belangen der betroffenen Person.

Keine Anwendung auf Behörden ▪ Soweit Behörden personenbezogene Daten in Erfüllung ihrer Aufgaben verarbeiten, ist → Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO nicht anwendbar, → Art. 6 Abs. 1 UAbs. 2 DSGVO.

Vertiefung

Warum hat eigentlich der Gesetzgeber eine solche Regelung getroffen? Wäre es nicht viel einfacher, wenn auch Behörden → Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO anwenden dürften?

Einfacher wäre das möglicherweise schon. Aber: Das nach→ Art. 6 Abs. 3 UAbs. 1 Buchst. b DSGVO weiterhin vorgesehene bereichsspezifische Datenschutzrecht des öffentlichen Sektors gleicht die Verarbeitungsinteressen der Behörden und die Belange der betroffenen Personen meist sehr viel genauer aus, als dies mit einer „Abwägungs-Generalklausel" wie → Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO möglich ist. Behörden verfügen – anders als etwa Unternehmen – über vielfältige Möglichkeiten, Rechtsverhältnisse zu Bürgerinnen und Bürgern zu regeln. Dies erfordert (auch) engere Vorgaben bei der Zulässigkeit von Verarbeitungen.

Für öffentliche Stellen, die keine Behörden sind, gilt der Anwendungsausschluss in → Art. 6 Abs. 1 UAbs. 2 DSGVO allerdings nicht. Sie können auch auf Grundlage eines berechtigten Interesses personenbezogene Daten verarbeiten.

Beispiel:

Sieht man – jedenfalls im Einklang mit Art. 1 Bayerisches Verwaltungsverfahrensgesetz – eine gemeindliche Tourismus-GmbH nicht als Behörde an, so kann diese auf Grundlage von → Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO personenbezogene Daten zu Zwecken der Werbung verarbeiten. Sie hat dabei selbstverständlich die allgemein geltenden Regeln über den lauteren Wettbewerb und über den Datenschutz bei der elektronischen Kommunikation einzuhalten. Das gilt insbesondere für § 7 Gesetz gegen den unlauteren Wettbewerb, der sich gegen bestimmte unerwünschte werbliche Kommunikation richtet. Künftig wird voraussichtlich eine europäische ePrivacy-Verordnung zu beachten sein.

Prüfung von Art. 6 Abs. 1 UAbs. 1Buchst. f DSGVO ▪ Die Rechtsgrundlage des Art. 6 Abs. 1 UAbs. 1 Buchst. f lässt sich in drei Schritten prüfen:

Erstens muss **ein berechtigtes Interesse** des Verantwortlichen oder eines Dritten vorliegen, das die Verarbeitung grundsätzlich legitimieren kann. Das berechtigte Interesse ist weit zu verstehen und kann zum Beispiel ideell oder wirtschaftlich begründet sein.

Beispiel:

> Nach dem letzten Satz in Erwägungsgrund 47 DSGVO kann der Zweck der Direktwerbung (also die individuelle Ansprache einer Person zu Werbezwecken) ein berechtigtes Interesse darstellen.

Zweitens muss die Verarbeitung für die Verwirklichung des berechtigten Interesses **erforderlich** sein. Nach der Rechtsprechung müssen sich die „Ausnahmen und Einschränkungen" des Rechts auf Datenschutz auf das „absolut Notwendige" beschränken.

Rückblick:

> In dem bereits in Abschnitt 3.3.4 vorgestellten Fall Ryneš erfasst die Videoüberwachung auch den öffentlichen Verkehrsraum neben dem Privatgrundstück des Herrn Ryneš. Insoweit wäre genauer zu prüfen, ob die Videoüberwachung mit den Grundstücksgrenzen auch die Grenzen des „absolut Notwendigen" überschritten hat. Das hängt von den Gegebenheiten ab: Kann ein erfolgreicher Angriff auf das Haus von Herrn Ryneš auch vom öffentlichen Verkehrsraum verübt werden, könnte die Videoüberwachung auch insoweit erforderlich sein. Falls ein solcher Angriff ausscheidet, müsste Herr Ryneš die Videoüberwachung strikt auf sein Grundstück begrenzen.

Drittens muss der Verantwortliche die **jeweiligen einander gegenüberstehenden Rechte und Interessen untereinander abwägen**. Hierbei sind die konkreten Umstände des Einzelfalls zu berücksichtigen.

Vertiefung:

> Ein Vorzug von → Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO liegt darin, dass die Vorschrift flexibel auf unterschiedliche Verarbeitungssituationen angewendet werden kann. Die Kehrseite dieser Flexibilität liegt in dem Risiko der Rechtsunsicherheit, das mit der Abwägung verbunden ist.
>
> So ist es eine Wertungsfrage, wann das wirtschaftliche Interesse eines Verantwortlichen an einer effektiven Werbung das Interesse der betroffenen Person überwiegen kann, von einer Verarbeitung zu Werbezwecken verschont zu bleiben. Derjenige, der die Bewertung vornimmt, verfolgt eines dieser Interessen.
>
> Bei diesem Beispiel gibt zwar → Art. 21 Abs. 2, Abs. 3 DSGVO wenigstens noch einen normativen Anhaltspunkt: Wenn es danach ein Recht auf Widerspruch gegen Direktwerbung gibt, dann müssen einerseits die Direktwerbung und die Verarbeitung zum Zweck

der Direktwerbung bis zu einem gewissen Grad zulässig sein. Andererseits bewirkt der Widerspruch gegen die Verarbeitung für Zwecke der Direktwerbung nach → Art. 21 Abs. 3 DSGVO, dass eine solche Verarbeitung unzulässig wird. Daraus folgt: Direktwerbung verfolgt im Grundsatz ein berechtigtes Interesse, das aber im Verhältnis zu gegenläufigen Interessen betroffener Personen kein allzu großes Gewicht hat.

4.2 Verarbeitung nach Treu und Glauben

Das Grundrecht auf Datenschutz aus Art. 8 Abs. 1 GRCh verlangt eine Verarbeitung nach Treu und Glauben. → Art. 5 Abs. 1 Buchst. a DSGVO konkretisiert diese grundrechtliche Vorgabe.

Ach, übrigens:

Im Vertragsrecht zielen vergleichbare Vorgaben auf einen redlichen Geschäftsverkehr. Zugeordnet werden etwa Verbote widersprüchlichen Verhaltens oder sittenwidriger Täuschungshandlungen. Auch im deutschen Recht gibt es mit § 242 Bürgerliches Gesetzbuch eine solche Regelung: „Der Schuldner ist verpflichtet, die Leistung so zu bewirken, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern."

Der Grundsatz der Verarbeitung nach Treu und Glauben – die englische Fassung spricht von „fairness" – soll gewährleisten, dass Verantwortliche bei ihrer Verarbeitung personenbezogener Daten die Interessen von betroffenen Personen angemessen mitberücksichtigen. Bei einer der Datenschutz-Grundverordnung entsprechenden Verarbeitung darf der Verantwortliche betroffene Personen nicht „über den Tisch ziehen".

Unter welchen Voraussetzungen Verarbeitungen dem Grundsatz von Treu und Glauben entsprechen, haben der Unionsgesetzgeber wie auch die nationalen Gesetzgeber in zahlreichen Regelungen, insbesondere über die Rechtmäßigkeit von Verarbeitungen und über die dabei herzustellende Transparenz festgelegt. Der Grundsatz der Verarbeitung nach Treu und Glauben wird durch solche Ausgestaltungen verwirklicht. Er ist nicht als ein Mittel gedacht, rechtliche Bewertungen aus einem moralischen Blickwinkel zu korrigieren. Die Bedeutung des Grundsatzes bei der Rechtsanwendung ist derzeit noch nicht abschließend geklärt.

Vertiefung:

Dem Grundsatz der Verarbeitung nach Treu und Glauben lässt sich möglicherweise ein Verbot zuordnen, überflüssige Einwilligungen einzuholen: Bei dieser – im öffentlichen Sektor immer wieder anzutreffenden – Praxis fordert eine Behörde, die personenbezogene Daten von einer betroffenen Person verarbeiten möchte, eine Einwilligung, obwohl

eine Befugnisnorm zur Verfügung steht. Die Einwilligung soll als Rechtsgrundlage „herhalten", weil die Behörde die Voraussetzungen der Befugnisnorm nicht prüfen möchte oder weil sie – falls sich die Voraussetzungen im Nachhinein als nicht erfüllt erweisen sollten – „auf der sicheren Seite" sein möchte. Manchmal „sprengt" auch der Umfang des Datensatzes den Rahmen, den die Befugnisnorm zieht. Wie auch immer: Bei der betroffenen Person entsteht der Eindruck, sie habe kraft ihrer Einwilligung und der damit verbundenen Widerrufsmöglichkeit alles in der Hand. Tatsächlich hat der Gesetzgeber aber schon alles geregelt – und meist gibt die betroffene Person mehr von ihren Rechten preis als vorgesehen. Kann das fair sein?

Auch der – etwa in → Art. 4 Abs. 2 Satz 1 BayDSG angeordnete – Vorrang der Direkterhebung lässt sich möglicherweise dem Grundsatz der Verarbeitung nach Treu und Glauben zuordnen. Der Vorrang der Direkterhebung ist ein aus dem früheren nationalen Datenschutzrecht stammendes Gebot. Kann der Verantwortliche an die personenbezogenen Daten einer betroffenen Person zum einen dadurch gelangen, dass er sie bei dieser erhebt (die sogenannte Direkterhebung), zum andern aber auch dadurch, dass er Dritte in Anspruch nimmt, so soll die Erhebung bei der betroffenen Person Vorrang haben – und zwar auch dann, wenn dies umständlicher ist oder die betroffene Person vorzeitig davon erfährt, dass sich der Verantwortliche mit ihr befasst.

Der Grundsatz der Verarbeitung nach Treu und Glauben gilt auch bei der Erfüllung von Aufgaben, die im öffentlichen Interesse liegen.

Beispiel:

Eine Person erzielt Einkünfte aus selbständiger Tätigkeit. Sie gibt dies auch gegenüber der Steuerbehörde an. Diese Steuerbehörde gibt die Informationen über die erzielten Einkünfte an die Krankenkasse der betroffenen Person weiter. Die Krankenkasse berechnet daraufhin die Beitragspflicht neu und fordert von der betroffenen Person Nachzahlungen. Das relevante nationale Recht (im Fall: das rumänische) erlaubt es den Finanzbehörden (nur), den Krankenkassen personenbezogene Daten zu übermitteln, um es ihnen zu ermöglichen, die Versicherteneigenschaft der betroffenen Personen festzustellen. Diese Daten betreffen die Personalien (Vor- und Zuname, persönliche Identifikationsnummer, Anschrift), schließen aber keine Informationen über die erzielten Einkünfte ein.

Auch diesen Fall hatte der Europäische Gerichtshof zu beurteilen (Urteil vom 1. Oktober 2015, C-201/14). Er kam zu dem Schluss, unabhängig vom Vorliegen einer Rechtsgrundlage sei die Verarbeitung rechtswidrig gewesen, weil sie gegen den Grundsatz von Treu und Glauben verstoßen habe. Denn Art. 6 Richtlinie 95/46/EG (jetzt → Art. 5 DSGVO) verpflichte eine Verwaltungsbehörde dazu, die betroffenen Personen zu unterrichten, bevor ihre personenbezogenen Daten an eine weitere Behörde weitergeleitet werden, um von dieser Daten empfangenden Behörde für eigene Zwecke verarbeitet zu werden. Nur wenn die Weitergabe gesetzlich ausdrücklich vorgesehen sei, hätte die betroffene Person mit

> einer solchen Weiterleitung rechnen müssen. Dann wäre eine Information möglicherweise nicht geboten gewesen.

4.3 Transparenz

Die vorangegangenen Ausführungen zum Grundsatz der Verarbeitung nach Treu und Glauben zeigen: Bei einer fairen Verarbeitung muss vorhersehbar sein, was mit den personenbezogenen Daten geschieht. Zu diesem Zweck muss der Verantwortliche die betroffene Person insbesondere über eine für sie unerwartete Verarbeitung informieren. Das verlangt (auch) der neue Grundsatz der Transparenz, der ebenfalls durch → Art. 5 Abs. 1 Buchst. a DSGVO gewährleistet wird. Erwägungsgrund 39 DSGVO führt zum Grundsatz der Transparenz aus:

> „Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten leicht zugänglich und verständlich und in klarer und verständlicher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können."

→ Art. 5 Abs. 1 Buchst. a DSGVO fasst den Grundsatz der transparenten Verarbeitung dahin knapp zusammen, dass sie **in einer für den Betroffenen nachvollziehbaren Weise** erfolgt.

Der Grundsatz der Transparenz wird insbesondere im Kapitel zu den Betroffenenrechten durch die → Art. 12 bis 15 DSGVO konkretisiert. Er setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung für die betroffenen Personen „leicht zugänglich und verständlich und in klarer Sprache abgefasst sind", wie es Erwägungsgrund 39 DSGVO hervorhebt.

4.4 Zweckbindung

Zentral für das neue Datenschutzrecht ist der Grundsatz der Zweckbindung, den → Art. 5 Abs.1 Buchst. b DSGVO regelt. Bereits dem in Abschnitt 2 vorgestellten

Volkszählungsurteil des Bundesverfassungsgerichts zufolge bedeutet Zweckbindung, dass eine Stelle personenbezogene Daten (zunächst nur) für den Zweck verarbeiten darf, zu dem sie die Daten rechtmäßig erhoben hat. Eine Weiterverarbeitung zu anderen Zwecken bedarf dagegen einer neuen Rechtfertigung – und damit zumeist auch einer eigenen Rechtsgrundlage. Diese verfassungsrechtlichen Vorgaben sind auf die Handlungssituation von Behörden angelegt, die an Gesetz und Recht, in diesem Rahmen insbesondere an ihre Verarbeitungsbefugnisse (vgl. → Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO), gebunden sind. Bei Unternehmen und Vereinen ist ein solches Verständnis von Zweckbindung nicht ganz passend, weil diese ihre Verarbeitungen nicht auf Verarbeitungsbefugnisse, sondern eher (etwa) auf → Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO stützen werden.

Deshalb unterscheidet sich der Grundsatz der Zweckbindung nach → Art. 5 Abs. 1 Buchst. b DSGVO – jedenfalls bei Verarbeitungen im privaten Interesse – etwas vom althergebrachten deutschen Zweckbindungsprinzip. Danach wird die Verarbeitung zu einem anderen Zweck grundsätzlich verboten, wenn sie **mit dem ursprünglichen Erhebungszweck unvereinbar** ist. Dieses Zweckbindungsprinzip wird in → Art. 6 Abs. 4 DSGVO konkretisiert. Verarbeitungen, die einen anderen Zweck als den ursprünglichen Verarbeitungszweck verfolgen, sind nur unter den Voraussetzungen dieser Vorschrift möglich.

→ Art. 6 Abs. 4 DSGVO sieht drei zulässige Varianten der Verarbeitung zu anderen Zwecken als dem ursprünglichen Verarbeitungszweck vor:

- erstens eine Zweckänderung auf Grundlage einer Einwilligung. Da diese bereits im Abschnitt 4.1.1 vorgestellt worden ist, wird sie hier nicht näher behandelt.
- Zweitens dürfen Verantwortliche im öffentlichen Interesse personenbezogene Daten zu anderen Zwecken verarbeiten, wenn dies in einer Rechtsvorschrift erlaubt wird. Diese Rechtsvorschrift muss dem Schutz von Zielen des → Art. 23 Abs. 1 DSGVO dienen und dem Verhältnismäßigkeitsgrundsatz genügen (dazu Abschnitt 4.4.1).
- Drittens ist eine zweckändernde Verarbeitung zulässig, wenn sie mit dem Ursprungszweck vereinbar ist. Um eine sachgerechte Überprüfung der Vereinbarkeit sicherzustellen, sieht → Art. 6 Abs. 4 Buchst. a bis e DSGVO Kriterien vor, die der Verantwortliche zu berücksichtigen hat (dazu Abschnitt 4.4.2).

Aus dem Zweckbindungsgrundsatz folgt auch, dass der Verantwortliche vor der ersten Verarbeitung **die zulässigen Verarbeitungszwecke eindeutig festlegen** muss. Diese Zwecke müssen legitim sein. Werden Daten zu anderen Zwecken weiterverarbeitet, müssen die neuen Zwecke „verträglich“ mit dem ursprünglichen Zweck sein.

4.4.1 Zweckbindung bei Verarbeitungen im öffentlichen Interesse

Verarbeitungen im öffentlichen Interesse zu anderen Zwecken als dem Erhebungszweck sind erlaubt → Art. 6 Abs. 4 DSGVO, wenn sie auf einer Einwilligung der betroffenen Person beruhen (Fall von → Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO) oder „auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in → Art. 23 Abs. 1 DSGVO genannten Ziele darstellt" (Fälle von → Art. 6 Abs. 1 UAbs. 1 Buchst. c und e DSGVO). Mit anderen Worten: Von der Konstellation „Einwilligung" abgesehen, darf der nationale Gesetzgeber (auch) Regelungen für zweckändernde Verarbeitungen schaffen. Das hat er getan: So widmen sich im Bundesrecht §§ 23 ff. BDSG und in §§ 67c ff. SGB X diesem Thema, im bayerischen Recht etwa → Art. 6 BayDSG und im Bereich der Datenschutz-Richtlinie für Polizei und Strafjustiz → Art. 29 BayDSG.

4.4.2 Zweckbindung bei sonstigen Verarbeitungen

Im Übrigen ist eine zweckändernde Verarbeitung nach → Art. 6 Abs. 4 DSGVO zulässig, wenn eine Prüfung ergibt, dass sie mit dem ursprünglichen Verarbeitungszweck vereinbar ist. Diese Vereinbarkeitsprüfung ist – jedenfalls im Grundsatz – wohl nur für Verarbeitungen gedacht, die nicht im öffentlichen Interesse erfolgen. Andernfalls würde der nationalrechtliche Vorbehalt des Gesetzes unterlaufen, den → Art. 6 Abs. 1 UAbs. 1 Buchst. c und e, Abs. 3 UAbs. 1 DSGVO anerkennt.

Nach Art. 6 Abs. 4 DSGVO müssen Verantwortliche im Falle einer zweckändernden Verarbeitung zunächst prüfen, ob es **Verbindungen zwischen dem Ursprungszweck und dem beabsichtigten Weiterverarbeitungszweck** gibt (→ Art. 6 Abs. 4 Buchst. a DSGVO).

Beispiel:

> Insbesondere eine Archivierung oder die wissenschaftliche Forschung können Zwecke sein, die vereinbar mit dem Ursprungszweck sind (→ Art. 5 Abs. 1 Buchst. b DSGVO am Ende).

Relevant ist ferner der **Zusammenhang, in dem die Daten erhoben wurden**. Das gilt auch hinsichtlich des Verhältnisses zwischen betroffenen Personen und Verantwortlichen (→ Art. 6 Abs. 4 Buchst. b DSGVO).

Beispiel:

> Üblicherweise kann der Verantwortliche im Vergleich zu anderen Verantwortlichen in größerem Umfang personenbezogene Daten zu Werbezwecken verarbeiten, wenn er bereits in einem gefestigten Vertragsverhältnis mit der betroffenen Person steht.

Die **Art der personenbezogenen Daten** ist zu berücksichtigen, weil die Datenschutz-Grundverordnung davon ausgeht, dass es Datenkategorien gibt, die ihrem Wesen nach risikoträchtig für die betroffenen Personen sind (→ Art. 6 Abs. 4 Buchst. c DSGVO).

Beispiel:

> Eine Verarbeitung von Gesundheitsdaten ist immer nur unter den zusätzlichen Voraussetzungen des → Art. 9 Abs. 2 bis 4 DSGVO zulässig!

Hat eine beabsichtigte Verarbeitung schwerwiegende negative **Folgen für die betroffene Person** (→ Art. 6 Abs. 4 Buchst. d DSGVO), spricht dies zunächst gegen eine zweckändernde Verarbeitung. Sie dürfte nur dann zulässig sein, wenn triftige Gründe für die Weiterverarbeitung sprechen.

Beispiel:

> Die Stadtwerke A. GmbH hat einen Unfall aufgenommen, der auf dem Betriebsgelände stattgefunden hat – ein Beschäftigter hatte mit seinem Wagen den LKW eines Lieferanten gerammt. Nun will der Lieferant Name und Adressdaten des Schädigers haben. – Die Weitergabe der Daten hätte für den Beschäftigten erhebliche Nachteile, weil er mit Schadensersatzforderungen rechnen muss. Andererseits ist es legitim, wenn eine geschädigte Person von dem Schädiger einen Ausgleich für den erlittenen Schaden verlangt.

Mit zu berücksichtigen ist schließlich, ob **geeignete Garantien** existieren, die bei einer Weiterverarbeitung der Daten einen angemessenen Schutz der betroffenen Person sicherstellen. Als Beispiel nennt → Art. 6 Abs. 4 Buchst. e DSGVO ausdrücklich die Verschlüsselung.

Der **Prüfkatalog** in → Art. 6 Abs. 4 DSGVO ist **nicht abschließend** gemeint. Das ergibt sich aus den Worten „unter anderem". Es kann also sein, dass der Verantwortliche weitere Kriterien hinzuziehen muss, wenn ein Einzelfall Besonderheiten aufweist.

Tipp:

> Nach → Art. 13 Abs. 3 und → Art. 14 Abs. 4 DSGVO hat der Verantwortliche Sie darüber zu informieren, wenn er beabsichtigt, über Sie erhobene Daten für andere Zwecke zu verarbeiten. Diese Mitteilung erfolgt, damit Sie die Rechtmäßigkeit der beabsichtigten Übermittlung überprüfen können. Falls Sie die Zulässigkeit der Datenübermittlung bezweifeln, sollten Sie das gegenüber dem Verantwortlichen unbedingt deutlich machen. Dabei ist es wichtig, dass Sie gegenüber dem Verantwortlichen möglichst die Gründe für Ihre Zweifel mitteilen. Ansonsten kann er Ihren Einwand nicht sachgerecht berücksichtigen.

Beispiel:

In dem zuletzt geschilderten Beispielsfall dürfte die Übermittlung an den Geschädigten des Unfalls auf dem Betriebsgelände im Grundsatz zulässig sein, da sie sich auf den Namen und die Adressdaten eines mutmaßlichen Schädigers beschränkt.

4.5 Datenminimierung

Nach → Art. 5 Abs. 1 Buchst. c DSGVO dürfen Verantwortliche personenbezogene Daten nur verarbeiten, soweit dies für einen legitimen Verarbeitungszweck angemessen und erheblich ist. Die Verarbeitung muss dabei auf das für die Zwecke der Verarbeitung erforderliche Maß beschränkt sein. Insbesondere sollen personenbezogene Daten nur solange eine Identifizierung einer natürlichen Person ermöglichen, wie es für den Verarbeitungszweck erforderlich ist.

Vertiefung:

Die Prüfung der Erforderlichkeit einer Verarbeitung – etwa im Rahmen eines entsprechenden Merkmals von Verarbeitungsbefugnissen – setzt regelmäßig (unter anderem) den Grundsatz der Datenminimierung um. Der Grundsatz der Datenminimierung richtet sich auch gegen Vorratsdatenspeicherungen (dazu bereits Abschnitt 2.1).

Der Grundsatz der Datenminimierung verpflichtet die Verantwortlichen, bei der Datenverarbeitung mit personenbezogenen Daten möglichst sparsam umzugehen, insbesondere gerade so viele Daten zu erheben, wie für eine Verarbeitung benötigt werden.

Den Bayerischen Landesbeauftragten für den Datenschutz erreichen viele Anfragen von Bürgerinnen und Bürgern, die sich auf Antragsformulare der öffentlichen Verwaltung beziehen. Im Grundsatz ist es nicht zu beanstanden, dass eine Behörde Daten erhebt, um einen Antrag bearbeiten zu können. Nicht selten werden allerdings neben erforderlichen Angaben auch Daten abgefragt, die für die Sachbearbeitung nicht notwendig sind. In solchen Fällen wirkt die Datenschutz-Aufsichtsbehörde regelmäßig darauf hin, die Formulare im Sinne der Datenminimierung zu überarbeiten und den Umfang ihrer Fragen zu verringern.

Vertiefung:

Das „rechte Maß“ bei der Datenerhebung ist im öffentlichen Sektor wesentlich durch das Fachrecht bestimmt. Vorschriften, die Voraussetzungen für eine Genehmigung oder für eine Geldleistung festlegen, regeln, auf welchen Sachverhalt es ankommt. Da die Behörde in einem Verwaltungsverfahren den Sachverhalt aufklären muss, bestimmen diese Vor-

schriften auch darüber, welche Daten erhoben werden müssen. Mit anderen Worten: Verlangt eine Behörde personenbezogene Daten, auf die es im Verwaltungsverfahren nicht ankommt, liegt ein Verstoß gegen den Grundsatz der Datenminimierung nahe.

Big Data-Anwendungen mit personenbezogenen Daten stehen typischerweise in einem erheblichen Spannungsverhältnis zum Grundsatz der Datenminimierung.

4.6 Richtigkeit und Aktualität

Personenbezogene Daten müssen sachlich richtig und aktuell sein. Konkretisiert wird der Grundsatz der Richtigkeit und Aktualität durch den Berichtigungsanspruch nach → Art. 16 DSGVO (siehe Abschnitt 5.5). Letztlich verpflichtet → Art. 5 Abs. 1 Buchst. d DSGVO den Verantwortlichen auf eine Qualitätssicherung hinsichtlich der von ihm verarbeiteten personenbezogenen Daten.

Beispiel:

Im nicht-öffentlichen Bereich bedienen große Wirtschaftsauskunfteien – das sind private Unternehmen, die Informationen sammeln und auswerten – ihre Kundinnen und Kunden mit Einschätzungen der Kreditwürdigkeit („Bonität") von möglichen Vertragspartnern. Dazu sammeln sie einschlägige Daten und werten sie unter diesem Gesichtspunkt aus. In Bezug auf Verbraucherinnen und Verbraucher werden insbesondere Schuldnerdaten aus den Schuldnerverzeichnissen der Amtsgerichte genutzt.

Erkundigt sich nun ein Unternehmen nach der Kreditwürdigkeit einer natürlichen Person, informiert die Auskunftei diese betroffene Person über die gespeicherten Daten und bittet um Auskunft, ob die Informationen korrekt und aktuell sind. Diese Vorgehensweise führte jedenfalls früher zu zahlreichen Beschwerden bei den Datenschutz-Aufsichtsbehörden. Im Grundsatz ist aber gerade diese Vorgehensweise datenschutzkonform, weil mit dem Anschreiben zugleich eine Information über die geplante Weitergabe von Schuldnerdaten erfolgt. Zugleich kann die Anfrage bei der betroffenen Person einen Beitrag liefern, dass die später an die Kundschaft der Auskunfteien weitergegebenen Daten richtig und aktuell sind.

4.7 Speicherbegrenzung

Der Verantwortliche darf personenbezogene Daten grundsätzlich nur so lange speichern, wie dies für den Verarbeitungszweck erforderlich ist. Dies legt → Art. 5 Abs. 1 Buchst. e DSGVO fest. Erwägungsgrund 39 DSGVO weist darauf hin, dass Verant-

wortliche Fristen für die Löschung oder zumindest regelmäßige Überprüfungen vorsehen sollen, um sicherzustellen, dass Daten nicht länger als nötig gespeichert werden.

Beispiel:

Für den Adresshandel sah § 35 Abs. 2 Nr. 4 BDSG-alt vor, dass der Verantwortliche spätestens jeweils am Ende des vierten Kalenderjahres beginnend mit der erstmaligen Speicherung von Daten zu prüfen hat, ob eine länger währende Speicherung noch erforderlich ist. Hintergrund dieser Regelung war wohl die Erfahrung, dass statistisch gesehen die Aktualität von Adressdaten innerhalb eines Zeitraums von drei bis vier Jahren erheblich abnimmt.

Vertiefung:

Im öffentlichen Sektor sind Aufbewahrungsfristen häufig im Fachrecht geregelt, so beispielsweise für Schülerunterlagen in § 40 Bayerische Schulordnung. Ist die Aufbewahrungsfrist abgelaufen, werden Unterlagen dem zuständigen Archiv angeboten. Das Archiv entscheidet, ob es die Unterlagen übernimmt. In diesem Fall ersetzt die Abgabe an das Archiv die Löschung. Kommt es nicht zu einer Übernahme, sind die Unterlagen zu vernichten (und nicht in einem Keller oder auf einem Speicher dauerhaft zu „parken").

4.8 Integrität und Vertraulichkeit

Integrität und Vertraulichkeit der Verarbeitung sind mit der Datenschutz-Grundverordnung neu hinzugekommene Datenschutz-Grundsätze, → Art. 5 Abs. 1 Buchst. f DSGVO. Sie werden in → Art. 24 ff. DSGVO, insbesondere durch → Art. 25 DSGVO und → Art. 32 DSGVO näher ausgeformt.

Beispiel:

Untechnisch gesprochen sind E-Mails wie Postkarten: Auf dem Weg von der Absenderin oder dem Absender zur Empfängerin oder zum Empfänger könnte sie jeder Betreiber lesen, der sie weiterleitet. Vertrauliche Informationen sollten deshalb nicht unverschlüsselt weitergegeben werden. Eine E-Mail wird nicht direkt zwischen Versenderin oder Versender und Empfängerin oder Empfänger auf dem kürzesten Weg ausgetauscht, sondern nimmt möglicherweise viele Umwege. Diese Umwege erhöhen die Gefahr, dass auch Unbefugte auf Nachrichten zugreifen können.

→ Art. 32 Abs. 1 DSGVO schreibt deshalb vor, dass der Verantwortliche verpflichtet ist, einen angemessenen Vertraulichkeitsschutz zu gewährleisten. Für ein „angemessenes Schutzniveau" kann es je nach Sensibilität der verarbeiteten Daten geboten sein, dass der Verantwortliche die ihm anvertrauten personenbezogenen Daten verschlüsselt. Das gilt

gerade auch im Rahmen der elektronischen Kommunikation: Öffentliche Stellen dürfen auf elektronischem Weg sensible Daten nicht unverschlüsselt versenden.

Ach, übrigens:

Nach dem Bayerischen E-Government-Gesetz hat im Grundsatz jeder das Recht, elektronisch über das Internet mit den bayerischen Behörden zu kommunizieren und ihre Dienste in Anspruch zu nehmen. Ab Januar 2020 haben die bayerischen Behörden dazu jeweils ein geeignetes Verschlüsselungsverfahren bereitzustellen, um die Vertraulichkeit der Kommunikation zwischen öffentlichen Stellen und Bürgerinnen und Bürgern sicherzustellen.

4.9 Rechenschaftspflicht

Neu ist auch die in → Art. 5 Abs. 2 DSGVO geregelte Rechenschaftspflicht des Verantwortlichen. Sie besagt, dass der Verantwortliche die Einhaltung der Datenschutz-Grundsätze im Zweifel auch nachweisen können muss. Um Rechenschaft über seine Verarbeitung personenbezogener Daten ablegen zu können, muss der Verantwortliche Dokumentationspflichten erfüllen, wie sie ihm etwa im Zusammenhang mit dem Verzeichnis der Verarbeitungstätigkeiten (→ Art. 30 Abs. 1, 3 DSGVO), der Datenschutz-Folgenabschätzung (→ Art. 35 Abs. 1, 7 DSGVO) oder der Meldepflicht bei Datenpannen (→ Art. 33 Abs. 3 DSGVO) aufgegeben sind.

4.10 Besonderer Schutz sensibler Daten

→ Art. 9 DSGVO regelt die Verarbeitung besonderer Kategorien personenbezogener Daten („sensible Daten"). Erwägungsgrund 51 DSGVO begründet den besonderen Schutz dieser Datenkategorien damit, sie seien „ihrem Wesen nach" besonders sensibel; im Zusammenhang mit ihrer Verarbeitung könnten besondere Risiken für die Grundrechte und Grundfreiheiten entstehen.

Beispiel:

Erfährt ein Arbeitgeber von der Erkrankung eines Bewerbers, kann dies erhebliche Nachteile beim Bewerbungsverfahren haben, selbst wenn die Erkrankung sich auf die Leistungsfähigkeit des Bewerbers nicht auswirkt.

Deshalb verbietet → Art. 9 Abs. 1 DSGVO im Grundsatz die Verarbeitung sensibler Daten. Die Risiken einer Verarbeitung personenbezogener Daten hängen allerdings oft vom **Verwendungszusammenhang** ab. Zudem gibt es triftige Gründe, weshalb sensible Daten verarbeitet werden müssen, obwohl das für betroffene Personen riskant ist.

Beispiel:

> Ohne Verarbeitung personenbezogener Gesundheitsdaten könnte ein Arzt oder eine Klinik Patienten nicht erfolgreich behandeln.

Das grundsätzliche Verbot in → Art. 9 Abs. 1 DSGVO wird deshalb in → Art. 9 Abs. 2 DSGVO unter bestimmten Voraussetzungen durchbrochen. Für Gesundheitsdaten, genetische und biometrische Daten gelten nach → Art. 9 Abs. 3 und 4 DSGVO noch zusätzliche Sonderregelungen.

Gerade bei der Verarbeitung sensibler Daten sollte der Grundsatz der Datenminimierung (siehe Abschnitt 4.5) besondere Beachtung finden.

Tipp:

> Falls Sie von einer Behörde aufgefordert werden, Kontoauszüge vorzulegen, haben Sie auf der **Ausgabenseite** grundsätzlich die Möglichkeit, diejenigen Überweisungen zu schwärzen, die Rückschlüsse auf besondere Kategorien personenbezogener Daten geben. Sie dürfen aber nur den **Verwendungszweck** sowie die **Empfängerin oder** den **Empfänger** der Überweisung schwärzen, **nicht** deren **Höhe**.

Personenbezogene **Daten über strafgerichtliche Verurteilungen sowie über durchgeführte Ermittlungsverfahren** gehören für die betroffenen Personen ebenfalls zu den Daten, deren Verarbeitung mit besonderen Risiken verbunden ist.

Beispiel:

> Gerät ein Mensch in den Ruf, bestimmte Straftaten begangen zu haben, kann dies für ihn in seinem gesellschaftlichen Umfeld zu massiven Nachteilen führen.

Gleichwohl ordnet die Datenschutz-Grundverordnung nicht wie bei sensiblen Daten nach → Art. 9 DSGVO ein grundsätzliches Verarbeitungsverbot an. → Art. 10 DSGVO sieht vielmehr einen besonderen **organisatorisch-verfahrensrechtlichen Schutz** vor, indem er die Verarbeitung grundsätzlich unter behördliche Aufsicht stellt.

Vertiefung:

> Das in → Art. 10 Satz 2 DSGVO angesprochene „Register der strafrechtlichen Verurteilungen" ist in Deutschland das Bundeszentralregister. Zu Datenschutzfragen im Zusammenhang mit diesem Register sowie weiteren Registern im Justizbereich siehe Hinweise auf https://www.datenschutz-bayern.de in der Rubrik „Themengebiete – Justiz – Wichtige Register im Bereich der Justiz (Strafrecht)".

Die Zulässigkeit der Verarbeitung sensibler Daten nach → Art. 9 und → Art. 10 DSGVO richtet sich im Übrigen nach den allgemeinen Grundsätzen, insbesondere muss eine Rechtfertigung im Sinne von → Art. 6 Abs. 1 DSGVO möglich sein.

Vertiefung:

In Deutschland gibt es neben diesen von der Datenschutz-Grundverordnung vorgesehenen Begrifflichkeiten für sensible Daten noch den Begriff der **Sozialdaten**. Hiervon spricht man, wenn bestimmte Stellen, insbesondere die Sozialleistungsträger (etwa ein Sozialamt, Jobcenter, Jugendamt) personenbezogene Daten (wie Name, Adresse, Geburtsdatum) im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch verarbeiten (siehe Begriffsbestimmung in § 67 Abs. 2 SGB X). Auch wenn diese Stellen Daten im Sinne von → Art. 9 Abs. 1 DSGVO verarbeiten, liegen Sozialdaten vor. Für die Verarbeitung von Sozialdaten gelten spezielle datenschutzrechtliche Vorschriften in den einzelnen Büchern des Sozialgesetzbuches.

5 Rechte der betroffenen Personen – Ihre Datenschutzrechte

Mit den Rechten der betroffenen Person schafft die Datenschutz-Grundverordnung ein Gegengewicht zu den Rechten des Verantwortlichen, personenbezogene Daten zu verarbeiten. Ist der Verantwortliche eine öffentliche Stelle, gewährleisten die Betroffenenrechte, dass Bürgerinnen und Bürger nicht zu Objekten hoheitlicher Datenverarbeitungen werden, sondern dabei ein – im Einzelfall durchaus gewichtiges – Wort mitzureden haben. Die Datenschutz-Grundverordnung gestaltet die Betroffenenrechte in ihrem Kapitel III näher aus. Was Verarbeitungen im öffentlichen Sektor betrifft, sind Betroffenenrechte häufig auch Gegenstand der jeweiligen Fachgesetze. Bei den nachfolgenden Erläuterungen stehen die Bestimmungen der Datenschutz-Grundverordnung im Vordergrund, fachrechtliche Bestimmungen werden nur beispielhaft beim Auskunftsrecht erläutert.

An der Spitze der Regelungen in Kapitel III DSGVO steht mit → Art. 12 DSGVO eine Vorschrift, die einige Regelungsfragen – „vor die Klammer gezogen" – einheitlich beantwortet.

Eine „Schlüsselfunktion" kommt den in → Art. 13 und 14 DSGVO niedergelegten Informationspflichten zu. Diese Pflichten des Verantwortlichen bezwecken, dass eine betroffene Person von nahezu jeder Verarbeitung erfährt, die ihre personenbezogenen Daten betrifft. Sind die geforderten Informationen ordnungsgemäß bereitgestellt, verschafft deren Kenntnisnahme jedenfalls ein ungefähres Bild vom Umfang der jeweiligen Verarbeitung, von den mit ihr verbundenen Risiken sowie von den Handlungsmöglichkeiten, welche die betroffene Person in Bezug auf diese Verarbeitung hat.

In → Art. 15 DSGVO und den nachfolgenden Vorschriften regelt die Datenschutz-Grundverordnung sodann einzelne Betroffenenrechte. Diese sind im Gesetzestext jeweils unschwer an der Wendung „Die betroffene Person hat das Recht, […]" zu erkennen. Zu unterscheiden sind insbesondere

- das Auskunftsrecht der betroffenen Person (→ Art. 15 Abs. 1 DSGVO, siehe Abschnitt 5.4.) mit dem in → Art. 15 Abs. 3 DSGVO geregelten Recht auf Kopie der eigenen personenbezogenen Daten (siehe Abschnitt 5.4.1);
- das Recht auf Berichtigung (→ Art. 16 DSGVO, siehe Abschnitt 5.5);

- das Recht auf Löschung („Recht auf Vergessenwerden", → Art. 17 Abs. 1 DSGVO, siehe Abschnitt 5.6);
- das Recht auf Einschränkung der Verarbeitung (→ Art. 18 Abs. 1 DSGVO, siehe Abschnitt 5.7);
- das Recht auf Datenübertragbarkeit (→ Art. 20 Abs. 1 und 2 DSGVO, siehe Abschnitt 5.8);
- das Recht, einer Verarbeitung zu widersprechen (→ Art. 21 Abs. 1, 2 und 6 DSGVO, siehe Abschnitt 5.9) und
- das Recht auf Abwehr automatisierter Entscheidungen im Einzelfall (→ Art. 22 Abs. 1 DSGVO, siehe Abschnitt 5.10).

Vertiefung:

Die Betroffenenrechte sind im unionsrechtlichen Grundrecht auf Datenschutz verankert. Sie gehören zu dessen wesentlichen Gewährleistungsgehalten. Die Rechte auf Auskunft und auf Berichtigung sind in Art. 8 Abs. 2 Satz 2 GRCh ausdrücklich angesprochen: „Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken."

Warum nur diese beiden Betroffenenrechte besonders hervorgehoben werden, ist nicht ganz klar, hat doch etwa das Recht auf Löschung für die Verwirklichung des Datenschutzgrundrechts einen durchaus vergleichbar hohen Stellenwert.

Mit dieser Erweiterung hätte Art. 8 Abs. 2 Satz 2 GRCh an das 1981 geschlossene erste europäische Datenschutzübereinkommen des Europarats (Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981, im Internet abrufbar auf https://www.coe.int/de in der Rubrik „Mehr – Vertragsbüro – Gesamtverzeichnis" unter Nr. 108) anknüpfen können, das – ebenfalls in seinem Art. 8 – sinngemäß Rechte der betroffenen Personen auf Auskunft, Berichtigung und Löschung vorsah. Der Anspruch auf Löschung lässt sich jedoch – wie auch die weiteren Betroffenenrechte – als Konkretisierung der allgemeinen, bereits in Art. 8 Abs. 2 Satz 1 GRCh niedergelegten Schutzaussage verstehen.

Die Frage nach der Zuordnung einzelner Betroffenenrechte zu Grundrechtspositionen ist keine rein akademische Frage. Je zuverlässiger ihre Verankerung im Datenschutzgrundrecht begründet werden kann, desto schwieriger ist es für den Gesetzgeber – und zwar sowohl auf der europäischen als auch der nationalen Ebene –, einmal ausformulierte Betroffenenrechte zum Nachteil ihrer Träger „weiterzuentwickeln" oder in Ausnahmetatbeständen zu beschränken.

5.1 Pflichten des Verantwortlichen im Zusammenhang mit Betroffenenrechten

Betroffenenrechte haben und Betroffenenrechte durchsetzen – das ist nicht dasselbe. Viele, meist größere Verwaltungen haben längst feste Routinen entwickelt, wie sie einen Auskunftsantrag, einen Antrag auf Löschung personenbezogener Daten oder einen Widerspruch effizient und bürgerfreundlich bearbeiten. Andere müssen entsprechende Erfahrungen erst noch gewinnen.

Die Erfüllung von Betroffenenrechten ist kein Gnadenakt, sondern eine gesetzliche Verpflichtung, welcher der Verantwortliche nachzukommen hat. → Art. 12 Abs. 1 DSGVO verpflichtet den Verantwortlichen zu „geeigneten Maßnahmen", um der betroffenen Person alle datenschutzrelevanten Informationen und Mitteilungen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln." Gemäß → Art. 12 Abs. 2 DSGVO hat der Verantwortliche den betroffenen Personen die Ausübung ihrer Rechte zu erleichtern.

Wenn Sie den Eindruck haben, mit Ihrem Anliegen kein Gehör zu finden, oder wenn unerwartet Hindernisse auftauchen, sollten Sie zunächst drei Dinge wissen:

- Die Betroffenenrechte richten sich gegen den Verantwortlichen.
- Im Zusammenhang mit der Ausübung von Betroffenenrechten dürfen regelmäßig Entgelte nicht erhoben werden.
- Ihr Antrag ist unverzüglich, grundsätzlich innerhalb eines Monats zu bearbeiten.

Verantwortlicher als Adressat ▪ Verpflichteter der datenschutzrechtlichen Betroffenenrechte ist der in Abschnitt 1.4.3 bereits vorgestellte **Verantwortliche**. Falls Sie also etwa Auskunft über Ihre Daten erhalten oder eine Berichtigung oder Löschung von personenbezogenen Daten erreichen wollen, müssen Sie Ihr Betroffenenrecht beim Verantwortlichen geltend machen. Die Kontaktdaten sollten in den Datenschutzhinweisen des Verantwortlichen enthalten sein; unterhält der Verantwortliche eine Internetpräsenz, sind die Datenschutzhinweise meist – wie das Impressum – von der Startseite aus erreichbar.

Tipp:

> Gerade bei größeren Verwaltungen ist es sinnvoll, das Anschreiben an die verantwortliche Stelle zu Händen der oder des **behördlichen Datenschutzbeauftragten** zu richten. Diese Person ist nach der Datenschutz-Grundverordnung nicht nur für die behördeninterne Beratung und Überwachung im Bereich des Datenschutzrechts zuständig. Sie fungiert auch als Ansprechpartnerin oder Ansprechpartner, wenn es um die Geltendmachung der Be-

troffenenrechte geht. Die oder der behördliche Datenschutzbeauftragte ist in der Ausübung dieser Funktion weisungsfrei und – nach bayerischem Datenschutzrecht – überdies ausdrücklich zur Verschwiegenheit verpflichtet, → Art. 12 Abs. 2 BayDSG. Sie oder er ist meist eine Beschäftigte oder ein Beschäftigter des Verantwortlichen, welche oder welcher die örtlichen Verhältnisse und die handelnden Personen kennt und bei der Bearbeitung Ihres Antrags im Bedarfsfall die nötigen Hilfestellungen geben kann.

Unentgeltlichkeit ▪ Wenn Sie ein Betroffenenrecht geltend machen, ist die Reaktion des Verantwortlichen nach Maßgabe von → Art. 12 Abs. 5 Satz 1 DSGVO unentgeltlich. Bei öffentlichen Stellen bedeutet dies: Beantragen Sie etwa nach → Art. 15 DSGVO eine Auskunft oder eine Datenkopie, begehren Sie eine Berichtigung oder eine Löschung (→ Art. 16, 17 DSGVO), so darf die öffentliche Stelle keine Gebühr (für die Amtshandlung) erheben. Auch wenn sie Ihnen eine umfangreiche erste Kopie zur Verfügung stellt, darf sie keine Auslagen (Kopierkosten) fordern.

Ach, übrigens:

Für weitere Kopien gilt der Grundsatz der Unentgeltlichkeit nicht (vgl. → Art. 15 Abs. 3 Satz 2 DSGVO).

Eine Ausnahme vom Grundsatz der Unentgeltlichkeit bezieht sich auf offenkundig unbegründete oder exzessive Anträge von betroffenen Personen. Die in → Art. 12 Abs. 5 Satz 2 DSGVO vorgesehene Einschränkung beruht auf dem Gedanken des Rechtsmissbrauchs.

Beispiel:

Eine betroffene Person stellt beim Verantwortlichen in kurzen Zeitabständen gleichartige Auskunftsanträge über sämtliche personenbezogene Daten, die über sie verarbeitet werden, obwohl sich zwischendurch ersichtlich nichts Neues ergeben haben kann. Aus dem begleitenden Schriftverkehr wird deutlich, dass es der betroffenen Person in erster Linie darum geht, die Ressourcen des Verantwortlichen intensiv in Anspruch zu nehmen. – Die Annahme eines „exzessiven" Antrags ist vertretbar.

Gegenbeispiel:

Eine betroffene Person stellt beim Verantwortlichen wiederholt Auskunftsanträge. Sie hat Gründe zu der Annahme, dass ein Dritter dem Verantwortlichen immer wieder potenziell nachteilige Informationen zuspielt.

Verantwortliche sollten die Ausnahme von der Unentgeltlichkeit in → Art. 12 Abs. 5 Satz 2 DSGVO zurückhaltend anwenden. Bei einem offenkundig unbegründeten oder exzessiven Antrag kann der Verantwortliche zwischen dem Verlangen eines Entgelts und der Weigerung wählen, tätig zu werden. Im ersten Fall muss der Verantwortliche der betroffenen Person zunächst mitteilen, dass er ein Entgelt erheben will

und wie hoch dieses voraussichtlich ausfallen wird. Die betroffene Person soll so die Möglichkeit erhalten, ihren Antrag zurückzunehmen, um unerwünschte finanzielle Folgen zu vermeiden.

5.2 Informationspflichten des Verantwortlichen

Ein effektiver Schutz der Persönlichkeitsrechte setzt voraus, dass Sie von Verarbeitungen erfahren. Sie müssen sich vergewissern können, ob Ihre personenbezogenen Daten rechtmäßig verarbeitet werden und die Verarbeitung auch sonst fehlerfrei ist. Dazu müssen Sie insbesondere in Erfahrung bringen können, wer von Ihnen welche Daten mit welcher Zweckbestimmung verarbeitet und an welche Empfänger diese Daten gegebenenfalls gelangen können. Das Gesetz sieht hier im Wesentlichen zwei Instrumente vor: die Informationspflichten des Verantwortlichen, die in → Art. 13 und 14 DSGVO geregelt sind, sowie ein Auskunftsrecht in → Art. 15 DSGVO (siehe Abschnitt 5.4).

Die Informationspflichten muss der Verantwortliche erfüllen, ohne dass Sie sich mit einem entsprechenden Begehren an ihn wenden. Umgekehrt steht es Ihnen frei, ob sie die angebotenen Informationen zur Kenntnis nehmen oder darauf verzichten.

Tipp:

Manche Verantwortliche verfassen Merkblätter mit Datenschutzhinweisen, die sie betroffenen Personen zur Unterschrift vorlegen. Die betroffene Person soll dann bestätigen, dass sie die Datenschutzhinweise gelesen hat. Eine solche Vorgehensweise ist nicht unproblematisch. Das Gesetz sieht weder eine Pflicht zur Kenntnisnahme von Informationen nach → Art. 13 und 14 DSGVO vor noch eine Pflicht, die Kenntnisnahme durch Unterschrift zu dokumentieren. Noch problematischer wäre es, wenn eine öffentliche Stelle eine Verwaltungsdienstleistung von der Unterzeichnung der Datenschutzhinweise abhängig macht.

Vertiefung:

Die → Art. 13 bis 15 DSGVO konkretisieren zunächst die Grundsätze einer fairen Verarbeitung sowie der Transparenz (→ Art. 5 Abs. 1 Buchst. a DSGVO). Letztlich können die Informationsrechte aber zur Verwirklichung aller Datenschutzgrundsätze beitragen. Die Informationsrechte können jedoch auch etwa den Gebrauch des Rechts auf Berichtigung vorbereiten helfen. Dann stehen sie im Dienst des Grundsatzes der Richtigkeit (→ Art. 5 Abs. 1 Buchst. d DSGVO).

Informationspflicht nach Art. 13 DSGVO ▪ Beschafft sich der Verantwortliche personenbezogene Daten bei Ihnen als der betroffenen Person (**Direkterhebung bei der betroffenen Person**), hat er Sie nach → Art. 13 DSGVO zu informieren.

Beispiel:

> Ein Elternpaar beantragt Kindergeld. Bevor die Kindergeldbehörde das Kindergeld an das Elternpaar auszahlt, müssen die Eltern ein Formular mit Informationen über sich und das Kind ausfüllen.

→ Art. 13 Abs. 1 und 2 DSGVO enthalten die **Informationen, die der Verantwortliche der betroffenen Person zur Verfügung stellen muss**. Dazu gehören Angaben zum Verantwortlichen, zu den Verarbeitungszwecken, zu den legitimen Grundlagen der Verarbeitung, zu möglichen Datenempfängern und zu einem möglichen Datentransfer an Stellen außerhalb der Europäischen Union. → Art. 13 Abs. 2 DSGVO enthält daneben auch Informationen zu den konkreten Betroffenenrechten.

Muss der Verantwortliche bei jeder Datenerhebung ein Informationsblatt über die beabsichtigte Verarbeitung personenbezogener Daten aushändigen? Die Antwort lautet: nein. Jedenfalls dann, wenn die betroffene Person alle relevanten Informationen bereits kennt, entfällt die Informationspflicht (→ Art. 14 Abs. 4 DSGVO).

Beispiel:

> Die Kindergeldbehörde hat im vorgenannten Beispiel noch eine Nachfrage. Da sie die betroffenen Eltern schon zuvor informiert hat, muss die Behörde nach → Art. 13 Abs. 4 DSGVO nicht noch einmal informieren. Die Nacherhebung von personenbezogenen Daten gehört zum behördlichen Alltag, auch wenn Online-Formulare verstärkt Ausfüllhilfen enthalten.

Ansonsten fallen oft Alltagssituationen unter → Art. 13 Abs. 4 DSGVO.

Beispiel:

> Ein öffentlicher Verkehrsbetrieb lässt in der U-Bahn Fahrscheine kontrollieren. Die für diese Datenerhebung relevanten Informationen liegen für jede Großstadtbewohnerin und jeden Großstadtbewohner auf der Hand. Eine individuelle Datenschutzbelehrung durch das Kontrollpersonal ist entbehrlich. Allerdings sollten mit den Beförderungsbedingungen entsprechende Datenschutzhinweise verbunden sein.

Wenn der Verantwortliche nicht davon ausgehen darf, dass die betroffene Person über die Informationen nach → Art. 13 Abs. 1 und 2 DSGVO verfügt, hat er diese Informationen der betroffenen Person zur Verfügung zu stellen.

Allerdings darf man sich das nicht so vorstellen, dass der Verantwortliche bei jeder Beschaffung von personenbezogenen Daten bei der betroffenen Person immer sämtliche Informationen mitteilen muss. Die Informationspflicht nach → Art. 13 DSGVO soll die betroffenen Personen befähigen, eine sie betreffende beabsichtigte Verarbeitung zu beurteilen. Sie soll hingegen nicht die betroffenen Personen mit überflüssigen, sie nicht interessierenden Informationen überfluten.

Vor diesem Hintergrund hat ein Verantwortlicher stets die Frage zu klären, wie umfangreich er die betroffene Person unterrichten muss. Muss er sämtliche Informationen mitteilen oder genügt es, wenn er der betroffenen Person einige Grundinformationen gibt und im Übrigen eine ausführliche Information vorhält, die er bei Bedarf zur Verfügung stellt?

Die Antwort lautet: In der Regel genügen gestaffelte Datenschutzhinweise. Das gilt sogar, wenn der Verantwortliche sensible Daten verarbeitet. Wenn der Verantwortliche allerdings davon ausgehen muss, dass eine bestimmte Verarbeitung die betroffene Person überraschen kann, muss er über sie ausführlich informieren. Bei einer zweckändernden Verarbeitung ist (auch) über alle Verarbeitungszwecke zu informieren, die von dem ursprünglichen Erhebungszweck abweichen.

Beispiel:

> Eine Krankenkasse erhebt im Rahmen eines Preisausschreibens personenbezogene Daten. Will sie diese personenbezogenen Daten nicht nur zur Durchführung des Preisausschreibens, sondern auch zu Werbezwecken verwenden, muss sie die betroffene Person darauf hinweisen.

In einem solchen Fall genügt es nicht, wenn die Krankenkasse einen solchen Hinweis in Internet-Datenschutzhinweisen „versteckt". Da die zweckändernde Verarbeitung betroffene Personen besonders häufig überraschen kann, wird sie in → Art. 13 Abs. 3 DSGVO ausdrücklich angesprochen.

Informationspflicht nach Art. 14 DSGVO ▪ Während → Art. 13 DSGVO die Situation regelt, in der ein Verantwortlicher personenbezogene Daten bei der betroffenen Person erhebt, normiert → Art. 14 DSGVO die **Informationspflicht in solchen Fällen, in denen die Daten ohne Mitwirkung der betroffenen Person erhoben worden sind**.

Gegenüber der in → Art. 13 DSGVO geregelten Situation ist die betroffene Person typischerweise mindestens auf zwei zusätzliche Informationen angewiesen: Wenn ein Verantwortlicher die Daten nicht bei der betroffenen Person erhebt, hat sie an der bisherigen Verarbeitung nicht mitgewirkt. Oft wird sie also nicht wissen, dass und welche Daten der Verantwortliche sich beschafft hat. Da die betroffene Person auch nicht selbst die sie betreffenden personenbezogenen Daten mitgeteilt hat, müssen die Daten zudem aus einer anderen Quelle kommen. Deshalb sieht → Art. 14 Abs. 1 Buchst. d DSGVO vor, dass der Verantwortliche der betroffenen Person die **Kategorien der personenbezogenen Daten** mitzuteilen hat, die er erhoben hat. Nach → Art. 14 Abs. 2 Buchst. f DSGVO muss er unter Umständen auch darüber informieren, **aus welchen Quellen** die erhobenen Daten stammen.

Nach → Art. 14 Abs. 1 Buchst. d DSGVO muss der Verantwortliche nur über die Kategorien personenbezogener Daten informieren (und nicht über die tatsächlich erhobenen Daten). Der Begriff „Kategorie" ist ein anderes Wort für „Arten". Wenn der Verantwortliche den Namen „Peter Mustermann" erhebt, ist die mitzuteilende Datenkategorie „Name" (oder „Vor- und Nachname"). Die Datenschutz-Grundverordnung will damit den Aufwand des Verantwortlichen für eine Erstinformation begrenzen. Falls die betroffene Person mehr wissen oder die Richtigkeit der Daten kontrollieren will, kann sie nach → Art. 15 DSGVO Auskunft über die sie betreffenden Daten verlangen.

Es gibt noch einen wichtigen Unterschied zwischen der Datenerhebung bei der betroffenen Person und sonstigen Datenerhebungen: Die Direkterhebung hat zur Folge, dass die betroffene Person weiß, wann der Verantwortliche eine Verarbeitung sie betreffender personenbezogener Daten beginnt. Bei der sonstigen Datenerhebung hat sie oft keine Kenntnis darüber, dass überhaupt eine Verarbeitung durch den Verantwortlichen stattfindet.

Beispiel:

> Eine Auskunftei erhält die Bonitätsanfrage eines Kunden K. zur Person der A. Sie übermittelt dann Informationen etwa über bereits laufende Darlehen und wie A. zuverlässig diese Darlehen tilgt. Zu welchem Zeitpunkt sollte die Auskunftei die A. informieren?

Wichtig sind also Vorschriften, die ausdrücklich klären, **ob und wann betroffene Personen zu informieren sind**. Diese Regelungen finden Sie in → Art. 14 Abs. 5 DSGVO und → Art. 14 Abs. 3 DSGVO.

→ Art. 14 Abs. 5 DSGVO klärt **Ausnahmefälle, in denen eine Information nicht erfolgen muss**. Dazu gehört zunächst die Situation, in der die betroffene Person ausnahmsweise schon über die Verarbeitung informiert ist, → Art. 14 Abs. 5 Buchst. a DSGVO.

In anderen Fällen kann es einen unverhältnismäßig großen Aufwand bedeuten, alle betroffenen Personen zu informieren. Ein solcher Fall kann etwa vorliegen, wenn der Verantwortliche eigentlich kein besonderes Interesse an der betroffenen Person hat, → Art. 14 Abs. 5 Buchst. b DSGVO.

Beispiel:

> Teilweise scannen Krankenkassen alle Unterlagen ein, die ihnen von Versicherten zugesandt werden. In einem Anschreiben erwähnt eine versicherte Person A. andere Personen B. und C., ohne dass die Verhältnisse dieser Personen aus Sicht der Krankenkasse von Bedeutung für das Rechtsverhältnis mit A. wären. – Scannt die Krankenkasse die Unterlagen ein, verarbeitet sie nicht nur die personenbezogenen Daten von A., sondern auch von

B. und C. Interesse hat sie eigentlich nur an Informationen über A. Auch darf sie normalerweise davon ausgehen, dass B. und C. nicht besonders intensiv von ihrer Verarbeitung betroffen sind. Sie muss B. und C. also meist nicht informieren. Allerdings muss sie „geeignete Garantien" ergreifen, um B. und C. angemessen zu schützen. So muss sie durch technische und organisatorische Maßnahmen dafür sorgen, dass die Daten nur im Rahmen des Versicherungsverhältnisses zwischen ihr und A. verwendet werden.

Die Beurteilung kann sich im Verlauf der Zeit, etwa auf Grund des Eintritts einer neuen Sachlage aber ändern. Dann kann eine nachträgliche Information erforderlich werden.

Beispiel:

Die Krankenkasse aus dem vorigen Beispiel wird von einem Unternehmen aufgefordert, das erwähnte Schreiben mit den Daten über A., B. und C. zu übermitteln. Spätestens jetzt muss die Krankenkasse sich im Klaren darüber sein, dass eine Weitergabe des Schreibens nicht nur mit Risiken für A., sondern auch für B. und C. verbunden sein kann. Geht es dem Datenempfänger ebenfalls nur um A., kann es notwendig sein, die nicht erforderlichen Daten von B. und C. zu schwärzen. Geht es dem Datenempfänger aber auch um B. und C., kann dies dazu führen, dass die Krankenkasse B. und C. jetzt doch über die Verarbeitung informieren muss.

In manchen Fällen schreiben Rechtsvorschriften ausdrücklich vor, dass sich eine Behörde oder öffentliche Stelle personenbezogene Daten beschafft oder sie gegenüber anderen offenlegt. Nach → Art. 14 Abs. 5 Buchst. c DSGVO sind in solchen Fällen die betroffenen Personen nicht zwingend zu informieren– man muss das Recht einfach kennen. Diese Weichenstellung der Datenschutz-Grundverordnung mag unter dem Gesichtspunkt der Transparenz als nicht optimal erscheinen. Allerdings hat in solchen Fällen der Gesetzgeber über die Voraussetzungen der Datenweitergabe entschieden und dabei Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen treffen können. Eine Informationspflicht entfällt nach → Art. 14 Abs. 5 Buchst. d DSGVO zudem bei besonderen Geheimhaltungspflichten.

Greift keine der in → Art. 14 Abs. 5 DSGVO geregelten Ausnahmen ein, richtet sich der Zeitpunkt der Information nach → Art. 14 Abs. 3 DSGVO. Im Normalfall muss der Verantwortliche innerhalb einer angemessenen Frist informieren, vgl. → Art. 14 Abs. 3 Buchst. a DSGVO. Was angemessen ist, hängt von den Umständen der jeweiligen Verarbeitung ab. Der Verantwortliche darf aber die Information nicht endlos hinausschieben – spätestens innerhalb eines Monats nach Erlangung der Daten ist zu informieren!

Daneben regelt → Art. 14 Abs. 3 DSGVO zwei Sonderfälle der Information. Der erste Sonderfall betrifft die Situation, in der ein Verantwortlicher mit der betroffenen Person kommunizieren will, → Art. 14 Abs. 3 Buchst. b DSGVO.

Der zweite Sonderfall, der in → Art. 14 Abs. 3 Buchst. c DSGVO geregelt ist, betrifft Datenübermittlungen durch Stellen, die Daten nur verarbeiten, um sie anderen zu offenbaren. Dazu gehören im privaten Sektor beispielsweise Auskunfteien und Adresshändler. Aus Sicht der betroffenen Personen wäre es unter Umständen von Vorteil, wenn sie vor der beabsichtigten Übermittlung ihrer Daten informiert werden. Denn dann können sie eine solche Übermittlung noch rechtzeitig unterbinden. Andererseits haben die Datenempfänger ein Interesse, dass für sie relevante Informationen nicht blockiert werden können. Ausgerechnet hier bleibt → Art. 14 Abs. 3 Buchst. c DSGVO allerdings unklar. Der Verantwortliche muss die Information „spätestens zum Zeitpunkt der ersten Offenlegung" erteilen. – Heißt „zum Zeitpunkt" vor der Offenlegung oder danach? In der Fachliteratur ist diese Frage umstritten. Ausgehend vom Schutzgedanken liegt es nahe, eine Information vor der Offenlegung anzunehmen.

Vertiefung:

> Zur Anwendung von → Art. 13 und 14 DSGVO liegt eine Orientierungshilfe des Bayerischen Landesbeauftragten für den Datenschutz vor („Informationspflichten des Verantwortlichen", im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Informationspflichten").

5.3 Benachrichtigungspflicht des Verantwortlichen

Neben den allgemeinen, in → Art. 13 und 14 DSGVO geregelten Informationspflichten gibt es auch noch eine besondere Informationspflicht: Kommt es bei dem Verantwortlichen zu einer „Datenpanne", schreibt → Art. 34 DSGVO die Benachrichtigung betroffener Personen vor, wenn „ein hohes Risiko für die Rechte und Freiheiten" entstanden ist. Der Verantwortliche muss die „Datenpanne" gemäß → Art. 33 DSGVO stets auch an die zuständige Datenschutz-Aufsichtsbehörde melden.

Beispiel:

> Weil ein öffentliches Krankenhaus auf Updates seines Virenschutzes verzichtet hat, konnte ein Angreifer einen Verschlüsselungstrojaner in dessen IT-System einschleusen. Über einen längeren Zeitraum waren Patientendaten nicht verfügbar. Der Betrieb des Krankenhauses war erheblich eingeschränkt. Behandlungen mussten verschoben oder in anderen Krankenhäusern durchgeführt werden. – Die Datenpanne hatte – mittelbar – erhebliche

gesundheitliche Risiken infolge verzögerter Behandlungen bei einer Vielzahl von Personen zur Folge. Daher ist neben einer Meldung an die Datenschutz-Aufsichtsbehörde auch eine Benachrichtigung der Patientinnen und Patienten erforderlich.

Der Umfang der Benachrichtigung ist in → Art. 34 Abs. 2 in Verbindung mit → Art. 33 Abs. 3 Buchst. b, c und d DSGVO geregelt. Der Verantwortliche muss der betroffenen Person danach mitteilen:

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten sowie
- 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.

Wenn Sie einmal eine Benachrichtigung nach → Art. 34 DSGVO erhalten, sollten Sie überlegen, mit welchen personenbezogenen Daten Sie von der „Datenpanne" betroffen sein könnten und welche Maßnahmen Sie treffen könnten, um Nachteile für Sie selbst möglichst gering zu halten. Die näheren Folgerungen hängen vom Einzelfall ab. Eine Information nach → Art. 34 DSGVO kann etwa Überlegungen anstoßen, ob die Ausübung von Betroffenenrechten (etwa des Rechts auf Löschung, siehe Abschnitt 5.6), der Widerruf einer Einwilligung (siehe Abschnitt 4.1.1) oder die Prüfung eines Schadensersatzanspruchs zur Wahrung der eigenen Interessen angezeigt sein könnte.

Vertiefung:

Zum Umgang mit → Art. 33 und 34 DSGVO liegt eine Orientierungshilfe des Bayerischen Landesbeauftragten für den Datenschutz vor („Meldepflicht und Benachrichtigungspflicht des Verantwortlichen", im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Melde- und Benachrichtigungspflicht").

5.4 Auskunftsrecht der betroffenen Person

Das Auskunftsrecht ergänzt die Regelungen zu den Informationspflichten. Hier hat es die betroffene Person nun selbst in der Hand, auf den Verantwortlichen zuzugehen, um mehr zu erfahren, als die Datenschutzhinweise bieten können: eine Information nämlich über die konkret verarbeiteten Daten, nicht nur über ihre Kategorien (zu

diesem Unterschied siehe Abschnitt 5.2). Das Auskunftsrecht ist eines der beiden zentralen Betroffenenrechte, die in Art. 8 Abs. 2 Satz 2 GRCh ausdrücklich garantiert werden. In der Datenschutz-Grundverordnung ist es in → Art. 15 DSGVO geregelt. Mit dem Auskunftsrecht ist das Recht auf eine Kopie der eigenen personenbezogenen Daten verknüpft (→ Art. 15 Abs. 3 DSGVO, siehe Abschnitt 5.4.1).

Was bringt mir das Auskunftsrecht? ▪ Sie erfahren, ob der Verantwortliche personenbezogene Daten von Ihnen verarbeitet und welche dies sind. Dazu erhalten Sie zahlreiche weitere Informationen. Auf dieser Grundlage können Sie beispielsweise einschätzen,

- ob der Verantwortliche Informationen über Sie hat, die Sie dort gar nicht vermutet haben;
- ob der Verantwortliche Informationen aufgehoben hat, die längst gelöscht sein sollten – insofern kommt als nächstes ein Löschungsantrag in Betracht (siehe Abschnitt 5.6);
- wohin der Verantwortliche diese Informationen weitergegeben hat;
- ob die Informationen alle „stimmen" oder ob der Verantwortliche mit Daten arbeitet, von denen man dies nicht behaupten kann – insofern könnten Sie über einen Berichtigungsantrag nachdenken (siehe Abschnitt 5.5).

Welche Voraussetzungen müssen erfüllt sein? ▪ Wie die übrigen datenschutzrechtlichen Betroffenenrechte steht Ihnen das Recht auf Auskunft gegenüber dem Verantwortlichen grundsätzlich nur dann zu, wenn Sie selbst von einer Verarbeitung personenbezogener Daten betroffen sind. Der Auskunftsantrag muss sich auf Ihre Daten, nicht auf die Daten eines Dritten beziehen. Sie müssen als Person identifiziert oder zumindest identifizierbar sein.

Beispiel 1:

> Sie verlangen beim Einwohnermeldeamt Ihrer Stadt Auskunft darüber, welche Informationen über Sie gespeichert sind. Sie sind die „betroffene Person", weil es um die Informationen geht, die sich auf Sie beziehen. Dieser Auskunftsanspruch ist übrigens im Fachrecht besonders geregelt, siehe § 10 Bundesmeldegesetz (BMG).

Beispiel 2:

> Sie verlangen beim Einwohnermeldeamt Ihrer Stadt Auskunft darüber, welche Informationen über Ihre Partnerin oder Ihren Partner gespeichert sind. Sie sind nicht die betroffene Person; wie eng Sie mit dieser verbunden sind, spielt für die Betroffenheit keine Rolle. Ihre Partnerin oder Ihr Partner muss einen Auskunftsantrag selbst stellen.

Beispiel 3:

> Sie verlangen beim Einwohnermeldeamt Ihrer Stadt Auskunft darüber, welche Informationen über Ihr zehnjähriges Kind gespeichert sind. Sie sind zwar nicht die betroffene Person, als Personensorgeberechtigte oder Personensorgeberechtigter können Sie das Auskunftsrecht aber regelmäßig für Ihr Kind ausüben.

Ein berechtigtes Interesse muss für den Auskunftsantrag nach → Art. 15 Abs. 1 DSGVO nicht geltend gemacht werden.

Vertiefung:

> Aufgrund gesetzlicher Sondervorschriften dürfen manche Behörden aber eine Begründung für Auskunftsbegehren verlangen. So sieht Art. 23 Abs. 1 Satz 1 Bayerisches Verfassungsschutzgesetz vor, dass die Auskunft auf einen Antrag erteilt wird, „in dem ein besonderes Interesse an einer Auskunft dargelegt ist". Auch dabei dürfen allerdings keine überspannten Anforderungen gestellt werden (nähere Hinweise auf https://www.datenschutz-bayern.de in der Rubrik „Themengebiete – Verfassungsschutz – Häufige Fragen").

Ach, übrigens:

> Die Datenverarbeitung des Bayerischen Landesamts für Verfassungsschutz unterliegt nicht unmittelbar der Datenschutz-Grundverordnung. Sie dient der nationalen Sicherheit, die nicht in den Anwendungsbereich des Unionsrecht fällt (vgl. → Art. 2 Abs. 2 Buchst. a DSGVO).

Wie mache ich das Auskunftsrecht geltend? ▪ Im Grundsatz kann der Auskunftsanspruch formlos geltend gemacht werden. Regelmäßig können Sie also selbst entscheiden, ob Sie einen Antrag schriftlich, per E-Mail oder in anderer Form stellen. Aus Sicht der Datenschutz-Aufsichtsbehörde ist die Schriftform zu empfehlen, alternativ eine verschlüsselte E-Mail. Bei diesen beiden Formen ist der Übertragungsweg hinreichend gesichert.

Ist sich ein Verantwortlicher nicht sicher, ob ein auf Ihren Namen lautender Antrag tatsächlich von Ihnen stammt, kann er von Ihnen einen Identitätsnachweis verlangen. Insbesondere, wenn der Verantwortliche besonders sensible Daten verarbeitet oder wenn er aufgrund eines Gesetzes verpflichtet ist, sich über die Identität der Antragstellerin oder des Antragstellers zu vergewissern, ist gegen entsprechende Nachfragen grundsätzlich nichts einzuwenden. Verantwortliche verlangen für die Identifizierung nicht selten die Übersendung einer Kopie Ihres Personalausweises.

Tipp:

> Die Vorlage einer Ausweiskopie ist allerdings längst nicht das einzige, dafür ein verhältnismäßig belastendes Identifizierungsmittel. Immerhin enthält der Ausweis zahlreiche Anga-

ben, die über die Zuordnung Name – Anschrift hinausreichen. Der Bayerische Landesbeauftragte für den Datenschutz hat zu diesem Thema Hinweise veröffentlicht (Identifizierung bei der Geltendmachung von Betroffenenrechten, Aktuelle Kurz-Information 22, im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen"). Darauf können Sie sich gegenüber bayerischen öffentlichen Stellen berufen. Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz sind Besonderheiten zu beachten.

Sollen Sie eine Kopie Ihres Personalausweises einsenden, dürfen Sie nicht erforderliche Angaben wie etwa die Zugangs- und die Seriennummer schwärzen. Die öffentliche Stelle muss Sie hierauf ausdrücklich hinweisen (→ Art. 13 Abs. 2 Buchst. e DSGVO).

Was kann ich vom Verantwortlichen erwarten? ▪ Machen Sie Ihr Auskunftsrecht geltend, hat der Verantwortliche Ihre Anfrage „unverzüglich" zu beantworten. „Unverzüglich" heißt normalerweise „ohne schuldhaftes Zögern" und ist ein nicht übermäßig dehnbarer Begriff. Nach der Datenschutz-Grundverordnung soll die Auskunft regelmäßig spätestens innerhalb eines Monats erfolgen, nachdem Ihr Auskunftsantrag den Verantwortlichen erreicht hat. Bei umfangreicheren oder komplizierteren Auskunftsanträgen darf der Verantwortliche diese Frist auf bis zu drei Monate ausdehnen. Er muss Ihnen eine solche Verzögerung aber jedenfalls innerhalb des ersten Monats mitteilen. Die Fristverlängerung ist ein Ausnahmefall und kommt bei unproblematischen Auskunftsanträgen regelmäßig nicht in Betracht.

Beispiel:

Eine betroffene Person verlangt gegenüber der Stadtverwaltung einer Großstadt umfassend Auskunft über ihre dort gespeicherten personenbezogenen Daten, ohne mögliche „Fundorte" anzugeben. In diesem Fall wird die Datenschutzstelle der Stadt regelmäßig bei verschiedenen Referaten und Eigenbetrieben nachfragen, ob und welche Daten über die betroffene Person gespeichert sind. Bis sämtliche Informationen aus verschiedenen Stellen zusammengetragen sind, können mehrere Wochen vergehen.

In einem solchen Fall ist damit zu rechnen, dass die Datenschutzstelle der betroffenen Person eine Zwischennachricht zuleitet, in der sie auf die mögliche zeitliche Verzögerung hinweist. Wenn die Anfrage wie im Beispiel sehr allgemein gehalten war, wird die Datenschutzstelle in ihrer Eingangsbestätigung die betroffene Person bitten, ihr Auskunftsinteresse konkreter zu beschreiben: Geht es der betroffenen Person tatsächlich um alle verarbeiteten Daten? Oder betrifft die Anfrage einen speziellen Vorgang bei der Stadt – etwa eine strittige Rechnung oder eine besondere Mitteilung?

Versäumt der Verantwortliche die Dreimonatsfrist, verstößt er gegen geltendes Datenschutzrecht – egal welche Gründe er für die Fristversäumnis vorbringt. Denn die Datenschutz-Grundverordnung sieht keine Ausnahmen von dieser Maximalfrist von drei Monaten vor.

Ach, übrigens:

> Bitte beachten Sie, dass die für die Bekämpfung von Straftaten zuständigen Behörden zumeist nicht der Datenschutz-Grundverordnung unterliegen. Sie müssen Ihnen zwar auch „unverzüglich" Auskunft erteilen – eine maximale Frist von drei Monaten ist aber dort nicht vorgesehen.

Der Verantwortliche muss dabei nach → Art. 12 Abs. 1 DSGVO „geeignete Maßnahmen" treffen, um Ihnen die Sie angehenden Mitteilungen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln." Bei komplexen Verarbeitungen kann der Verantwortliche sogar verpflichtet sein, die Verarbeitungen für Sie zu „visualisieren", falls er sie anders nicht verständlich machen kann (vgl. Erwägungsgrund 58 DSGVO). Das Gebot der einfachen und verständlichen Sprache gilt ganz besonders für Informationen, die sich speziell an Kinder richten. Mit anderen Worten muss die Auskunft so gestaltet sein, dass ein Kind diese Information auch verstehen kann.

Nach → Art. 12 Abs. 2 DSGVO hat der Verantwortliche der betroffenen Person die Ausübung des Auskunftsrechts zu erleichtern. Wenn Sie also als betroffene Person Auskunft über eine Sie betreffende Datenverarbeitung verlangen, darf Ihnen der Verantwortliche keine Steine in den Weg legen, sondern muss versuchen, Sie möglichst darin zu unterstützen, damit Sie an die begehrte Information gelangen.

Beispiel:

> Sie verlangen gegenüber Ihrer Stadt allgemein Auskunft „hinsichtlich aller Daten, die über mich gespeichert sind". – Die Stadt könnte jetzt natürlich versuchen, sämtliche über Sie gespeicherten personenbezogenen Daten herauszufinden und Ihnen mitzuteilen. Dann würden Sie unter Umständen mit einer Masse von Informationen überflutet, die Sie überhaupt nicht interessieren. Erfahrungsgemäß haben betroffene Personen meistens einen konkreten Anlass, weswegen sie ihren Auskunftsanspruch geltend machen. Sie müssen deshalb damit rechnen, dass die Stadt Sie zunächst ganz allgemein über ihre Verarbeitungen informiert und fragt, an welchen Informationen Sie konkret interessiert sind.

Regelmäßig sind Sie zwar nicht verpflichtet, Ihren Auskunftsanspruch zu begründen. Eine solche Begründung ist aber oft sinnvoll, um die Bearbeitung Ihres Auskunftsantrags zu beschleunigen. Falls Sie also einen konkreten Anlass haben, weswegen Sie vom Verantwortlichen eine Auskunft haben wollen, versuchen Sie Ihr Anliegen möglichst genau zu beschreiben. Falls dies schwierig erscheint, kann es oft auch sinnvoll sein, den Anlass Ihres Auskunftsantrags zu benennen. Auf diese Weise erleichtern Sie dem Verantwortlichen die Suche nach den begehrten Informationen ganz erheblich.

Vertiefung

Ein Begründungserfordernis kann bei einem Antrag auf Auskunft über Sozialdaten zu beachten sein. Nach § 83 Abs. 2 Satz 1, 2 SGB X soll die betroffene Person die Art der Sozialdaten, über die Auskunft erteilt werden soll, näher bezeichnen. Bei nicht automatisiert oder nicht in nicht automatisierten Dateisystemen gespeicherten Sozialdaten müssen zudem Angaben gemacht werden, die das Auffinden der Daten ermöglichen.

Tipp:

Sie haben übrigens auch die Möglichkeit, sich von der oder dem behördlichen Datenschutzbeauftragten der öffentlichen Stelle beraten zu lassen, wie Sie Ihren Auskunftsantrag zweckmäßig formulieren. Dieses Recht ist in → Art. 38 Abs. 4 DSGVO geregelt.

Da sich das Auskunftsrecht nach → Art. 15 Abs. 1 DSGVO auf die Sie betreffenden Daten bezieht, genügt es nicht, wenn der Verantwortliche Ihnen auf Ihren Antrag hin lediglich „Kategorien personenbezogener Daten" mitteilt. Der Sinn des Auskunftsrechts besteht ja auch darin, Ihnen die Nachprüfung zu ermöglichen, ob der Verantwortliche Ihre Daten richtig und rechtmäßig verarbeitet hat.

Beispiel:

Wenn das Einwohnermeldeamt Ihnen mitteilt, es habe „Ihren Namen und Ihre Adresse" gespeichert, teilt es Ihnen Kategorien von Daten, nicht aber Ihre konkreten Daten mit. Sie als betroffene Person können aus einer solchen Auskunft insbesondere nicht ablesen, ob das Einwohnermeldeamt Ihren Namen und Ihre Anschrift richtig gespeichert hat.

Sonderproblem: Datenquellen und Datenempfänger ▪ Im Allgemeinen haben Sie als betroffene Person häufig ein besonderes Interesse daran, die **Datenquellen** und **Datenempfänger** zu erfahren. Denn eine Datenquelle kann möglicherweise „weiter sprudeln" und die personenbezogenen Daten der betroffenen Person auch an andere Verantwortliche weitergeben. Der Datenempfänger ist für Sie als betroffene Person wichtig, weil Daten regelmäßig anlassbezogen weitergegeben werden. Sie müssen also damit rechnen, dass der Datenempfänger Ihre Daten weiterverwendet.

In der Vergangenheit liefen Auskunftsersuchen gerade in Bezug auf Datenquellen und Datenempfänger oft leer, weil die Verantwortlichen diese Daten – wenn überhaupt – nur kurzfristig speicherten.

Beispiel:

Herr Rijkeboer beantragte bei der Stadtverwaltung von Rotterdam Auskunft darüber, an wen sie in den vergangenen zwei Jahren seine personenbezogenen Daten übermittelt hat. Die Stadt Rotterdam erteilt ihm auf Grundlage des niederländischen Rechts nur Auskunft über den Zeitraum des zurückliegenden Jahres.

Hier stehen zwei Datenschutzvorschriften in einem Spannungsverhältnis zueinander, die eigentlich beide dem Interesse der betroffenen Person dienen. Wenn die betroffene Person ihr Auskunftsrecht nach → Art. 15 DSGVO effektiv ausüben können soll, muss der Verantwortliche bestimmte Daten längerfristig aufbewahren. Eine solche Speicherung wirft allerdings die Frage nach dem Grundsatz der Datenminimierung auf, vgl. → Art. 5 Abs. 1 Buchst. c DSGVO (zu diesem Grundsatz können Sie sich in Abschnitt 4.5 informieren).

Beispiel (Fortsetzung)

In dem Fall entschied der Europäische Gerichtshof [Urteil vom 7. Mai 2009, C-553/07], dass die Mitgliedstaaten Aufbewahrungsfristen vorzusehen haben, die einen „gerechten Ausgleich bilden", zwischen den datenschutzrechtlichen Auskunftsinteressen der betroffenen Person und dem Interesse der Verantwortlichen, nicht über Gebühr mit Aufbewahrungspflichten belastet zu werden. Zu berücksichtigen ist dabei, dass bestimmte Basisdaten (Name, Adresse usw.) zumeist sehr langfristig aufbewahrt und auch oft übermittelt werden. Andere Daten sind für einen berechtigten Verarbeitungszweck nur relativ kurz aufzubewahren. Häufig werde ein Jahr Aufbewahrungsfrist in Bezug auf Angaben über Datenempfänger den berechtigten Informationsinteressen der betroffenen Person allerdings nicht gerecht.

5.4.1 Recht auf Kopie

Der Verantwortliche hat der betroffenen Person nach → Art. 15 Abs. 3 Satz 1 DSGVO eine kostenlose Kopie der sie betreffenden Daten zur Verfügung zu stellen. Das bedeutet allerdings nicht, dass Sie von einer Behörde oder von anderen Verantwortlichen pauschal verlangen können, alle über Sie geführten Akten kostenlos vollständig zu kopieren und Ihnen zur Verfügung zu stellen. Das Recht auf Kopie bezieht sich (gerade) auf personenbezogene Daten. Es ergänzt das Recht auf Auskunft, darf aber weder mit einem allgemeinen Recht auf Zugang zu Verwaltungsdokumenten – wie es in anderen Bundesländern ein Informationsfreiheitsgesetz oder in Bayern → Art. 39 Abs. 1 BayDSG vermittelt – noch mit einem Akteneinsichtsrecht verwechselt werden.

Oft enthalten Verwaltungsvorgänge nur zu einem verhältnismäßig geringen Teil Informationen, die als personenbezogene Daten zu werten sind. Machen Sie das Recht auf Kopie geltend, muss Ihnen der Verantwortliche auch nur diese Informationen zugänglich machen. Das kann durch Bereitstellung von Kopien in Papierform oder in elektronischer Form geschehen, wobei Sie damit rechnen müssen, dass der Verantwortliche unter Umständen erhebliche Teile dieser Kopien schwärzt. Er kann aber auch eine Art „Datenauszug" aus dem betreffenden Verwaltungsvorgang herstellen,

in dem Ihre von ihm verarbeiteten personenbezogenen Daten – möglichst nach den Kategorien – aufgelistet sind.

Enthalten einmal – eher ausnahmsweise – Dokumente in einem Vorgang ganz überwiegend personenbezogene Daten von Ihnen, so verschafft Ihnen das Recht auf Kopie aber einen Anspruch, eine Ablichtung oder eine entsprechende Datei zu erhalten.

Beispiele:

> Anträge oder Erklärungen der betroffenen Person; Dokumente, mit welchen die betroffene Person einen persönlichen Wissensstand wiedergibt; Dokumente, die in erster Linie Gesundheitsdaten der betroffenen Person, Informationen über den Lebensweg und den beruflichen Werdegang sowie über die Familien- oder Vermögensverhältnisse enthalten.

Erteilt der Verantwortliche Ihnen Auskunft über die über Sie verarbeiteten Daten, darf er die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Das ergibt sich für Ihr Recht auf Kopie unmittelbar aus → Art. 15 Abs. 4 DSGVO.

Ach, übrigens:

> Für medizinische **Behandlungsverträge** sieht § 630g Abs. 2 des Bürgerlichen Gesetzbuchs (BGB) eine Sonderregelung vor. Danach kann der Patient elektronische Abschriften von der Patientenakte verlangen. Er hat dem Behandelnden allerdings die entstandenen Kosten zu erstatten. – Der grundsätzlich gebührenfreie datenschutzrechtliche Auskunftsanspruch aus → Art. 15 DSGVO und das Patientenrecht auf Kopie der Patientenakte sind nicht immer einfach voneinander zu trennen. Geht es vor allem darum, die Diagnose und die Behandlung nachzuvollziehen, ist zumeist § 630g Abs. 2 BGB anzuwenden. Geht es stattdessen in erster Linie darum, welche personenbezogenen Daten verarbeitet wurden, gilt der Grundsatz der Gebührenfreiheit nach → Art. 12 Abs. 5 DSGVO.

5.4.2 Nicht enttäuscht sein! Ausnahmen vom Auskunftsanspruch

→ Art. 15 DSGVO sieht nicht vor, dass Ihr Auskunftsanspruch im Einzelfall ausgeschlossen sein kann. Gleichwohl darf eine öffentliche Stelle Ihnen manchmal eine Auskunft über Ihre personenbezogenen Daten rechtmäßig verweigern. Wie kann das sein?

Die Antwort hierauf finden Sie etwas versteckt in → Art. 23 Abs. 1 DSGVO. Diese Vorschrift erlaubt den Mitgliedstaaten, die Betroffenenrechte einzuschränken. Allerdings muss die Beschränkung Ihres Auskunftsrechts eine „in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme" sein. Das ist eine Anforderung an den nationalen Gesetzgeber, der den Ausschluss nicht „einfach so" oder mit dem Zweck anordnen darf, den nationalen Behörden die Arbeit zu erleichtern. Für den

Ausschluss müssen gute Gründe sprechen. Für bayerische öffentliche Stellen regelt → Art. 10 BayDSG einige Beschränkungen des Auskunftsrechts.

Beispiel:

Die zuständige Behörde erhält Hinweise auf hygienische Missstände in einer bereits auffällig gewordenen Bäckerei, welche die Prüfung einer Gewerbeuntersagung nahelegen. Der Inhaber glaubt, dass eine Beschäftigte oder ein Beschäftigter mit der Behörde Kontakt aufgenommen hat und beantragt dort Selbstauskunft mit dem Ziel, Informationen zur Herkunft der Daten zu erlangen (vgl. → Art. 15 Abs. 1 Buchst. g DSGVO). Er will der betreffenden Person – bei Bestätigung des Verdachts – anschließend kündigen. – Die Behörde wird jedenfalls diese Informationen nicht herausgeben, um den Schutz ihrer Informantin oder ihres Informanten sicherzustellen. Das ist von → Art. 10 Abs. 2 Nr. 3 BayDSG gedeckt.

5.4.3 Auskunft im Sozialrecht

Bitte beachten Sie: Im Sozialrecht besteht das Auskunftsrecht unter anderem nicht, soweit die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben gefährden würde und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss. Das ergibt sich aus § 83 Abs. 1 Nr. 1, § 82a Abs.1 Nr. 1 Buchst. a Zehntes Buch Sozialgesetzbuch.

Beispiel:

Einem Elternpaar ist wegen Gewalttätigkeiten gegen seine Kinder das Aufenthaltsbestimmungsrecht entzogen worden. Die Kinder sind in eine Pflegefamilie gekommen, die dem Elternpaar nicht mitgeteilt wird.

5.4.4 Auskunft im Beamtenrecht

Nach Art. 107 Abs. 1 Bayerisches Beamtengesetz können Beamtinnen und Beamte während und nach Beendigung des Beamtenverhältnisses **Auskunft aus ihrer Personalakte** und aus anderen Akten verlangen, die personenbezogene Daten über sie enthalten und für das Dienstverhältnis verarbeitet werden. Das Auskunftsrecht umfasst ein **Recht auf Akteneinsicht**.

5.5 Recht auf Berichtigung

Die bei einem Verantwortlichen gespeicherten personenbezogenen Daten sind dort Grundlage für Entscheidungen. Bei öffentlichen Stellen geht es oftmals um Nachteile, die Bürgerinnen und Bürgern einseitig auferlegt, oder um Vorteile, die ihnen gewährt werden. Stimmt die Entscheidungsgrundlage nicht, kann die Entscheidung „an

der Realität vorbeigehen" – auch zum Nachteil einer betroffenen Person. Vor diesem Hintergrund obliegt dem Verantwortlichen in Bezug auf die von ihm verarbeiteten personenbezogenen Daten eine Pflicht zur Qualitätssicherung (siehe Abschnitt 4.6). In Art. 8 Abs. 2 Satz 2 GRCh ist das Recht auf Berichtigung ausdrücklich garantiert. Schon dieser Umstand gibt dem Berichtigungsrecht einen besonderen Stellenwert.

Was bringt mir das Berichtigungsrecht? ▪ Das Recht auf Berichtigung (→ Art. 16 DSGVO) gibt Ihnen die Möglichkeit, an der Qualitätssicherung durch den Verantwortlichen mitzuwirken. Es versetzt Sie insbesondere in die Lage, entsprechende Maßnahmen anzustoßen. Mitunter weiß der Verantwortliche nämlich gar nicht, dass von ihm gespeicherte Daten unrichtig sind. Hat ein Berichtigungsantrag Erfolg, wird die Datengrundlage, mit welcher der Verantwortliche arbeitet, korrigiert; Sie müssen nicht mehr befürchten, Nachteile nur dadurch zu erleiden, dass der Verantwortliche eine Entscheidungen auf Grund unrichtiger personenbezogener Daten trifft. Vermieden werden so auch gerichtliche Auseinandersetzungen, die darauf zielen, solche Entscheidungen nachträglich zu ändern.

Welche Voraussetzungen müssen erfüllt sein? ▪ Nach → Art. 16 Satz 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Es muss also um personenbezogene Daten gehen – und zwar um solche der betroffenen Person –, und diese Daten müssen unrichtig sein. Was der Gesetzgeber mit „unrichtigen" Daten meint, ist nicht ganz klar. „Unrichtig" sind zumindest Tatsachenangaben, die nicht mit einer verbindlichen „Messgröße" übereinstimmen.

Beispiele:

> Einem Beamten wird in einem Personalverwaltungsprogramm der Eintrittstermin „1. August 2010" zugeschrieben, obwohl er ausweislich der bei seiner Personalakte befindlichen Ernennungsurkunde bereits zum 1. August 2001 erstmals ernannt wurde. – Eine Bewerberin um öffentlich geförderten Wohnraum wird in einer verwaltungsinternen Datenbank als „kinderlos" geführt, obwohl sie – belegt durch die entsprechenden Personenstandsurkunden – zwei Kinder hat und diese auch in ihrem Haushalt aufzieht.

„Unrichtig" können nur Tatsachen sein. Sieht man Werturteile als personenbezogene Daten an – was umstritten ist –, so sind sie vom Berichtigungsanspruch nicht erfasst. Das Fachrecht regelt hier aber oftmals eigenständig weitere Reaktionsmöglichkeiten für eine betroffene Person, so im Fall nachteiliger Bewertungen in Personalakten von Beschäftigten des bayerischen öffentlichen Dienstes in Art. 106 Satz 2, Art. 19 Abs. 1 Satz 1 Bayerisches Beamtengesetz.

Beispiel:

Die A. hat die Zweite Staatsprüfung für das Lehramt an Gymnasien erfolgreich abgelegt. Die zuständige Behörde hat ihre Einstellung im Beamtenverhältnis auf Probe gleichwohl abgelehnt. Sie begründet dies mit der Einschätzung des Amtsarztes, bei der A. sei mit dem Eintritt vorzeitiger Dienstunfähigkeit zu rechnen. A. stellt die bei ihrer Untersuchung getroffenen Feststellungen zum Gesundheitszustand nicht in Frage, beantragt aber, die getroffene Prognose zu berichtigen.

A. wendet sich gegen das Ergebnis der amtsärztlichen Beurteilung. Dabei handelt es sich um eine Gesamtbewertung (einer Vielzahl) erhobener Befunde, die nicht Gegenstand des Berichtigungsanspruchs sein kann. A. könnte aber beim Verwaltungsgericht um Überprüfung der ablehnenden Einstellungsentscheidung nachsuchen. Dabei könnte sie sich auch gegen ein möglicherweise fehlerhaftes amtsärztliches Gutachten wenden.

Kann die Richtigkeit einer Tatsache nicht anhand einer verbindlichen „Messgröße" beurteilt werden, können Meinungsverschiedenheiten zwischen der betroffenen Person und dem Verantwortlichen oft nur gerichtlich geklärt werden. Macht die betroffene Person einen Berichtigungsanspruch gegen eine bayerische öffentliche Stelle vor einem Verwaltungsgericht geltend, wird dieses die Frage der Richtigkeit oder Unrichtigkeit von Amts wegen aufzuklären haben. Das Gericht kann verbindlich feststellen, ob ein streitiger Berichtigungsanspruch besteht.

Zu beachten ist im Übrigen, dass der Erfolg eines Berichtigungsantrags auch vom Verwendungszusammenhang der betreffenden Daten abhängt. Dazu zwei Beispiele:

Beispiel 1:

Der A. hat erfolglos an einer berufsqualifizierenden Prüfung teilgenommen. Erfreut nimmt er zur Kenntnis, dass die Datenschutz-Grundverordnung nun ein Recht auf Berichtigung vorsieht. Schließlich enthalten fast alle seine Antworten „unrichtige Daten". Der Prüfungsausschuss lehnt den Berichtigungsantrag des A. gleichwohl ab. Zu Recht?

Die Antworten des A. sind als personenbezogene Daten zu werten, nicht zuletzt, weil sie gerade über seinen Kenntnisstand Auskunft geben. Aus fachlicher Sicht mögen die Antworten noch so falsch sein – das macht sie noch nicht zu „unrichtigen Daten". Denn im konkreten Verwendungszusammenhang kommt es darauf an, dass gerade der Kenntnisstand von A. dokumentiert ist. → Art. 16 Abs. 1 DSGVO verschafft daher keinen Anspruch auf eine nachträgliche Berichtigung fehlerhafter Prüfungsleistungen. Ein Berichtigungsanspruch könnte dem A. aber insbesondere dann zustehen, wenn ihm – etwa aufgrund einer Verwechslung von Kennziffern – die Antworten eines anderen Prüflings zugeordnet worden wären.

Beispiel 2:

Die B. hat eine Eigentumswohnung in einem Mehrfamilienhaus. Ein Nachbar behauptet gegenüber der zuständigen Bauaufsichtsbehörde, die B. nutze ihre Wohnung für ihren Beruf als Buchhalterin gewerblich. In einem daraufhin mit dem Ziel einer Nutzungsuntersagung eingeleiteten Verwaltungsverfahren kann die Behörde die illegale Nutzung aber nicht nachweisen. Das Verfahren wird daher eingestellt; das Schreiben, mit welchem der Nachbar die B. angeschwärzt hat, bleibt zunächst bei den Akten. B. verlangt Berichtigung. Zu Recht?

Die Behauptung, die B. nutze ihre Wohnung gewerblich, ist ein personenbezogenes Datum, weil sie das (angebliche) Verhalten der B. beschreibt. Das eingeleitete Verfahren zielt darauf, herauszufinden, ob der Vorwurf stimmt. Gelingt der Nachweis nicht, kann das unterschiedliche Gründe haben. Ein Rückschluss auf die Unrichtigkeit der Angaben des Nachbarn wäre verfrüht; möglicherweise lässt sich der Sachverhalt zu einem späteren Zeitpunkt aufklären.

Wie mache ich das Berichtigungsrecht geltend ▪ Wie das Auskunftsrecht kann auch das Berichtigungsrecht formlos geltend gemacht werden; der Verantwortliche wird erforderlichenfalls überprüfen, ob ein entsprechender Antrag auch tatsächlich von derjenigen Person stammt, der er dem äußeren Anschein nach zuzurechnen ist (siehe Abschnitt 5.4).

Der Antrag sollte klar und unmissverständlich darlegen, welche bei dem Verantwortlichen verarbeiteten personenbezogenen Daten unrichtig sind. Eine betroffene Person sollte sich überlegen, mit welchen Nachweisen sie die ihrer Auffassung nach richtigen Angaben untermauern kann. Diese Nachweise müssen nicht sogleich mitgeschickt werden. Eine Benennung ist aber sinnvoll, weil der Verantwortliche dann weiß, welche Erkenntnismittel zur Verfügung stehen und wo er gegebenenfalls auch selbst nachsehen könnte.

Beispiel:

Der Beamte A. hat festgestellt, dass ihm im Personalverwaltungsprogramm seines Dienstherrn für das Jahr 2017 eine Leistungsprämie von 500 Euro zugeschrieben wird. Tatsächlich hat er 2016 und 2018 je 1000 Euro erhalten, 2017 jedoch nichts. – A. wird Berichtigung beantragen und auf die bei seiner Personalakte befindlichen Mitteilungen über die Gewährung von Leistungsprämien verweisen.

Was kann ich vom Verantwortlichen erwarten? ▪ Wie beim Auskunftsrecht können Sie auch beim Berichtigungsrecht erwarten, dass Sie der Verantwortliche bei der Ausübung Ihres Rechts unterstützt, und dass er über Ihren Antrag unverzüglich entscheidet. Wenn die Voraussetzungen dafür vorliegen, muss er außerdem eine Berichtigung bewirken.

Manche Verantwortliche neigen zur „Verteidigung“ einmal aufgebauter Datenbestände. Dies gilt insbesondere für personenbezogene Daten, die in IT-Systemen verarbeitet werden – und zwar selbst dann, wenn vorhandene Papierakten solche Daten als unrichtig erweisen. Ist der Verantwortliche eine bayerische öffentliche Stelle, sollte in solchen Fällen grundsätzlich der behördliche Datenschutzbeauftragte zu Rate gezogen werden, der die örtlichen IT-Systeme und die handelnden Personen am besten kennt und auf eine Berichtigung hinwirken kann, ohne dass die Hilfe des Bayerischen Landesbeauftragten für den Datenschutz oder eines Verwaltungsgerichts in Anspruch genommen werden muss.

Unvollständige Daten ▪ Aus → Art. 16 Satz 2 DSGVO ergibt sich, dass mit „unrichtigen Daten“ nicht nur sachlich unrichtige Daten, sondern auch unvollständige Daten gemeint sind. Wenn → Art. 16 Satz 2 DSGVO festlegt, dass die betroffene Person das Recht hat, gegenüber dem Verantwortlichen die Vervollständigung unvollständiger Daten – auch mittels einer eigenen Erklärung – zu verlangen, ähnelt dieser Anspruch dem presserechtlichen Recht auf Gegendarstellung.

5.6 Recht auf Löschung („Recht auf Vergessenwerden“)

Auch das Recht auf Löschung gibt der betroffenen Person die Möglichkeit, auf den Datenbestand eines Verantwortlichen einzuwirken. Anders als beim Recht auf Berichtigung geht es aber hier nicht darum, den Datenbestand zu verbessern, sondern darum, ihn ganz oder in Teilen wieder loszuwerden: Der Verantwortliche soll mit den Daten nicht mehr arbeiten können. Das Recht auf Löschung ist in → Art. 17 Abs. 1 DSGVO geregelt.

Was ist eigentlich „Löschung“? ▪ Der Begriff „Löschung“ wird in der Datenschutz-Grundverordnung nicht näher definiert. Das bisherige deutsche Datenschutzrecht verstand darunter das „Unkenntlichmachen gespeicherter Daten“ (vgl. § 3 Abs. 4 Nr. 5 BDSG-alt). Im Unterschied dazu sprach man von Anonymisierung, wenn personenbezogene Daten derart verändert wurden, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder „nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren Person zugeordnet“ werden konnte (vgl. § 3 Abs. 6 BDSG-alt).

Was bringt mir das Recht auf Löschung? ▪ Verantwortliche haben häufig das Bestreben, ihre Informationsbestände – zu denen auch personenbezogene Daten in unübersehbarer Zahl gehören – möglichst auf Dauer zu bewahren. Manchmal fehlt

es an Zeit, hin und wieder „auszumisten", manchmal an Vorgaben, wie dies „rechtssicher" zu bewerkstelligen ist, manchmal liegt es aber auch im Interesse aller Beteiligten, wenn eine Überlieferung nicht „gekappt" wird.

Beispiel:

> In Bauamtsregistraturen bayerischer Städte können durchaus Bauakten vorhanden sein, welche die „Genehmigungsgeschichte" zu einer bestimmten Anschrift – etwa in einem Altstadtbereich – kontinuierlich seit der Mitte des 19. Jahrhunderts dokumentieren – einschließlich aller historischen Baupläne. Für Grundstückeigentümer, die ein Gebäude denkmalgerecht sanieren wollen, kann dies eine wertvolle Hilfe sein.

In den Fachgesetzen sind teilweise Fristen geregelt, wie lange bestimmte Unterlagen aufzubewahren sind. Derartige Regelungen bestehen aber längst nicht für alle Verwaltungsbereiche.

Beispiele:

> Geburtenregister werden im Standesamt 110 Jahre fortgeführt, anschließend dem zuständigen Archiv angeboten (§ 5 Abs. 5 Nr. 2, § 7 Abs. 3 Satz 1 Personenstandsgesetz – PStG); sie sind dauernd aufzubewahren (§ 7 Abs. 2 Satz 1 PStG). – Die Abschlusszeugnisse bayerischer öffentlicher Schulen sind dort 50 Jahre aufzubewahren (§ 40 Satz 1 Nr. 1, § 37 Satz 1 Nr. 1 Buchst. b Bayerische Schulordnung).

Nun sind ausgreifende Verwaltungsüberlieferungen für die einzelnen Bürgerinnen und Bürger nicht immer vorteilhaft. Viele Informationen können Nachteile bereiten – je nach dem Kontext, in den sie geraten, auch einmal völlig überraschend. Es muss hier nicht immer um den Vorwurf rechtswidrigen Verhaltens, um Eintragungen in polizeilichen oder nachrichtendienstlichen Registern gehen. Auch Informationen über die eigene Herkunft, über die Zugehörigkeit zu einer religiösen oder politischen Gruppierung können, heute vermeintlich „harmlos", übermorgen schon nachteilig sein.

Das Recht auf Löschung gibt Ihnen hier ein Stück weit Kontrolle über das, was die Verwaltungen über Sie wissen. Insbesondere dann, wenn Sie nach Gebrauch des Rechts auf Auskunft erfahren haben, wie Sie in einem konkreten Datenbestand erscheinen, können Sie mit dem Recht auf Löschung auf eine Verkleinerung der Wissensbasis, dabei gerade auch auf die Eliminierung potenziell nachteiliger Informationen hinwirken.

Welche Voraussetzungen müssen erfüllt sein? ▪ Allerdings besteht eine Löschpflicht nach → Art. 17 Abs. 1 DSGVO nur dann, wenn ein **Löschtatbestand** verwirklicht ist. Die Löschtatbestände sind in → Art. 17 Abs. 1 Buchst. a bis f DSGVO abschließend katalogmäßig erfasst.

Nach **Art. 17 Abs. 1 Buchst. a DSGVO** sind personenbezogene Daten zu löschen, wenn sie für den ursprünglichen Verarbeitungszweck nicht mehr notwendig sind.

Beispiel:

> Ein Unternehmen verkauft eine Ware an einen Verbraucher. Es liefert die Ware an den Verbraucher aus. Der Verbraucher bezahlt die Ware. Jetzt ist der Kaufvertrag durchgeführt. – Im Grundsatz ist die Verarbeitung personenbezogener Daten des Verbrauchers durch das Unternehmen nicht mehr notwendig.

Art. 17 Abs. 1 Buchst. b DSGVO betrifft Verarbeitungen, die der Verantwortliche auf die Einwilligung der betroffenen Person stützt. Einwilligungen sind im Grundsatz frei widerruflich, → Art. 7 Abs. 3 DSGVO. Widerruft die betroffene Person ihre Einwilligung, entfällt diese – mit Wirkung ab dem Widerruf – als Grundlage für die Verarbeitung.

Beispiel:

> Eine betroffene Person hat an einem Preisausschreiben teilgenommen. Dabei hat sie darin eingewilligt, dass der Verantwortliche ihre Adressdaten auch für Werbezwecke verwenden darf. Zwei Wochen später widerruft die betroffene Person ausdrücklich ihre Einwilligung. – Die betroffene Person kann das Recht auf Löschung mit dem Ziel geltend machen, dass ihre Kontaktdaten aus dem für Werbemaßnahmen genutzten Datenbestand entfernt werden.

Ach, übrigens:

> Die Einwilligungserklärung selbst sowie den Widerruf darf der Verantwortliche so lange aufheben, wie dies zur Erfüllung seiner Rechenschaftspflicht erforderlich ist (siehe dazu im Einzelnen Bayerischer Landesbeauftragter für den Datenschutz, Aufbewahren von Einwilligungen, Aktuelle Kurz-Information 8, im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen“).

In einem solchen Fall ist allerdings zu beachten, dass eine Verarbeitung außer auf einer Einwilligung auch noch auf einer anderen Rechtsgrundlage beruhen kann. Bei nicht-öffentlichen Stellen kommt hier insbesondere → Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO in Betracht, bei öffentlichen Stellen ist an Verarbeitungsbefugnisse des nationalen Rechts zu denken (die nach → Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO ebenfalls Rechtsgrundlagen schaffen können).

Beispiel:

> In dem zuletzt geschilderten Fall spricht viel gegen die Zulässigkeit einer weiteren Verarbeitung zu Werbezwecken. Die betroffene Person hat schließlich mit dem Widerruf ihrer Einwilligung deutlich zum Ausdruck gebracht, dass sie eine solche Verarbeitung nicht

mehr wünscht. Dem stehen keine überwiegenden Interessen des Verantwortlichen gegenüber (vgl. → Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO). Der Widerruf der Einwilligung hat hier eine ähnliche Wirkung wie der Widerspruch gegen eine Verarbeitung zu Zwecken der Direktwerbung, → Art. 21 Abs. 2, Abs. 3 DSGVO.

Das führt zum nächsten Löschgrund: Legt die betroffene Person nach → Art. 21 Abs. 1 DSGVO oder nach → Art. 21 Abs. 2 und 3 DSGVO erfolgreich einen Widerspruch gegen eine Verarbeitung ein, hat der Verantwortliche die betroffenen Daten nach → **Art. 17 Abs. 1 Buchst. c DSGVO** ebenfalls zu löschen.

Beispiel:

Der Verantwortliche sendet der betroffenen Person ein Werbeanschreiben zu. Die betroffene Person widerspricht der Nutzung ihrer Daten zu Werbezwecken. – Der Widerspruch ist auch dann wirksam, wenn die betroffene Person keine Gründe dafür geltend macht. Die Kontaktdaten sind aus dem Datenbestand zu entfernen, der den Werbeanschreiben zugrunde liegt.

Vertiefung:

In dieser Situation kann eine Art „Löschfalle" entstehen: Nehmen Sie an, der Verantwortliche hat personenbezogene Daten bei einem Adresshändler eingekauft. Wenn er diese Daten vollständig löscht und später neue Adressdaten zum Zweck der Direktwerbung einkauft, kann er nicht erkennen, ob diese neu eingekauften Daten auch Personen betreffen, die der Direktwerbung schon einmal widersprochen haben. Dementsprechend wird der Verantwortliche bei einem Widerspruch der betroffenen Person deren Identitätsdaten (Name und Adresse, vielleicht auch Geburtstag) in einer speziellen Sperrdatei speichern dürfen. Diese Datei ist dahin zweckbestimmt, dass sie nur zur Sicherung des Widerspruchsrechts, nicht jedoch im operativen Geschäftsbetrieb eingesetzt werden darf. Bei künftigen Dateneinkäufen kann der Verantwortliche dann die eingekauften Daten mit der Sperrdatei abgleichen, um so die Datensätze von Personen herauszufiltern, die Widerspruch eingelegt haben.

Wurden personenbezogene Daten unrechtmäßig verarbeitet, besteht ein Löschanspruch der betroffenen Person nach → **Art. 17 Abs. 1 Buchst. d DSGVO**.

Beispiel:

Ein Fahrzeughalter montiert an seinem Fahrzeug eine sog. Dashcam. Sie nimmt während Autofahrten permanent Bilddaten von anderen Verkehrsteilnehmern auf; die Aufnahmen sollen im Bedarfsfall als Beweismittel zur Verfügung stehen. – Nach einer Entscheidung des Bundesgerichtshofs spricht viel dafür, dass der Einsatz von Dashcams mit dem Datenschutzrecht nicht in Einklang steht (näher Bundesgerichtshof, Urteil vom 15. Mai 2018, VI ZR 233/17, Rn. 7 ff., noch zur Rechtslage vor der Datenschutzreform 2018). Es besteht also grundsätzlich ein Löschanspruch durch die betroffene Person.

Die beiden weiteren Löschgründe nach → **Art. 17 Abs. 1 Buchst. e und f DSGVO** sollen hier nicht näher behandelt werden. Sie betreffen rechtlich begründete Löschpflichten und den bereits oben nicht behandelten Fall der Ansprache von Kindern im Rahmen eines „Dienstes der Informationsgesellschaft“.

→ Art. 17 Abs. 1 DSGVO beschreibt die Voraussetzungen, unter denen im Grundsatz eine Löschpflicht besteht. Ausnahmen regelt → Art. 17 Abs. 3 DSGVO, im nationalen Recht ist etwa § 84 SGB X zu beachten.

Wie mache ich das Recht auf Löschung geltend? ▪ Ein Antrag auf Löschung personenbezogener Daten muss keine besonderen Formanforderungen erfüllen; Sie müssen allerdings damit rechnen, dass der Verantwortliche Ihre Identität überprüfen möchte (siehe Abschnitt 5.4). Der Antrag sollte die personenbezogenen Daten so genau wie möglich angeben. Er sollte außerdem erkennen lassen, auf welche Löschungsgründe Sie den Antrag stützen möchten.

Beispiel:

> [Widerruf mit Löschungsantrag an eine öffentliche Kultureinrichtung, Löschungsgründe aus → Art. 17 Abs. 1 Buchst. a und b DSGVO] „Ich widerrufe meine Einwilligung in den Bezug Ihres Newsletters und möchte die Angebote Ihrer Einrichtung nicht mehr in Anspruch nehmen. Ich beantrage, den Eintrag in Ihrer Kundendatei zu meiner Person zu löschen.“

Was kann ich vom Verantwortlichen erwarten? ▪ Sie können beim Recht auf Löschung ebenfalls erwarten, dass der Verantwortliche Sie bei der Ausübung Ihres Rechts unterstützt. Er muss über Ihren Antrag unverzüglich entscheiden und eine rechtlich geforderte Löschung von personenbezogenen Daten bewirken.

Manchmal stellen sich Verantwortliche – auch im öffentlichen Sektor – auf den Standpunkt: „Das geht technisch nicht.“ Diese Ausrede geht aber fehl: Der Verantwortliche darf nur technische Verfahren einsetzen, die eine vorschriftsgemäße Löschung zulassen. Das Recht verlangt nichts, was technisch nicht leistbar ist; es lässt aber technische Lösungen nicht zu, die seinen Anforderungen nicht entsprechen. Besteht ein Löschungsanspruch, erfasst dieser grundsätzlich auch Sicherungsdateien, die der Verantwortliche anlegt, um IT-Systeme nach einem „Störfall“ wieder ordnungsgemäß in Betrieb nehmen zu können.

„Recht auf Vergessenwerden“ ▪ → Art. 17 DSGVO enthält nicht nur ein Betroffenenrecht auf Löschung, sondern in → Art. 17 Abs. 2 DSGVO auch das sogenannte „Recht auf Vergessenwerden“. Der Sache nach begründet dieses Recht in Fällen der

Veröffentlichung personenbezogener Daten eine Pflicht des Verantwortlichen, regelmäßige Datenempfänger von dem Löschbegehren der betroffenen Person zu unterrichten.

5.7 Recht auf Einschränkung der Verarbeitung

Nach → Art. 18 DSGVO kann die betroffene Person unter bestimmten Voraussetzungen vom Verantwortlichen verlangen, dass er die Verarbeitung sie betreffender personenbezogener Daten einschränkt. Der Begriff der Einschränkung wird in → Art. 4 Nr. 3 DSGVO definiert. Sie ist „eine Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken."

Was bringt mir das Recht auf Einschränkung der Verarbeitung? ▪ Wenn Sie dieses Recht geltend machen, hat dies – zunächst – keine Folgen für den Datenbestand beim Verantwortlichen. Der Datenbestand wird nicht – wie beim Recht auf Löschung – „verkleinert" oder – wie beim Recht auf Berichtigung – inhaltlich verändert. Die Einschränkung bezieht sich vielmehr auf die Zweckbestimmung der Daten. Eine solche Zweckbestimmung muss der Verantwortliche – wie oben in Abschnitt 4.4 besprochen – für alle Daten in seinem Datenbestand treffen. Verlangt eine betroffene Person nun erfolgreich eine Einschränkung der Verarbeitung, gilt für die Zweckbestimmung → Art. 18 Abs. 2 DSGVO. Von der fortdauernden Speicherung und einer Verarbeitung auf Grundlage einer Einwilligung der betroffenen Person abgesehen, sind andere Verarbeitungen dann nur noch in einem eng begrenzten Umfang zulässig. Ausgeschlossen ist grundsätzlich insbesondere die Verarbeitung mit der ursprünglichen Zweckbestimmung.

Die betroffenen Daten werden durch die Einschränkung ihrer Verarbeitung also in eine Art datenschutzrechtlichen „Winterschlaf" versetzt. Im Ergebnis bringt das Recht auf Einschränkung der Verarbeitung nicht ganz so viel wie eine Löschung; allerdings sind die Daten auch nicht „weg". An das Recht auf Einschränkung der Verarbeitung sollten Sie daher insbesondere dann denken, wenn es in Ihrem Interesse liegt, dass der Verantwortliche mit den Daten zu einem späteren Zeitpunkt wieder arbeiten kann.

Welche Voraussetzungen müssen erfüllt sein? ▪ Eine Einschränkung der Verarbeitung kann die betroffene Person verlangen, wenn ein „Einschränkungsgrund" nach → Art. 18 Abs. 1 Buchst. a bis d DSGVO gegeben ist.

Zwei Einschränkungsgründe, nämlich → Art. 18 Abs. 1 Buchst. a und d DSGVO zielen auf den „Winterschlaf" während einer Zeit, in der eine betroffene Person und der Verantwortliche klären, wie mit dort vorhandenen personenbezogenen Daten weiter zu

verfahren ist. Im Fall von → **Art. 18 Abs. 1 Buchst. a DSGVO** wird die betroffene Person meist ein Berichtigungsrecht nach → Art. 16 DSGVO geltend gemacht haben. Der Verantwortliche muss dann für sich klären, ob er die Daten auch für unrichtig hält, und er muss über den Antrag entscheiden. Bis zu einer Berichtigung bietet die Einschränkung der Verarbeitung eine vorläufige Regelung, die den Interessen der betroffenen Person möglichst weitgehend entgegenkommt.

Beispiel:

> Der Beamte B. hat einen Auszug aus dem seine Person betreffenden Datensatz im Personal- und Stellenverwaltungsverfahren VIVA-PSV erhalten. Die Angaben stimmen nicht in jeder Hinsicht mit der erlebten Biografie überein. B. stellt die Abweichungen zusammen, in manchen Punkten kann er auf seine Personalakte verweisen, in anderen legt er der personalverwaltenden Stelle Nachweise vor. – Die personalverwaltende Stelle muss erst einmal prüfen, was von dem Antrag des B. zu halten ist und inwieweit sie seinen VIVA-PSV-Datensatz berichtigen muss. Das kann einige Zeit dauern. Für diese Zeit könnte B. insofern eine Einschränkung der Verarbeitung beantragen. Das wird er aber nur tun, wenn der Datensatz unrichtige Angaben enthält, die für B. ungünstig sind.

Der Einschränkungsgrund des → **Art. 18 Abs. 1 Buchst. d DSGVO** kommt ebenfalls in einer Situation zum Tragen, in der Sie ein Betroffenenrecht ausgeübt haben: nämlich das Widerspruchsrecht (siehe dazu Abschnitt 5.9). In einem solchen Fall muss der Verantwortliche grundsätzlich (→ Art. 21 Abs. 1 DSGVO) die von Ihnen vorgebrachten Gründe prüfen. Auch dafür kann er eine gewisse Zeit benötigen, insbesondere wenn Rückfragen zu stellen sind oder der Sachverhalt einer weiteren Aufklärung bedarf. Für diesen Zeitraum können Sie ebenfalls eine Einschränkung der Verarbeitung verlangen.

Beispiel:

> Ein kommunaler Wasserversorger baut einen elektronischen Wasserzähler in das Haus einer Bürgerin ein. Der Wasserzähler übermittelt punktgenau die Verbrauchsdaten der Bürgerin an den kommunalen Wasserversorger. Die Bürgerin will das unterbinden. – Möglicherweise kann die Bürgerin aufgrund einer besonderen Situation (siehe dazu Abschnitt 5.9) einer solchen Datenerfassung durch einen digitalen Wasserzähler nach → Art. 21 Abs. 1 DSGVO widersprechen. In der Regel wird der Wasserversorger die Argumentation der Bürgerin überprüfen müssen. Für die Dauer einer solchen Überprüfung muss er die erfassten Daten nicht löschen, er muss sie aber nach → Art. 18 Abs. 1 Buchst. d DSGVO einschränken. Das bedeutet konkret: Der Versorger darf die Daten zwar speichern. Er darf sie aber nur zu den sehr eingeschränkten Zwecken verarbeiten, etwa, soweit dies zur Behebung einer Störung in der Trinkwasserversorgung erforderlich ist (Suche nach einem Rohrbruch).

Beabsichtigt der Verantwortliche die Einschränkung aufzuheben, muss er die betroffene Person vorher informieren, → Art. 18 Abs. 3 DSGVO.

Beispiel:

Der Wasserversorger hat den Widerspruch der Bürgerin überprüft. Er hält ihre Begründung nicht für stichhaltig und beabsichtigt deshalb, die Wasserzählerdaten weiter zu nutzen.

Ach, übrigens:

In Bayern hat der Gesetzgeber die Verarbeitung personenbezogener Daten mithilfe von digitalen Wasserzählern – unbeschadet des Widerspruchsrechts nach → Art. 21 DSGVO – in Art. 24 Abs. 4 Gemeindeordnung besonders geregelt. Dort ist auch ein gegenüber → Art. 21 DSGVO eigenständiges – Widerspruchsrecht normiert. Zu den rechtlichen Hintergründen im Einzelnen: Bayerischer Landesbeauftragter für den Datenschutz, 28. Tätigkeitsbericht 2018, Nr. 7.3 (im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Tätigkeitsberichte").

Die beiden anderen Einschränkungsgründe, → **Art. 18 Abs. 1 Buchst. b und c DSGVO**, betreffen Situationen, in denen „eigentlich" auch das Recht auf Löschung ausgeübt werden könnte: Vorausgesetzt wird nämlich, dass der Verantwortliche personenbezogene Daten nicht mehr benötigt (Löschung nach → Art. 17 Abs. 1 Buchst. a DSGVO) oder unrechtmäßig verarbeitet (Löschung nach → Art. 17 Abs. 1 Buchst. d DSGVO). Eine betroffene Person kann hier „ersatzweise" eine Einschränkung der Verarbeitung verlangen. Das kann insbesondere dann sinnvoll sein, wenn die Daten später noch einmal benötigt werden und der Aufwand einer Neuerhebung vermieden werden soll, oder wenn sich die betroffene Person noch nicht zu einem Löschungsantrag entschließen will. Jedenfalls wenn der Verantwortliche rechtmäßig verarbeitete Daten nicht mehr benötigt, muss er dem Anliegen der betroffenen Person aber nur entsprechen, wenn diese das in → Art. 18 Abs. 1 Buchst. c DSGVO umschriebene (Beweis-)Interesse geltend machen kann. Der Verantwortliche ist nämlich nicht nur verpflichtet, nicht mehr benötigte Daten zu löschen, sondern auch berechtigt. Er muss grundsätzlich nicht Speicherressourcen für personenbezogene Daten bereitstellen, die für ihn nicht mehr relevant sind.

Wie mache ich das Recht auf Einschränkung der Verarbeitung geltend? ▪ Sie richten einen formlosen Antrag an den Verantwortlichen. Darin sollten Sie die personenbezogenen Daten bezeichnen, auf die sich die Einschränkung beziehen soll. Dies gilt insbesondere dann, wenn nur ein Teil des zu Ihrer Person verfügbaren Datenbestandes beim Verantwortlichen betroffen ist. Ferner sollten Sie den Einschränkungsgrund darlegen. Im Fall von → Art. 18 Abs. 1 Buchst. a DSGVO ist es sinnvoll, den

Einschränkungsantrag mit dem Berichtigungsantrag (→ Art. 16 DSGVO, siehe Abschnitt 5.5) zu verbinden, im Fall von Art. → 18 Abs. 1 Buchst. d DSGVO mit dem Widerspruch (→ Art. 21 DSGVO, siehe Abschnitt 5.9). Wird das Recht auf Einschränkung der Verarbeitung in einer „Löschungssituation" geltend gemacht (→ Art. 18 Abs. 1 Buchst. b und d DSGVO), empfiehlt es sich, die entsprechenden Löschungsgründe darzulegen (dazu näher Abschnitt 5.5).

Was kann ich vom Verantwortlichen erwarten? • Sie können zunächst Unterstützung bei Ihrem Anliegen verlangen. Richtet sich der Antrag gegen eine bayerische öffentliche Stelle, ist es ratsam, mit der oder dem behördlichen Datenschutzbeauftragten Kontakt aufzunehmen. Sie oder er kann Ihnen nicht nur das Stellen interessegerechter Anträge erleichtern, sondern auch die jeweilige Fachstelle anleiten. Der Verantwortliche muss Ihrem Antrag auch unverzüglich nachkommen. Dabei ist für → Art. 18 Abs. 1 Buchst. a und d DSGVO zu beachten, dass ein vorläufiger Zustand geregelt werden soll. Benötigt der Verantwortliche Zeit, um die Richtigkeit von personenbezogenen Daten (→ Art. 18 Abs. 1 Buchst. a DSGVO) oder die Gründe für einen Widerspruch (→ Art. 18 Abs. 1 Buchst. d DSGVO) zu prüfen, so kann er nicht (auch noch) die Einschränkung der Verarbeitung zurückstellen. Er kann diese aber (jedenfalls) dann ablehnen, wenn die Daten offensichtlich nicht unrichtig oder die Gründe für den Widerspruch offenkundig nicht tragfähig sind.

5.8 Recht auf Datenübertragbarkeit

Ein ganz neues Betroffenenrecht begründet → Art. 20 DSGVO: Das Recht auf Datenübertragbarkeit. Es dürfte vor allem auf Soziale Netzwerke abzielen. Verlässt die betroffene Person ein Soziales Netzwerk, kann sie von der Anbieterin oder dem Anbieter verlangen, die sie betreffenden Daten in einem gängigen, strukturierten Format zu erhalten. Falls sie wechselt, kann sie auch verlangen, dass die sie betreffenden Daten der neuen Anbieterin oder dem neuen Anbieter direkt übermittelt werden.

Allerdings kann sich eine betroffene Person nur auf das Recht auf Datenübertragbarkeit berufen, wenn die Verarbeitung auf einer Einwilligung oder einem Vertrag beruht. Zudem muss die Verarbeitung mithilfe automatisierter Verfahren erfolgen und die Daten müssen von der betroffenen Person selbst dem Verantwortlichen zur Verfügung gestellt worden sein.

Alles in Allem ist derzeit noch unklar, welche praktische Bedeutung das Recht auf Datenübertragbarkeit – gerade im Bereich der bayerischen öffentlichen Verwaltung – erlangen wird.

5.9 Widerspruchsrecht

Das Widerspruchsrecht nach → Art. 21 Abs. 1 Satz 1 DSGVO soll einer betroffenen Person die Möglichkeit geben, im Hinblick auf eine rechtmäßige (!) Verarbeitung ihre besondere Situation geltend zu machen. Zuweilen kann nämlich eine an sich zulässige Verarbeitung für die betroffene Person im Vergleich mit anderen, ähnlichen Verarbeitungen als erheblich belastender erscheinen. In einem solchen Fall erhöht das Widerspruchsrecht zunächst einmal die „Begründungslast" des Verantwortlichen.

Was bringt mir das Widerspruchrecht? ▪ Wie die aufsichtsbehördliche Praxis zeigt, sind mit dem Widerspruchsrecht gelegentlich Erwartungen verbunden, die das Gesetz nicht erfüllen kann. Zwei Dinge sollten Sie hier insbesondere beachten:

- Das Widerspruchsrecht verschafft Ihnen nicht das Recht, dem Verantwortlichen die Verarbeitung Ihrer personenbezogenen Daten zu untersagen. Ob eine Verarbeitung rechtmäßig ist, bestimmt das Gesetz; maßgeblich ist hier im Grundsatz → Art. 6 Abs. 1 DSGVO (siehe Abschnitt 4.1). Liegt ein begründeter Widerspruch vor, darf der Verantwortliche Ihre Daten zwar im Grundsatz zukünftig nicht mehr verarbeiten. In den von → Art. 21 Abs. 1 Satz 2 DSGVO bezeichneten Fällen darf er die Verarbeitung aber trotz des Widerspruchs fortsetzen. Das muss der Verantwortliche im Einzelfall prüfen. Bei Verarbeitungen auf Grund hoheitlicher Verarbeitungsbefugnisse (→ Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO) wird der Verantwortliche auch einer durch → Art. 21 Abs. 1 Satz 2 DSGVO gesteigerten „Begründungslast" häufig entsprechen können.
- Ein Widerspruch hat ohne eine Begründung regelmäßig keinen Erfolg. Etwas anderes gilt nur, wenn sich die betroffene Person gegen eine Nutzung ihrer Daten zum Zweck der Direktwerbung wehrt (→ Art. 21 Abs. 2 und 3 DSGVO). Das Widerspruchsrecht dient der Bewältigung von „Sondersituationen", die bei einer sorgfältigen gesetzlichen Regelung von Verarbeitungen nicht alle vorhergesehen und schon durch den Gesetzgeber „eingeplant" werden können.

Soweit Sie allerdings eine „Sondersituation" darlegen können, muss der Verantwortliche darauf eingehen und prüfen, ob er eine Verarbeitung noch fortführen kann; kann er der gesteigerten „Begründungslast" nicht nachkommen, muss er die Verarbeitung unterlassen. In diesem Fall haben Sie durch Ihren Widerspruch die weitere Verarbeitung unterbunden; auf zurückliegende Verarbeitungen hat der Widerspruch keinen Einfluss.

Welche Voraussetzungen müssen erfüllt sein? ▪ → Art. 21 Abs. 1 DSGVO sieht zunächst vor, dass ein Widerspruch nur in Bezug auf Verarbeitungen statthaft ist, die der Verantwortliche auf → Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO (Verarbeitung im

öffentlichen Interesse) oder auf → Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO (Verarbeitung auf Grundlage einer Interessenabwägung) stützt. Ist eine Verarbeitung auf eine Einwilligung gestützt (→ Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO), benötigen Sie das Widerspruchsrecht nicht, weil Sie die Einwilligung widerrufen können (siehe Abschnitt 4.1.1). In den Fällen von → Art. 6 Abs. 1 UAbs. 1 Buchst. b und c DSGVO ist anzunehmen, dass die vertragliche Regelung oder die rechtliche Verpflichtung, auf der die Verarbeitung beruht, „Sondersituationen" bereits Rechnung trägt.

Im Fall von → Art. 21 Abs. 1 DSGVO muss die betroffene Person ihren Widerspruch mit Gründen belegen, die sich aus ihrer besonderen Situation ergeben. Der Widerspruch wird insbesondere auf eine Interessenlage der betroffenen Person hinweisen, die vom „Normalfall" abweicht und/oder dem Verantwortlichen (so) nicht bekannt ist. Insofern kommt es auf Argumente an, die für eine (atypisch) höhere Gewichtung Ihrer Interessen sprechen, auf Aspekte, die dem Verantwortlichen bisher verborgen geblieben waren oder die für eine besondere Schutzbedürftigkeit Ihrer Person im Vergleich mit Anderen sprechen.

Wie erhebe ich Widerspruch? ▪ Sie stellen beim Verantwortlichen den Antrag, bestimmte, möglichst konkret bezeichnete personenbezogene Daten von Ihnen nicht mehr zu verarbeiten. Der Antrag bedarf keiner besonderen Form. Vor dem oben dargelegten Hintergrund sollten Sie zur Begründung möglichst viele Argumente zusammenstellen, die Ihre „Sondersituation" begründen. Hilfreich ist es, auf Grund der Datenschutzhinweise des Verantwortlichen sowie durch Ausübung des Auskunftsrechts herauszufinden, auf welche Rechtsgrundlage der Verantwortliche die Verarbeitung stützt und welche Informationen er der Prüfung ihrer Rechtmäßigkeit (bereits) zugrunde legen konnte.

Was kann ich vom Verantwortlichen erwarten? ▪ Der Verantwortliche muss Ihren Antrag unverzüglich prüfen. Liegt die vom Gesetz geforderte besondere Situation vor, darf der Verantwortliche die personenbezogenen Daten nur noch verarbeiten, wenn überwiegende „zwingende schutzwürdige Gründe" für die Verarbeitung sprechen oder wenn die Verarbeitung der Wahrung von Rechtsansprüchen dient.

Sonderfall: Verarbeitung zum Zweck der Direktwerbung ▪ Verarbeitet der Verantwortliche personenbezogene Daten allerdings lediglich zu Zwecken der Direktwerbung, muss die betroffene Person ihren Widerspruch nicht begründen. Ihr einer Werbung entgegenstehender Wille genügt nach → Art. 21 Abs. 2, Abs. 3 DSGVO, um das berechtigte Interesse des Verantwortlichen an einer Direktwerbung auszuschalten.

5.9.1 Wie unterbinden Sie Auskünfte aus dem Melderegister?

Ärgern Sie sich in Wahlkampfzeiten über persönliche Zuschriften von Parteien, die Sie politisch nie unterstützen würden? Dann sollten Sie in Erwägung ziehen, in Bezug auf Melderegisterdaten eine Übermittlungssperre einzurichten.

In Deutschland sind Melderegister amtliche Verzeichnisse, die den Aufenthalt von Personen dokumentieren. Ein Melderegister enthält unter anderem Angaben zu Ihrer Identität, zu Ihren Kontaktdaten, zu Ihrem Familienstand oder zu Ihrer Religionszugehörigkeit. Die Melderegister werden von den Meldebehörden, in der Regel den Gemeinden geführt („Einwohnermeldeamt" oder „Meldestelle"). Die Melderegister dienen dazu, unter gesetzlich bestimmten Voraussetzungen Daten von Ihnen an andere, insbesondere öffentliche Stellen zu übermitteln. Sie ermöglichen jedoch auch die Auskunft an Private, etwa im Fall der sogenannten „einfachen Melderegisterauskunft", die nicht an ein berechtigtes Interesse gebunden, sondern nur von der Zahlung einer Gebühr abhängig ist.

Mit einer „Übermittlungssperre" können Sie die Weitergabe Ihrer Meldedaten an bestimmte Stellen ausschließen (§ 9 Satz 1 Nr. 5, § 50 Abs. 5 BMG), und zwar

- Auskünfte an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen vor Wahlen oder Abstimmungen (siehe dazu die FAQ auf https://www.datenschutz-bayern.de in der Rubrik „Themengebiete – Kommunales – Bürger können sich gegen Wahlwerbung schützen");
- bestimmte Auskünfte über Alters- und Ehejubiläen (siehe dazu Bayerischer Landesbeauftragter für den Datenschutz, Melderegisterdaten und Gratulationen, Aktuelle Kurz-Information 5, im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen");
- Auskünfte an Adressbuchverlage (siehe dazu die FAQ auf https://www.datenschutz-bayern.de in der Rubrik „Themengebiete – Kommunales – Bürger können der Weitergabe ihrer Meldedaten an Adressbuchverlage widersprechen");

Auch bestimmte Datenübermittlungen an öffentlich-rechtliche Religionsgemeinschaften sowie an das Bundesamt für Personalmanagement der Bundeswehr können durch entsprechende Erklärungen unterbunden werden. Eine Übermittlungssperre hinsichtlich einer Weitergabe von Meldedaten an den „ARD ZDF Deutschlandradio Beitragsservice" (früher „Gebühreneinzugszentrale") ist dagegen nicht möglich, siehe dazu ausführlich Bayerischer Landesbeauftragter für den Datenschutz, 27. Tätigkeitsbericht 2016, Nr. 6.17 (im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Tätigkeitsberichte").

Der Eintrag einer Übermittlungssperre ist kostenfrei. Er kann bei der örtlichen Meldebehörde gestellt werden. Manche Gemeinden bieten die Einrichtung einer Übermittlungssperre auch online auf ihrer Webseite an.

Tipp:

> Falls Sie mehrere Wohnsitze haben, müssen Sie beachten, dass eine Übermittlungssperre nur für den Wohnsitz gilt, bei dem Sie die Übermittlungssperre eingerichtet haben. Wenn Sie eine Datenübermittlung für alle Wohnsitze ausschließen wollen, müssen Sie Übermittlungssperren bei allen für Ihre Wohnsitze zuständigen Meldebehörden einrichten lassen.

Ach, übrigens:

> Das Bundesmeldegesetz sieht vor, dass Meldebehörden einfache Melderegisterauskünfte an Unternehmen nur erteilen dürfen, wenn diese ausdrücklich versichern, dass die Auskunft nicht für Zwecke der Werbung und des Adresshandels verwendet wird oder wenn Sie in eine solche Verwendung eingewilligt haben. Eine solche Einwilligung können Sie gegenüber der Meldebehörde oder gegenüber der Auskunft verlangenden Person erklären – und auch jederzeit widerrufen.

Eine Unterbindung von Melderegisterauskünften – insbesondere an Privatpersonen – kann grundsätzlich nur durch eine Auskunftssperre erreicht werden (§ 51 BMG), die nicht mit der Übermittlungssperre zu verwechseln ist. Eine Auskunftssperre setzt „Tatsachen [voraus], die die Annahme rechtfertigen, dass der betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann". Ein entsprechender Antrag muss eingehend begründet werden; die Meldebehörden verlangen meist Nachweise für die Gefahrenlage, etwa polizeiliche Ermittlungsberichte.

Beispiele:

> Eine Staatsanwältin ermittelt im Bereich der Schwerkriminalität und wird konkret bedroht. – Eine betroffene Person wird „gestalkt"; andere Maßnahmen als ein heimlicher Wohnortwechsel waren bisher erfolglos.

5.9.2 Mitgliedergewinnung bei Krankenkassen

Gesetzliche Krankenkassen dürfen nur nach Maßgabe von § 284 Abs. 4 Satz 1 Fünftes Buch Sozialgesetzbuch (SGB V) „allgemein zugängliche Daten" zur Gewinnung von neuen Mitgliedern verarbeiten. „Allgemein zugänglich" sind beispielsweise im Telefonbuch veröffentlichte oder im Internet frei verfügbare Daten. Die Daten dürfen mit dem Versichertenverzeichnis abgeglichen werden, um bereits versicherte Personen von der Mitgliederwerbung auszuschließen.

Sie haben die Möglichkeit, bei der Krankenkasse einer Verarbeitung formlos und ohne Begründung zu widersprechen. Die Krankenkasse darf Ihre Daten dann nicht mehr für die Mitgliederwerbung nutzen, § 284 Abs. 4 Satz 3 SGB V.

5.10 Recht auf Abwehr automatisierter Entscheidungen im Einzelfall

Das in → Art. 22 DSGVO geregelte Betroffenenrecht reagiert auf eine Bedrohung, die das Datenschutzgrundrecht durch den Rückzug des Menschen als Entscheidungsträger in der digitalisierten Welt erfährt. Die betroffene Person soll nicht „Spielball" in Entscheidungen sein, die ausschließlich von informationstechnischen Systemen aufgrund der Anwendung von Algorithmen getroffen werden.

Beispiel:

> Ein Verbraucher stellt einen Kreditantrag. Die Bank fragt bei einer Wirtschaftsauskunftei an, die den Verbraucher mittels eines automatisierten Scoringverfahrens bewertet. Das Ergebnis fällt so aus, dass die Bank entsprechend ihren internen Richtlinien keinen Kredit vergeben kann. Der Verbraucher hatte keine Möglichkeit, irgendwem irgendetwas zu erklären. Er wird letztlich mit dem „Urteil" einer Maschine konfrontiert – und zwar in aller Regel auch noch ohne zu erfahren, wie dieses überhaupt zustande gekommen ist.

Automatisierte Entscheidungen beruhen gegenwärtig noch regelmäßig auf statistischen Erfahrungen. Sie führen in typischen Situationen zu brauchbaren Ergebnissen, mitunter jedoch nicht, wenn eine Situation nicht in das „Raster" passt, das dem automatisierten Entscheidungsprozess zugrunde liegt. In solchen Fällen kann eine betroffene Person Nachteile erleiden, weil die Besonderheiten ihrer individuellen Lage ausgeblendet werden.

Vor diesem Hintergrund bestimmt → Art. 22 Abs. 1 DSGVO, dass die betroffene Person das Recht hat, nicht einer automatisierten Entscheidung unterworfen zu werden, die „ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Wirkung erheblich beeinträchtigt." Dieses grundsätzliche Verbot einer automatisierten Einzelfallentscheidung gilt jedoch nicht in den Fällen des → Art. 22 Abs. 2 DSGVO.

Beispiel:

> Der Verantwortliche aus dem vorigen Beispiel holt eine ausdrückliche Einwilligung der betroffenen Person für die Durchführung eines Scoringverfahrens ein. Er muss dann durch technische und organisatorische Maßnahmen dafür sorgen, dass die berechtigten Interessen der betroffenen Personen angemessen geschützt werden, insbesondere sicherstellen, dass eine automatisierte Entscheidung in einer Begegnung „Mensch-zu-Mensch" hinterfragt werden kann.

Besonders strenge Anforderungen sind im Übrigen zu erfüllen, wenn automatisierte Entscheidungen auf sensiblen Daten beruhen (können), → Art. 22 Abs. 4 DSGVO.

5.11 Recht auf Beschwerde bei der Datenschutz-Aufsichtsbehörde

Das Recht auf Beschwerde bei einer Datenschutz-Aufsichtsbehörde ist in → Art. 77 Abs. 1 DSGVO geregelt. Es dient neben anderen Zwecken einer Durchsetzung der in → Art. 15 bis 22 DSGVO geregelten Betroffenenrechte. Sie können daher eine Beschwerde bei der Datenschutz-Aufsichtsbehörde auch mit dem Vorbringen begründen, ein Verantwortlicher komme von Ihnen geltend gemachten Betroffenenrechten nicht oder nicht zureichend nach. Das Beschwerderecht ist in Abschnitt 6 näher erläutert.

5.12 Beschränkung von Betroffenenrechten

Bereits wiederholt ist deutlich geworden, dass die Datenschutz-Grundverordnung einheitliche Verarbeitungsstandards für Verarbeitungen festlegt, die rein wirtschaftlichen Interessen dienen. Im Gegensatz dazu eröffnet die Datenschutz-Grundverordnung für die Verarbeitung personenbezogener Daten im öffentlichen Interesse gewisse Konkretisierungsspielräume. Gleiches gilt für die Betroffenenrechte.

Schweigt der nationale Gesetzgeber eines Mitgliedstaats, bleibt es bei den Betroffenenrechten, wie sie in der Datenschutz-Grundverordnung in den → Art. 12 bis 22 DSGVO geregelt sind. Der nationale Gesetzgeber kann allerdings bei Verarbeitungen im öffentlichen Interesse die Betroffenenrechte einschränken, wenn diese Beschränkung a) den Wesensgehalt der Grundrechte und Grundfreiheiten achtet, b) eine „in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme darstellt und c) dabei ein Ziel verfolgt, das im Katalog des → Art. 23 Abs. 1 DSGVO enthalten ist.

Wie bereits in Abschnitt 5.4.2 dargestellt, sieht das Bayerische Datenschutzgesetz solche Beschränkungen vor allem bei der Informationspflicht und beim Auskunftsrecht vor, → Art. 9, 10 BayDSG. Beschränkungen finden sich ferner etwa in §§ 83 und 84 SGB X.

6 Datenschutzaufsicht und Rechtsbehelfe

Der Erlass von Datenschutzrecht ist eine Sache, die Beachtung des Datenschutzrechts eine andere. Diese Erfahrung haben die nationalen Gesetzgeber recht bald nach dem Erlass der ersten Datenschutzgesetze gemacht.

Beispiel:

> Das Datenschutzübereinkommen des Europarats (siehe Abschnitt 5 am Anfang) enthielt zwar Datenschutzprinzipien, aber noch keine Vereinbarung zur Einrichtung einer unabhängigen Datenschutzkontrolle. Diese wurde nachträglich durch ein Zusatzprotokoll eingeführt.

Nach der Datenschutz-Grundverordnung sind die Datenschutz-Aufsichtsbehörden völlig unabhängig, → Art. 52 DSGVO. Eine Aufsicht kann wirksam sein, wenn der Verantwortliche oder der Auftragsverarbeiter einsichtig ist. Ist er es nicht, benötigen die Datenschutz-Aufsichtsbehörden allerdings auch Befugnisse, die es ihnen ermöglichen, Beschwerdefälle zu untersuchen und Datenschutzverstöße abzustellen. Dementsprechend sieht → Art. 58 Abs. 1 DSGVO diverse **Untersuchungsbefugnisse** und → Art. 58 Abs. 2 DSGVO bestimmte **Abhilfebefugnisse** der Datenschutz-Aufsichtsbehörden vor.

Abhilfebefugnisse lösen regelmäßig konkrete Einzelfälle. Bei fehlender Einsicht der Datenverarbeiter wirken sie allerdings nur bedingt präventiv.

Beispiel:

> Die Datenschutz-Aufsichtsbehörde untersagt einem Unternehmen, seine Belegschaft mithilfe von Kameras zu überwachen. Das Unternehmen baut die Kameras zwar ab. Kurze Zeit später jedoch richtet es wieder Videoüberwachung ein.

Die Datenschutz-Aufsichtsbehörde müsste dann erneut ein Verbotsverfahren einleiten. Die Abhilfebefugnisse werden durch **Sanktionsbefugnisse** ergänzt, → Art. 83 DSGVO. Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein, wie → Art. 84 DSGVO ausdrücklich festhält. Die in → Art. 83 DSGVO vorgesehenen Bußgelder können im Extremfall sehr schmerzhaft sein, sie reichen bis zu 20 Millionen Euro bzw. 4 % des Weltjahresumsatzes eines Unternehmens.

Von Gesetzes wegen kann der Bayerische Landesbeauftragte für den Datenschutz (im Folgenden: Landesbeauftragter) gegen öffentliche Stellen Geldbußen allerdings nur verhängen, soweit sie als „Unternehmen am Wettbewerb" teilnehmen (vgl.

→ Art. 83 DSGVO, näher Bayerischer Landesbeauftragter für den Datenschutz, Geldbußen nach Art. 83 Datenschutz-Grundverordnung gegen bayerische öffentliche Stellen, Aktuelle Kurz-Information 17, im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen").

Beispiele:

> Am Wettbewerb nehmen etwa viele öffentliche Krankenhäuser und Pflegeeinrichtungen sowie Stadt- oder Gemeindewerke teil (Ausnahme aber insbesondere: die öffentliche Wasserversorgung).

Der Wortlaut der Datenschutz-Grundverordnung legt die Annahme nahe, dass die Sanktion die Regel und die sanktionsfreie Abhilfe die Ausnahme ist. Im Vollzug der Datenschutz-Grundverordnung ist es eher umgekehrt: Zumindest in der ersten Zeit der Geltung der Datenschutz-Grundverordnung haben die Datenschutz-Aufsichtsbehörden jedenfalls in Deutschland eher zurückhaltend Bußgelder verhängt.

Beispiel:

> Die portugiesische Datenschutz-Aufsichtsbehörde hat vor einiger Zeit ein Bußgeld in Höhe von 400.000 Euro gegen eine Klinik verhängt, die massiv gegen ihre Verpflichtung zu technisch-organisatorischen Maßnahmen verstoßen hatte. Unter anderem beschäftigt die Klinik zwar nur knapp 300 Ärztinnen und Ärzte, hatte aber über 900 Personen entsprechende Zugriffsrechte Ärzten auf das Klinikinformationssystem gestattet. – Hier verstieß die Klinik offenkundig gegen die Vorgaben des → Art. 32 Abs. 1 Buchst. b DSGVO. Damit verbunden war die massenhafte Offenlegung sensibler Gesundheitsdaten gegenüber nichtberechtigten Personen.

Sie sind der Auffassung, dass eine Verarbeitung Ihrer personenbezogenen Daten durch eine bayerische öffentliche Stelle (Behörde) gegen die Datenschutz-Grundverordnung oder andere datenschutzrechtliche Vorschriften verstößt? Dann können Sie eine Beschwerde beim Landesbeauftragten einreichen.

6.1 Was müssen Sie bei einer Beschwerde beachten?

Die Beschwerde ist grundsätzlich formlos und kostenfrei. Sie erleichtern allerdings die Bearbeitung sehr, wenn Sie die Beschwerde schriftlich formulieren. Bitte nutzen Sie möglichst hierzu das elektronische Beschwerdeformular. Sie finden es im Internet auf https://www.datenschutz-bayern.de in der Rubrik „Online-Meldungen".

Schildern Sie bitte den Sachverhalt, der nach Ihrer Einschätzung mit dem Datenschutzrecht nicht in Einklang steht. In der Regel empfiehlt es sich, den Sachverhalt

der zeitlichen Abfolge nach darzustellen. Besitzen Sie Unterlagen, die Ihre Schilderung untermauern? Dann kann es sinnvoll sein, Ihrer Beschwerde Kopien beizufügen oder bei einer Online-Beschwerde entsprechende Dateien hochzuladen. Das elektronische Beschwerdeformular sieht eine solche Möglichkeit vor.

Bitte teilen Sie in Ihrer Eingabe auch mit, ob Sie gegebenenfalls mit einer Abgabe an eine andere Datenschutz-Aufsichtsbehörde einverstanden sind, wenn der Landesbeauftragte nicht zuständig sein sollte.

Mit einer Beschwerde können Sie nur Verletzungen Ihrer eigenen Datenschutzrechte geltend machen. Selbstverständlich können Sie sich bei der Formulierung der Beschwerde von anderen helfen lassen.

Teilen Sie einen Sachverhalt mit, bei dem Sie nicht selbst betroffen sind? Dann kann der Landesbeauftragte den Vorgang zum Anlass für eine Überprüfung nehmen. Sie haben allerdings darauf keinen Anspruch, im Falle eines Tätigwerdens auch nicht auf die Mitteilung des Ergebnisses.

Beispiel:

> Die G. erwarb in den sechziger Jahren von einer bayerischen Stadt günstig ein Grundstück und errichtete darauf ein Einfamilienhaus. Die Stadt verwahrt den Grundstückskaufvertrag mittlerweile im Stadtarchiv. Ein entsprechender Datensatz in der Erschließungsdatenbank wurde nun im Internet bereitgestellt. Darin finden sich neben dem Namen der G. und der Lage des Grundstücks auch dessen Größe sowie der damalige Kaufpreis. Empört wendet sich der Ehemann der G. an den Landesbeauftragten und rügt eine schwerwiegende Datenschutzverletzung zum Nachteil seiner Frau.
>
> Der Landesbeauftragte wird den Ehemann der G. darauf aufmerksam machen, dass nur diese selbst eine Verletzung ihrer eigenen Datenschutzrechte geltend machen kann. Davon unabhängig wird er die Eingabe zum Anlass nehmen, das Veröffentlichungsverhalten des Stadtarchivs zu überprüfen. Handelt es sich bei dem Eintrag in der Erschließungsdatenbank nicht um einen Einzelfall, wird er insgesamt auf eine datenschutzgerechte Bereinigung hinwirken.

6.2 Wie läuft ein Beschwerdeverfahren üblicherweise ab?

Sobald Ihre Beschwerde beim Landesbeauftragten vorliegt, prüft dieser anhand Ihrer Schilderung, ob ein Datenschutzverstoß möglich erscheint.

Ergibt sich bereits aus Ihrer Schilderung, dass die öffentliche Stelle datenschutzkonform gehandelt hat, wird Ihnen dies kurz erläutert. Falls der Landesbeauftragte den Sachverhalt ohne weitere Informationen nicht beurteilen kann, wird er Sie bitten, Ihre

Schilderung zu ergänzen und unter Umständen aussagekräftige Unterlagen beizufügen. Hierzu sind Sie selbstverständlich nicht verpflichtet.

Erscheint aufgrund Ihrer –gegebenenfalls ergänzten – Schilderung ein Datenschutzverstoß als möglich, fordert der Landesbeauftragte die betroffene öffentliche Stelle zur Abgabe einer Stellungnahme auf. Bisweilen wird er sich im Rahmen einer Vor-Ort-Prüfung ein eigenes Bild von der Verarbeitung machen.

Manchmal können die zur Sachverhaltsaufklärung erforderlichen Fragen nur gestellt werden, wenn Ihr Name und der von Ihnen geschilderte Sachverhalt offengelegt werden. In diesem Fall holt der Landesbeauftragte in aller Regel Ihr Einverständnis ein, sofern Sie dieses nicht bereits mitgeteilt haben. Sie können frei über das Einverständnis entscheiden: Falls Sie eine Offenlegung Ihrer Identität nicht wünschen, wird der Landesbeauftragte Ihren Wunsch selbstverständlich respektieren. Dies kann allerdings dazu führen, dass ein Datenschutzverstoß nicht festgestellt werden kann und Ihre Beschwerde deshalb erfolglos bleibt.

Die öffentlichen Stellen sind verpflichtet, dem Landesbeauftragten die gewünschten Auskünfte zu erteilen. Der damit verbundene Schriftwechsel kann mitunter mehrere Wochen oder – insbesondere bei (wiederholten) Nachfragen – mehrere Monate in Anspruch nehmen. Bitte haben Sie insoweit etwas Geduld. Im Rahmen der Sachverhaltsaufklärung können auch Unterlagen eingesehen oder eine örtliche Prüfung bei der öffentlichen Stelle durchgeführt werden.

Sobald alle notwendigen Informationen vorliegen, wird der Landesbeauftragte den Sachverhalt abschließend bewerten. Wird ein Datenschutzverstoß festgestellt, entscheidet er darüber, welche Maßnahmen er gegenüber der öffentlichen Stelle trifft. Sie erhalten über das Ergebnis der Prüfung Nachricht.

Hierzu gibt es allerdings einige Ausnahmen.

Beispiel:

> Sie wünschen vom Landesamt für Verfassungsschutz eine Auskunft über die Sie betreffenden Daten. Diese Auskunft wird Ihnen verweigert, weil die Verfassungsschutzbehörde meint, dass hierdurch die Sicherheitslage gefährdet wird. In einem solchen Fall prüft der Landesbeauftragte, ob die Auskunft zu Recht verweigert wird; sind Speicherungen vorhanden, prüft er zudem deren Rechtmäßigkeit. Sie erhalten in einem solchen Fall von Gesetzes wegen keine Informationen, die Rückschlüsse auf den Erkenntnisstand des Landesamts für Verfassungsschutz zulassen.

Vergleichbare Fälle kann es auch bei Finanzbehörden, bei der Staatsanwaltschaft, bei Polizeidienststellen und anderen Sicherheitsbehörden geben.

6.3 Grenzen des Beschwerderechts

Beschwerden über Datenverarbeitungen der Gerichte, des Bayerischen Landtags sowie des Bayerischen Obersten Rechnungshofs sind im Grundsatz auf Fälle beschränkt, in welchen diese Stellen „in Verwaltungsangelegenheiten" tätig werden. Grund für diese Einschränkung ist die verfassungsrechtlich begründete Unabhängigkeit der genannten Institutionen.

Beispiel:

> Der A. hat eine Petition beim Landtag eingelegt, die erfolglos blieb. Er begehrt beim Petitionsausschuss, in dem seine Petition behandelt wurde, Auskunft nach → Art. 15 Abs. 1 DSGVO. Das Landtagsamt lehnt dies ab. Eine hiergegen gerichtete Eingabe beim Landesbeauftragten hätte ebenfalls keine Aussicht auf Erfolg: Die Arbeit des Petitionsausschusses gehört zum Bereich der parlamentarischen Tätigkeit, die nicht der Datenschutzaufsicht durch den Landesbeauftragten unterliegt.

6.4 Grenzen der Zuständigkeit

In manchen Fällen kann Ihnen der Landesbeauftragte nicht helfen, weil er örtlich oder sachlich nicht zuständig ist. Die Zuständigkeit liegt dann bei einer anderen Datenschutz-Aufsichtsbehörde.

Wollen Sie sich etwa über ein privates Unternehmen oder eine private Vereinigung beschweren (das Datenschutzrecht spricht auch von einer „nicht-öffentlichen Stelle")? Dann kann Sie die Datenschutz-Aufsichtsbehörde unterstützen, in deren Zuständigkeitsbereich das Unternehmen oder die Vereinigung seinen oder ihren Sitz hat. In Deutschland sind insofern die Ländergrenzen maßgeblich. Die Datenschutzaufsicht über Unternehmen und Vereine mit Sitz in Bayern führt das Bayerische Landesamt für Datenschutzaufsicht (Kontakt: https://www.lda.bayern.de).

Sie halten eine Datenverarbeitung des Bayerischen Rundfunks für rechtswidrig? Dann können Sie sich an den Rundfunkdatenschutzbeauftragten wenden.

Kontakt:

> Der Rundfunkdatenschutzbeauftragte von BR, SR, WDR, Deutschlandradio und ZDF
> 14482 Potsdam, Marlene-Dietrich-Allee 20
> Telefon: +49 331 70989 85501
> E-Mail: kontakt@rundfunkdatenschutz.de

Es geht um eine Datenverarbeitung im Zuständigkeitsbereich der Bayerischen Landeszentrale für neue Medien? Dann können Sie sich beim Medienbeauftragten für den Datenschutz beschweren.

Kontakt:

Mediendatenbeauftragter der Bayerischen Landeszentrale für neue Medien
81737 München, Heinrich-Lübke-Straße 27
Telefon: +49 89 63808-0
E-Mail: datenschutzaufsicht@blm.de

Nach Ihrer Meinung hat eine Bundesbehörde oder eine Behörde eines anderen (Bundes-) Landes einen Datenschutzverstoß begangen? Bei Bundesbehörden wenden Sie sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, bei Landesbehörden anderer (Bundes-) Länder an die/den jeweiligen Landesbeauftragte(n).

Kontakt:

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
53117 Bonn, Husarenstraße 30
Telefon: +49 228 997799-0
E-Mail: poststelle@bfdi.bund.de

Es geht um Datenschutz bei einer Religionsgemeinschaft (insbesondere einer Kirche)? Dann können Sie die Datenschutzbeauftragten dieser Religionsgemeinschaft kontaktieren.

Kontakt (bayerische [Erz-]Diözesen der römisch-katholischen Kirche):

Gemeinsame Datenschutzaufsicht der bayerischen (Erz-)Diözesen
80333 München, Kapellenstraße 4
Telefon: +49 89 2137-1796
E-Mail: jjoachimski@eomuc.de

Kontakt (Evangelisch-Lutherische Kirche in Bayern):

Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland
Datenschutzregion Süd – Außenstelle Ulm
89073 Ulm, Hafenbad 22
Telefon: +49 731 140593-0
E-Mail: sued@datenschutz.ekd.de

Haben Sie Zweifel, an wen Sie sich wenden sollen? Fragen Sie den Landesbeauftragten, er hilft Ihnen gerne weiter. Falls Sie eine Beschwerde mit der Anmerkung versehen, dass Sie mit einer Weiterleitung Ihrer Beschwerde an die zuständige Datenschutz-Aufsichtsbehörde einverstanden sind, leitet er Ihr Schreiben ohne weiteres an die zuständige Datenschutz-Aufsichtsbehörde weiter.

Weitere Kontaktdaten von Datenschutz-Aufsichtsbehörden finden Sie auf der Internetpräsenz https://www.datenschutz-bayern.de in der Rubrik „Zuständigkeiten“.

7 Anhang

7.1 Datenschutz-Grundverordnung (Auszug)

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates
vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung
personenbezogener Daten, zum freien Datenverkehr und
zur Aufhebung der Richtlinie 95/46/EG
(Datenschutz-Grundverordnung)

(ABl. L 119 vom 4. Mai 2016, S. 1,
berichtigt ABl. L 314 vom 22. November 2016, S. 72 und
ABl. L 127 vom 23. Mai 2018, S. 2).

Kapitel I
Allgemeine Bestimmungen

Artikel 1
Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

(3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

Artikel 2
Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,

b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,

c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,

d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

(3) Für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union gilt die Verordnung (EG) Nr. 45/2001. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, werden im Einklang mit Artikel 98 an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst.

(4) Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit der Vermittler unberührt.

Artikel 3
Räumlicher Anwendungsbereich

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

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

a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

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

Artikel 4
Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

2. „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. „Einschränkung der Verarbeitung" die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher In-

formationen 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 Verarbeitungstätigkei-

ten 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 oder 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;

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

Kapitel II
Grundsätze

Artikel 5
Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz");

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Artikel 6
Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

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

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

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vor-

schriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

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

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,

d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Artikel 7
Bedingungen für die Einwilligung

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

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

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

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

Artikel 8
Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

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

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

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

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

Artikel 9
Verarbeitung besonderer Kategorien personenbezogener Daten

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

(2) Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,

b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,

c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,

d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung,

Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,

f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,

h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

i) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

j) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht,

den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.

(3) Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

(4) Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

Artikel 10
Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende 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

(1) Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.

(2) Kann der Verantwortliche in Fällen gemäß Absatz 1 des vorliegenden Artikels nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet er die betroffene Person hierüber, sofern möglich. In diesen Fällen finden die Artikel 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

Kapitel III
Rechte der betroffenen Person

Abschnitt 1
Transparenz und Modalitäten

Artikel 12
Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

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

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

(3) Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des

Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

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

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

a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder

b) sich weigern, aufgrund des Antrags tätig zu werden.

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

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

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

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

Abschnitt 2
Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten

Artikel 13
Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

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

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

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

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

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

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

Artikel 14
Informationspflicht, wenn die personenbezogenen Daten
nicht bei der betroffenen Person erhoben wurden

(1) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) zusätzlich die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) die Kategorien personenbezogener Daten, die verarbeitet werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;

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

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

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

c) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

e) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

f) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;

g) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

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

a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,

b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,

c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

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

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

a) die betroffene Person bereits über die Informationen verfügt,

b) die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien oder soweit die in Absatz 1 des vorliegenden Artikels genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit,

c) die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder

d) die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

Artikel 15
Auskunftsrecht der betroffenen Person

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

a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und

die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

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

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

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Abschnitt 3
Berichtigung und Löschung

Artikel 16
Recht auf Berichtigung

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

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

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

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

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a

stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

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

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

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;

b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;

d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder

e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Artikel 18
Recht auf Einschränkung der Verarbeitung

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

a) die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,

b) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;

c) der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder

d) die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

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

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

Artikel 19
Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

Der Verantwortliche teilt allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten o-

der eine Einschränkung der Verarbeitung nach Artikel 16, Artikel 17 Absatz 1 und Artikel 18 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

Artikel 20
Recht auf Datenübertragbarkeit

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

a) die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und

b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

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

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

(4) Das Recht gemäß Absatz 1 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Abschnitt 4
Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall

Artikel 21
Widerspruchsrecht

(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Wider-

spruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

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

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

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

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

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

Artikel 22
Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

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

(2) Absatz 1 gilt nicht, wenn die Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,

b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

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

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

Abschnitt 5
Beschränkungen

Artikel 23
Beschränkungen

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

a) die nationale Sicherheit;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;

f) den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;

g) die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;

h) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind;

i) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;

j) die Durchsetzung zivilrechtlicher Ansprüche.

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

a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien,

b) die Kategorien personenbezogener Daten,

c) den Umfang der vorgenommenen Beschränkungen,

d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung;

e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen,

f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,

g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und

h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist.

Kapitel IV
Verantwortlicher und Auftragsverarbeiter

Abschnitt 1
Allgemeine Pflichten

Artikel 24
Verantwortung des für die Verarbeitung Verantwortlichen

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

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

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

Artikel 25
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung —, 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 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 Verantwortliche

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

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

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

[Artikel 27: nicht abgedruckt]

Artikel 28
Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

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 und die vorhandenen Kopien löscht, 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 93 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

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

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

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

Artikel 29
Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

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

Artikel 30
Verzeichnis von Verarbeitungstätigkeiten

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

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

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

(4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn, die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10.

Artikel 31
Zusammenarbeit mit der Aufsichtsbehörde

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

Abschnitt 2
Sicherheit personenbezogener Daten

Artikel 32
Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Artikel 33
Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

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

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

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

(5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

Artikel 34
Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

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

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

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

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

b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;

c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

Abschnitt 3
Datenschutz-Folgenabschätzung und vorherige Konsultation

Artikel 35
Datenschutz-Folgenabschätzung

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

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

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

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

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

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

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

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

[Artikel 36: nicht abgedruckt]

Abschnitt 4
Datenschutzbeauftragter

Artikel 37
Benennung eines Datenschutzbeauftragten

(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, soweit sie 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.

[Artikel 40 bis 50: nicht abgedruckt]

Kapitel VI
Unabhängige Aufsichtsbehörden

Abschnitt 1
Unabhängigkeit

Artikel 51
Aufsichtsbehörde

(1) Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird (im Folgenden „Aufsichtsbehörde").

(2) Jede Aufsichtsbehörde leistet einen Beitrag zur einheitlichen Anwendung dieser Verordnung in der gesamten Union. Zu diesem Zweck arbeiten die Aufsichtsbehörden untereinander sowie mit der Kommission gemäß Kapitel VII zusammen.

(3) Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so bestimmt dieser Mitgliedstaat die Aufsichtsbehörde, die diese Behörden im Ausschuss vertritt, und führt ein Verfahren ein, mit dem sichergestellt wird, dass die anderen Behörden die Regeln für das Kohärenzverfahren nach Artikel 63 einhalten.

(4) Jeder Mitgliedstaat teilt der Kommission bis spätestens 25. Mai 2018 die Rechtsvorschriften, die er aufgrund dieses Kapitels erlässt, sowie unverzüglich alle folgenden Änderungen dieser Vorschriften mit.

Artikel 52
Unabhängigkeit

(1) Jede Aufsichtsbehörde handelt bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse gemäß dieser Verordnung völlig unabhängig.

(2) Das Mitglied oder die Mitglieder jeder Aufsichtsbehörde unterliegen bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Verordnung weder direkter noch indirekter Beeinflussung von außen und ersuchen weder um Weisung noch nehmen sie Weisungen entgegen.

(3) Das Mitglied oder die Mitglieder der Aufsichtsbehörde sehen von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen ab und üben während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus.

(4) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können.

(5) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde ihr eigenes Personal auswählt und hat, das ausschließlich der Leitung des Mitglieds oder der Mitglieder der betreffenden Aufsichtsbehörde untersteht.

(6) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt und dass sie über eigene, öffentliche, jährliche Haushaltspläne verfügt, die Teil des gesamten Staatshaushalts oder nationalen Haushalts sein können.

Artikel 53
Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde

(1) Die Mitgliedstaaten sehen vor, dass jedes Mitglied ihrer Aufsichtsbehörden im Wege eines transparenten Verfahrens ernannt wird, und zwar

— vom Parlament,

— von der Regierung,

— vom Staatsoberhaupt oder

— von einer unabhängigen Stelle, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird.

(2) Jedes Mitglied muss über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen.

(3) Das Amt eines Mitglieds endet mit Ablauf der Amtszeit, mit seinem Rücktritt oder verpflichtender Versetzung in den Ruhestand gemäß dem Recht des betroffenen Mitgliedstaats.

(4) Ein Mitglied wird seines Amtes nur enthoben, wenn es eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung seiner Aufgaben nicht mehr erfüllt.

Artikel 54
Errichtung der Aufsichtsbehörde

(1) Jeder Mitgliedstaat sieht durch Rechtsvorschriften Folgendes vor:

a) die Errichtung jeder Aufsichtsbehörde;

b) die erforderlichen Qualifikationen und sonstigen Voraussetzungen für die Ernennung zum Mitglied jeder Aufsichtsbehörde;

c) die Vorschriften und Verfahren für die Ernennung des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde;

d) die Amtszeit des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde von mindestens vier Jahren; dies gilt nicht für die erste Amtszeit nach 24. Mai 2016, die für einen Teil der Mitglieder kürzer sein kann, wenn eine zeitlich versetzte Ernennung zur Wahrung der Unabhängigkeit der Aufsichtsbehörde notwendig ist;

e) die Frage, ob und — wenn ja — wie oft das Mitglied oder die Mitglieder jeder Aufsichtsbehörde wiederernannt werden können;

f) die Bedingungen im Hinblick auf die Pflichten des Mitglieds oder der Mitglieder und der Bediensteten jeder Aufsichtsbehörde, die Verbote von Handlungen, beruflichen Tätigkeiten und Vergütungen während und nach der Amtszeit, die mit diesen Pflichten unvereinbar sind, und die Regeln für die Beendigung des Beschäftigungsverhältnisses.

(2) Das Mitglied oder die Mitglieder und die Bediensteten jeder Aufsichtsbehörde sind gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten sowohl während ihrer Amts- beziehungsweise Dienstzeit als auch nach deren Beendigung verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben oder der Ausübung ihrer Befugnisse bekannt geworden sind, Verschwiegenheit zu wahren. Während dieser Amts- beziehungsweise Dienstzeit gilt diese Verschwiegenheitspflicht insbesondere für die von natürlichen Personen gemeldeten Verstößen gegen diese Verordnung.

Abschnitt 2
Zuständigkeit, Aufgaben und Befugnisse

Artikel 55
Zuständigkeit

(1) Jede Aufsichtsbehörde ist für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig.

(2) Erfolgt die Verarbeitung durch Behörden oder private Stellen auf der Grundlage von Artikel 6 Absatz 1 Buchstabe c oder e, so ist die Aufsichtsbehörde des betroffenen Mitgliedstaats zuständig. In diesem Fall findet Artikel 56 keine Anwendung.

(3) Die Aufsichtsbehörden sind nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

Artikel 56
Zuständigkeit der federführenden Aufsichtsbehörde

(1) Unbeschadet des Artikels 55 ist die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters gemäß dem Verfahren nach Artikel 60 die zuständige federführende Aufsichtsbehörde für die von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführte grenzüberschreitende Verarbeitung.

(2) Abweichend von Absatz 1 ist jede Aufsichtsbehörde dafür zuständig, sich mit einer bei ihr eingereichten Beschwerde oder einem etwaigen Verstoß gegen diese Verordnung zu befassen, wenn der Gegenstand nur mit einer Niederlassung in ihrem Mitgliedstaat zusammenhängt oder betroffene Personen nur ihres Mitgliedstaats erheblich beeinträchtigt.

(3) In den in Absatz 2 des vorliegenden Artikels genannten Fällen unterrichtet die Aufsichtsbehörde unverzüglich die federführende Aufsichtsbehörde über diese Angelegenheit. Innerhalb einer Frist von drei Wochen nach der Unterrichtung entscheidet die federführende Aufsichtsbehörde, ob sie sich mit dem Fall gemäß dem Verfahren nach Artikel 60 befasst oder nicht, wobei sie berücksichtigt, ob der Verantwortliche oder der Auftragsverarbeiter in dem Mitgliedstaat, dessen Aufsichtsbehörde sie unterrichtet hat, eine Niederlassung hat oder nicht.

(4) Entscheidet die federführende Aufsichtsbehörde, sich mit dem Fall zu befassen, so findet das Verfahren nach Artikel 60 Anwendung. Die Aufsichtsbehörde, die die

federführende Aufsichtsbehörde unterrichtet hat, kann dieser einen Beschlussentwurf vorlegen. Die federführende Aufsichtsbehörde trägt diesem Entwurf bei der Ausarbeitung des Beschlussentwurfs nach Artikel 60 Absatz 3 weitestgehend Rechnung.

(5) Entscheidet die federführende Aufsichtsbehörde, sich mit dem Fall nicht selbst zu befassen, so befasst die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, sich mit dem Fall gemäß den Artikeln 61 und 62.

(6) Die federführende Aufsichtsbehörde ist der einzige Ansprechpartner der Verantwortlichen oder der Auftragsverarbeiter für Fragen der von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführten grenzüberschreitenden Verarbeitung.

Artikel 57
Aufgaben

(1) Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet

a) die Anwendung dieser Verordnung überwachen und durchsetzen;

b) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;

c) im Einklang mit dem Recht des Mitgliedsstaats das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten;

d) die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren;

e) auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Verordnung zur Verfügung stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenarbeiten;

f) sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 80 befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das

Ergebnis der Untersuchung unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;

g) mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten;

h) Untersuchungen über die Anwendung dieser Verordnung durchführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;

i) maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken;

j) Standardvertragsklauseln im Sinne des Artikels 28 Absatz 8 und des Artikels 46 Absatz 2 Buchstabe d festlegen;

k) eine Liste der Verarbeitungsarten erstellen und führen, für die gemäß Artikel 35 Absatz 4 eine Datenschutz-Folgenabschätzung durchzuführen ist;

l) Beratung in Bezug auf die in Artikel 36 Absatz 2 genannten Verarbeitungsvorgänge leisten;

m) die Ausarbeitung von Verhaltensregeln gemäß Artikel 40 Absatz 1 fördern und zu diesen Verhaltensregeln, die ausreichende Garantien im Sinne des Artikels 40 Absatz 5 bieten müssen, Stellungnahmen abgeben und sie billigen;

n) die Einführung von Datenschutzzertifizierungsmechanismen und von Datenschutzsiegeln und -prüfzeichen nach Artikel 42 Absatz 1 anregen und Zertifizierungskriterien nach Artikel 42 Absatz 5 billigen;

o) gegebenenfalls die nach Artikel 42 Absatz 7 erteilten Zertifizierungen regelmäßig überprüfen;

p) die Anforderungen an die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 abfassen und veröffentlichen;

q) die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 vornehmen;

r) Vertragsklauseln und Bestimmungen im Sinne des Artikels 46 Absatz 3 genehmigen;

s) verbindliche interne Vorschriften gemäß Artikel 47 genehmigen;

t) Beiträge zur Tätigkeit des Ausschusses leisten;

u) interne Verzeichnisse über Verstöße gegen diese Verordnung und gemäß Artikel 58 Absatz 2 ergriffene Maßnahmen und

v) jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen.

(2) Jede Aufsichtsbehörde erleichtert das Einreichen von in Absatz 1 Buchstabe f genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(3) Die Erfüllung der Aufgaben jeder Aufsichtsbehörde ist für die betroffene Person und gegebenenfalls für den Datenschutzbeauftragten unentgeltlich.

(4) Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anfragen kann die Aufsichtsbehörde eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

Artikel 58
Befugnisse

(1) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Untersuchungsbefugnisse, die es ihr gestatten,

a) den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind,

b) Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen,

c) eine Überprüfung der nach Artikel 42 Absatz 7 erteilten Zertifizierungen durchzuführen,

d) den Verantwortlichen oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen diese Verordnung hinzuweisen,

e) von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten,

f) gemäß dem Verfahrensrecht der Union oder dem Verfahrensrecht des Mitgliedstaats Zugang zu den Räumlichkeiten, 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 betroffene 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.

[Artikel 60 bis 66: nicht abgedruckt]

Kapitel VIII
Rechtsbehelfe, Haftung und Sanktionen

Artikel 77
Recht auf Beschwerde bei einer Aufsichtsbehörde

(1) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.

(2) Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 78.

Artikel 78

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde

(1) Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde.

(2) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen 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

(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 gewöhnlichen 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

(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

(1) Erhält ein zuständiges Gericht in einem Mitgliedstaat Kenntnis von einem Verfahren zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter, das vor einem Gericht in einem anderen Mitgliedstaat anhängig ist, so nimmt es mit diesem Gericht Kontakt auf, um sich zu vergewissern, dass ein solches Verfahren existiert.

(2) Ist ein Verfahren zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter vor einem Gericht in einem anderen Mitgliedstaat anhängig, so kann jedes später angerufene zuständige Gericht das bei ihm anhängige Verfahren aussetzen.

(3) Sind diese Verfahren in erster Instanz anhängig, so kann sich jedes später angerufene Gericht auf Antrag einer Partei auch für unzuständig erklären, wenn das zuerst angerufene Gericht für die betreffenden Klagen zuständig ist und die Verbindung der Klagen nach seinem Recht zulässig ist.

Artikel 82
Haftung und Recht auf Schadenersatz

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

(4) Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer 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 dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(6) Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.

Artikel 83
Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 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 j 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

(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.

[Artikel 85 bis 99: nicht abgedruckt]

7.2 Bayerisches Datenschutzgesetz (Auszug)

Bayerisches Datenschutzgesetz (BayDSG)
vom 15. Mai 2018 (GVBl. S. 230, BayRS 204-1-I),
geändert durch § 6 Gesetz vom 18. Mai 2018 (GVBl. S. 301)

Teil 1
Allgemeine Vorschriften

Art. 1
Anwendungsbereich des Gesetzes

(1) [1]Dieses Gesetz gilt für die Behörden und sonstigen öffentlichen Stellen des Freistaates Bayern, der Gemeinden, Gemeindeverbände und der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts. [2]Für den Landtag gilt dieses Gesetz nur, soweit er in Verwaltungsangelegenheiten tätig wird. [3]Für den Obersten Rechnungshof und die Gerichte gilt Teil 2 Kapitel 5 nur, soweit diese in Verwaltungsangelegenheiten tätig werden. [4] Art. 38 gilt auch für nicht öffentliche Stellen, soweit die Verarbeitung nicht ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten erfolgt.

(2) [1]Öffentliche Stellen sind auch Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen – ungeachtet der Beteiligung nicht öffentlicher Stellen – eine oder mehrere der in Abs. 1 Satz 1 genannten juristischen Personen des öffentlichen Rechts unmittelbar oder durch eine solche Vereinigung beteiligt sind. [2]Öffentlich rechtliche Finanzdienstleistungsunternehmen sowie ihre Zusammenschlüsse und Verbände gelten als nicht öffentliche Stellen.

(3) [1]Soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, gelten für sie selbst, ihre Zusammenschlüsse und Verbände die Vorschriften für nicht öffentliche Stellen. [2]Die Zuständigkeit des Landesbeauftragten für den Datenschutz (Landesbeauftragter) nach Art. 15 bleibt hiervon unberührt.

(4) Soweit nicht öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten für sie die Vorschriften für öffentliche Stellen.

(5) Soweit besondere Rechtsvorschriften über den Datenschutz oder über Verfahren der Rechtspflege auf personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.

(6) Die Vorschriften dieses Gesetzes gelten nicht für die Verarbeitung personenbezogener Daten zur Ausübung des Begnadigungsrechts.

Teil 2
Verarbeitung personenbezogener Daten

Kapitel 1
Allgemeines

Art. 2
Anwendung der Verordnung (EU) 2016/679

[1]Für die Verarbeitung personenbezogener Daten durch öffentliche Stellen gelten vorbehaltlich anderweitiger Regelungen die Vorschriften der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) auch außerhalb des sachlichen Anwendungsbereichs des Art. 2 Abs. 1 und 2 DSGVO. [2]Die Art. 30, 35 und 36 DSGVO gelten nur, soweit die Verarbeitung automatisiert erfolgt oder die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Kapitel 2
Grundsätze der Verarbeitung

Art. 3
Sicherstellung des Datenschutzes, Verantwortlicher (zu Art. 4 Nr. 7 DSGVO)

(1) Die Staatskanzlei, die Staatsministerien und die sonstigen obersten Dienststellen des Staates, die Gemeinden, die Gemeindeverbände und die sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts sowie die privatrechtlichen Vereinigungen, auf die dieses Gesetz gemäß Art. 1 Abs. 1 und 2 Anwendung findet, haben für ihren Bereich die Ausführung der DSGVO, dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen.

(2) Verantwortlicher für die Verarbeitung personenbezogener Daten im Sinne der DSGVO ist die für die Verarbeitung zuständige öffentliche Stelle, soweit nichts anderes bestimmt ist.

Art. 4
Rechtmäßigkeit der Verarbeitung
(zu Art. 6 Abs. 1 bis 3 DSGVO)

(1) Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist.

(2) [1]Personenbezogene Daten, die nicht aus allgemein zugänglichen Quellen entnommen werden, sind bei der betroffenen Person mit ihrer Kenntnis zu erheben. [2]Bei Dritten dürfen personenbezogene Daten erhoben werden, wenn

1. dies durch Rechtsvorschrift vorgesehen oder zwingend vorausgesetzt wird,
2. die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder im Einzelfall eine solche Erhebung erforderlich macht,
3. die Erhebung bei der betroffenen Person einen unverhältnismäßigen Aufwand erfordern würde oder keinen Erfolg verspricht oder
4. die Daten von einer anderen öffentlichen Stelle an die erhebende Stelle übermittelt werden dürfen.

[3]In den Fällen des Satzes 2 Nr. 2 und 3 dürfen keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Person beeinträchtigt werden. [4]Werden Daten bei der betroffenen Person ohne ihre Kenntnis erhoben, gilt Satz 2 Nr. 1 und 2 entsprechend.

Art. 5
Übermittlung
(zu Art. 6 Abs. 2 bis 4 DSGVO)

(1) [1]Eine Übermittlung personenbezogener Daten ist zulässig, wenn

1. sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist oder
2. der Empfänger eine nicht öffentliche Stelle ist, diese Stelle ein berechtigtes Interesse an ihrer Kenntnis glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat; dies gilt auch, soweit die Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben wurden, übermittelt werden.

[2]Bei einer Übermittlung nach Satz 1 Nr. 2 darf der Empfänger die übermittelten Daten nur für den Zweck verarbeiten, zu dem sie ihm übermittelt wurden.

(2) Sind mit personenbezogenen Daten weitere personenbezogene Daten der betroffenen Person oder Dritter so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, ist die Übermittlung auch dieser Daten an öffentliche Stellen zulässig, soweit nicht schutzwürdige Interessen der betroffenen Person oder Dritter offensichtlich überwiegen.

(3) [1]Wenn die Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen durch andere Stellen vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, gilt Art. 28 Abs. 1 bis 4, 9 und 10 DSGVO hierfür entsprechend. [2]Kann der nach Art. 28 Abs. 3 DSGVO erforderliche Vertrag oder das andere Rechtsinstrument vor der Verarbeitung nicht schriftlich oder elektronisch abgefasst werden, muss dies unverzüglich nachgeholt werden.

(4) [1]Werden personenbezogene Daten an eine andere öffentliche Stelle auf deren Ersuchen übermittelt, trägt diese die Verantwortung für die Zulässigkeit der Übermittlung. [2]Die ersuchte Stelle übermittelt Daten nur, wenn das Ersuchen im Rahmen der Aufgaben des Empfängers liegt. [3]Im Übrigen trägt sie die Verantwortung nur dann, wenn besonderer Anlass zur Prüfung der Zulässigkeit besteht.

Art. 6
Zweckbindung
(zu Art. 6 Abs. 3 und 4 DSGVO)

(1) Öffentliche Stellen, die personenbezogene Daten verarbeiten dürfen, dürfen diese auch zur Wahrnehmung von Aufsichts- oder Kontrollbefugnissen, zur Erstellung von Geschäftsstatistiken, zur Rechnungsprüfung, zur Durchführung eigener Organisationsuntersuchungen oder zur Prüfung oder Wartung automatisierter Verfahren der Datenverarbeitung und zur Gewährleistung der Netz- und Informationssicherheit sowie, soweit nicht offensichtlich überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen, zu eigenen Ausbildungs- oder Prüfungszwecken verarbeiten.

(2) Eine Verarbeitung zu anderen Zwecken als zu denjenigen, zu denen die Daten erhoben wurden, ist unbeschadet der Bestimmungen der DSGVO zulässig, wenn

1. offensichtlich ist, dass die Verarbeitung im Interesse der betroffenen Person liegt, und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung hierzu verweigern würde,
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die Daten verarbeitende Stelle sie veröffentlichen dürfte,

3. die Verarbeitung erforderlich ist

   a) zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit und Ordnung,

   b) zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen,

   c) zur Durchführung wissenschaftlicher oder historischer Forschung, das wissenschaftliche oder historische Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann,

   d) zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person,

   e) zur Überprüfung von Angaben der betroffenen Person, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

   f) zum Vergleich von Angaben der betroffenen Person zur Erlangung von finanziellen Leistungen öffentlicher Stellen mit anderen derartigen Angaben oder

   g) zur Sicherung des Steuer- und Zollaufkommens.

(3) Art. 9 DSGVO und die Art. 8 und 24 Abs. 3 bleiben unberührt.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle verarbeitet werden, dürfen nicht zu anderen Zwecken verarbeitet werden.

Art. 7
Besondere automatisierte Verfahren
(zu Art. 6 Abs. 3, Art. 26 DSGVO)

(1) [1]Öffentliche Stellen dürfen automatisierte Verfahren, welche die Übermittlung personenbezogener Daten durch Abruf ermöglichen, nur einrichten, soweit

1. der Abruf aus Datenbeständen erfolgt, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen, oder

2. das Verfahren die Rechte und Freiheiten der betroffenen Personen und die Aufgaben der beteiligten Stellen angemessen berücksichtigt.

[2]Für Abrufe nach Satz 1 Nr. 2

1. trägt der Empfänger die Verantwortung für die Zulässigkeit des einzelnen Abrufs,
2. hat die einrichtende Stelle zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann; sie prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht.

(2) [1]Die Einrichtung automatisierter Verfahren, die mehreren öffentlichen Stellen die Verarbeitung personenbezogener Daten in einem Datenbestand ermöglichen sollen oder bei denen die beteiligten öffentlichen Stellen sich wechselseitig Zugriffe auf die gespeicherten personenbezogenen Daten ermöglichen sollen, ist zulässig, soweit dies unter Berücksichtigung der Rechte und Freiheiten der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist und durch technische und organisatorische Maßnahmen Risiken für die Rechte und Freiheiten der betroffenen Personen vermieden werden können. [2]Verfahren nach Satz 1, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen beinhalten können, sind nur zulässig, wenn sie durch Gesetz oder auf Grund eines Gesetzes eingerichtet werden.

Art. 8
Verarbeitung besonderer Kategorien personenbezogener Daten (zu Art. 9 DSGVO)

(1) [1]Die Verarbeitung von Daten im Sinne des Art. 9 Abs. 1 DSGVO ist auch zulässig, soweit sie erforderlich ist

1. zur Wahrnehmung von Rechten und Pflichten, die aus dem Recht der sozialen Sicherheit und des Sozialschutzes folgen,
2. zur Wahrnehmung von Rechten und Pflichten der öffentlichen Stellen auf dem Gebiet des Dienst- und Arbeitsrechts,
3. zum Zweck der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit von beschäftigten Personen, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder auf Grund eines Vertrags der betroffenen Person mit einem Ange-

hörigen eines Gesundheitsberufs, wenn diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden,

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

5. für die in Art. 6 Abs. 2 Nr. 3 Buchst. a bis c genannten Zwecke.

[2]Bei Verarbeitungen nach Satz 1 bleibt Art. 6 Abs. 1 unberührt.

(2) [1]Bei der Verarbeitung von Daten im Sinne des Art. 9 Abs. 1 DSGVO sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen vorzusehen. [2]Diese Maßnahmen sind in dem Verzeichnis nach Art. 30 DSGVO darzustellen.

(3) Art. 26 Abs. 2 und Art. 27 Abs. 2 bleiben unberührt.

Kapitel 3
Rechte der betroffenen Person

Art. 9
Informationspflicht
(zu Art. 13, 14 DSGVO)

(1) Eine Pflicht zur Information der betroffenen Person besteht unbeschadet sonstiger Bestimmungen dann nicht, soweit und solange ein Fall des Art. 6 Abs. 2 Nr. 3 Buchst. a, b oder Buchst. d vorliegt.

(2) In den Fällen des Art. 4 Abs. 2 Satz 2 ist eine nicht öffentliche Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

Art. 10
Auskunftsrecht der betroffenen Person
(zu Art. 15 DSGVO)

(1) [1]Ob einer Person Auskunft erteilt wird, dass personenbezogene Daten an die Staatsanwaltschaft, Polizei, Finanzverwaltung, Organe der überörtlichen Rech-

nungsprüfung, den Verfassungsschutz, den Bundesnachrichtendienst, den Militärischen Abschirmdienst oder andere Behörden des Bundesministeriums der Verteidigung übermittelt wurden, entscheidet der Verantwortliche im Einvernehmen mit den Stellen, an die diese Daten übermittelt wurden. [2]Dies gilt auch für die Auskunft über personenbezogene Daten, die dem Verantwortlichen von einer der in Satz 1 genannten Stellen übermittelt wurden.

(2) Unbeschadet des Abs. 1 unterbleibt die Auskunft, soweit

1. die Auskunft die ordnungsgemäße Erfüllung von Aufgaben der Gefahrenabwehr oder die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, Ordnungswidrigkeiten oder berufsrechtlichen Vergehen oder die Strafvollstreckung gefährden würde,
2. die Auskunft die öffentliche Sicherheit und Ordnung, die Landesverteidigung oder ein wichtiges wirtschaftliches oder finanzielles Interesse des Freistaates Bayern, eines anderen Landes, des Bundes oder der Europäischen Union – einschließlich Währungs-, Haushalts- und Steuerangelegenheiten – gefährden würde,
3. personenbezogene Daten oder die Tatsache ihrer Speicherung zum Schutz der betroffenen Person oder wegen der überwiegenden berechtigten Interessen Dritter geheim gehalten werden müssen,
4. personenbezogene Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle verarbeitet werden, eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist oder
5. personenbezogene Daten weder automatisiert verarbeitet werden noch in einem Dateisystem gespeichert sind oder gespeichert werden sollen und
   a) die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, oder
   b) der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem geltend gemachten Informationsinteresse steht.

(3) [1]Wird die Auskunft nicht oder nur eingeschränkt erteilt,

1. sind die Gründe dafür aktenkundig zu machen,
2. ist die betroffene Person unter Darlegung der Gründe zu unterrichten, soweit dies nicht einem der in Abs. 2 Nr. 1 bis 3 genannten Zwecke zuwiderliefe, und

3. ist auf Verlangen der betroffenen Person uneingeschränkte Auskunft der Aufsichtsbehörde zu erteilen.

[2]Die Aufsichtsbehörde darf der betroffenen Person ohne Zustimmung der in Abs. 1 Satz 1 genannten Stellen keine Informationen mitteilen, die Rückschlüsse auf deren Erkenntnisstand zulassen.

(4) Art. 25 Abs. 4, Art. 26 Abs. 3 und Art. 27 Abs. 4 bleiben unberührt.

Kapitel 4
Verantwortlicher und Auftragsverarbeiter

Art. 11
Datengeheimnis
(zu Art. 32 Abs. 4 DSGVO)

[1]Den bei öffentlichen Stellen beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). [2]Das Datengeheimnis besteht nach dem Ende ihrer Tätigkeit fort.

Art. 12
Behördliche Datenschutzbeauftragte
(zu Art. 35 Abs. 2, Art. 37 bis 39 DSGVO)

(1) [1]Behördliche Datenschutzbeauftragte erhalten insbesondere

1. Zugang zu dem Verzeichnis nach Art. 30 DSGVO und
2. Gelegenheit zur Stellungnahme vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden.

[2] Art. 24 Abs. 5 bleibt unberührt.

(2) Behördliche Datenschutzbeauftragte dürfen Tatsachen, die ihnen in Ausübung ihrer Funktion anvertraut wurden, und die Identität der mitteilenden Personen nicht ohne deren Einverständnis offenbaren.

(3) Behördliche Datenschutzbeauftragte staatlicher Behörden können durch eine höhere Behörde bestellt werden.

Art. 13
Benachrichtigung bei Datenschutzverletzungen
(zu Art. 34 DSGVO)

Die Benachrichtigung kann auch unter den Voraussetzungen des Art. 6 Abs. 2 Nr. 3 Buchst. a, b oder Buchst. d unterbleiben.

Art. 14
Datenschutz-Folgenabschätzung
(zu Art. 35 DSGVO)

(1) Eine Datenschutz-Folgenabschätzung (Folgenabschätzung) durch den Verantwortlichen kann unterbleiben, soweit

1. eine solche für den Verarbeitungsvorgang bereits vom fachlich zuständigen Staatsministerium oder einer von diesem ermächtigten öffentlichen Stelle durchgeführt wurde und dieser Verarbeitungsvorgang im Wesentlichen unverändert übernommen wird oder
2. der konkrete Verarbeitungsvorgang in einer Rechtsvorschrift geregelt ist und im Rechtsetzungsverfahren bereits eine Folgenabschätzung erfolgt ist, es sei denn, dass in der Rechtsvorschrift etwas anderes bestimmt ist.

(2) [1]Entwickelt eine öffentliche Stelle ein automatisiertes Verfahren, das zum Einsatz durch öffentliche Stellen bestimmt ist, so kann sie, sofern die Voraussetzungen des Art. 35 Abs. 1 DSGVO bei diesem Verfahren vorliegen, die Folgenabschätzung nach den Art. 35 und 36 DSGVO durchführen. [2]Soweit das Verfahren von öffentlichen Stellen im Wesentlichen unverändert übernommen wird, kann eine weitere Folgenabschätzung durch die übernehmenden öffentlichen Stellen unterbleiben.

Kapitel 5
Unabhängige Aufsichtsbehörden

Abschnitt 1
Landesbeauftragter für den Datenschutz

Art. 15
Ernennung und Aufgaben
(zu Art. 51 bis 58 DSGVO)

(1) [1]Der Landesbeauftragte nach Art. 33a der Verfassung ist zuständige Aufsichtsbehörde nach Art. 51 DSGVO und überwacht die Einhaltung dieses Gesetzes und

anderer Vorschriften über den Datenschutz bei den öffentlichen Stellen. [2]Der Landesbeauftragte ist Beamter auf Zeit. [3]Die Ernennung, Entlassung und Abberufung erfolgt durch den Präsidenten des Landtags.

(2) [1]Die Aufsicht durch den Landesbeauftragten erstreckt sich nicht auf

1. Akten zu einer Sicherheitsüberprüfung, soweit die betroffenen Personen der Aufsicht schriftlich gegenüber dem Verantwortlichen widersprochen haben,
2. personenbezogene Daten, die der Kontrolle durch die Kommission nach Art. 2 des Ausführungsgesetzes Art. 10-Gesetz unterliegen, es sei denn, die Kommission ersucht den Landesbeauftragten, die Aufsicht bei bestimmten Vorgängen und in bestimmten Bereichen wahrzunehmen; der Landesbeauftragte berichtet insoweit ausschließlich an die Kommission.

[2]Der Verantwortliche unterrichtet die betroffenen Personen in allgemeiner Form über ihr Widerspruchsrecht nach Satz 1 Nr. 1.

(3) Der Landtag oder die Staatsregierung können den Landesbeauftragten unbeschadet seiner Unabhängigkeit ersuchen, zu bestimmten Vorgängen aus seinem Aufgabenbereich Stellung zu nehmen.

(4) [1]Der Landesbeauftragte bedient sich einer Geschäftsstelle, die beim Landtag eingerichtet wird. [2]Verwaltungsangelegenheiten der Geschäftsstelle werden vom Landtagsamt wahrgenommen, soweit sie nicht der Zuständigkeit des Landesbeauftragten unterliegen.

Art. 16
Ergänzende Rechte und Befugnisse
(zu Art. 57, 58 DSGVO)

(1) [1]Der Landesbeauftragte ist von allen öffentlichen Stellen in der Erfüllung seiner Aufgaben zu unterstützen. [2]Ihm sind alle zur Erfüllung seiner Aufgaben notwendigen Auskünfte zu geben und auf Anforderung alle Unterlagen über die Verarbeitung personenbezogener Daten zur Einsicht vorzulegen. [3]Er hat ungehinderten Zutritt zu allen Diensträumen, in denen öffentliche Stellen Daten verarbeiten.

(2) [1]Die Verpflichtungen nach Abs. 1 gelten für

1. Einrichtungen der Rechtspflege, soweit sie strafverfolgend, strafvollstreckend oder strafvollziehend tätig werden,
2. Behörden, soweit sie Steuern verwalten oder strafverfolgend oder in Bußgeldverfahren tätig werden, und

3. Polizei und Verfassungsschutzbehörden

nur gegenüber dem Landesbeauftragten selbst und gegenüber den von ihm schriftlich besonders damit Beauftragten. [2]Abs. 1 Satz 2 und 3 gilt für diese Stellen nicht, soweit das jeweils zuständige Staatsministerium im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Freistaates Bayern, eines anderen Landes oder des Bundes gefährden würde.

(3) Die Staatskanzlei und die Staatsministerien unterrichten den Landesbeauftragten rechtzeitig über ihre Entwürfe von Rechts- und Verwaltungsvorschriften des Freistaates Bayern sowie über ihre Planungen bedeutender Verfahren zur Verarbeitung personenbezogener Daten.

(4) [1]Unbeschadet der Bestimmungen des Art. 58 DSGVO kann der Landesbeauftragte festgestellte Verstöße gegen dieses Gesetz oder gegen andere Vorschriften über den Datenschutz beanstanden und ihre Behebung in angemessener Frist fordern. [2]Er kann die nach Art. 3 Abs. 1 für die Sicherstellung des Datenschutzes verantwortliche Stelle sowie die Rechts- und Fachaufsichtsbehörde hierüber verständigen. [3]Werden die beanstandeten Verstöße nicht behoben, kann der Landesbeauftragte von den in Satz 2 genannten Stellen binnen angemessener Frist geeignete Maßnahmen fordern. [4]Nach fruchtlosem Fristablauf kann der Landesbeauftragte den Landtag und die Staatsregierung verständigen.

Art. 17
Datenschutzkommission

(1) [1]Der Landtag bildet zur Unterstützung des Landesbeauftragten eine Datenschutzkommission. [2]Sie besteht aus zehn Mitgliedern. [3]Der Landtag bestellt sechs Mitglieder aus seiner Mitte nach Maßgabe der Stärke seiner Fraktionen; dabei wird das Verfahren nach Sainte-Laguë/Schepers angewandt. [4]Für Fraktionen, die hiernach nicht zum Zuge kommen, kann der Landtag jeweils ein weiteres Mitglied bestellen, auch wenn sich dadurch die Zahl der Mitglieder nach Satz 2 erhöht. [5]Ferner bestellt der Landtag jeweils ein weiteres Mitglied auf Vorschlag

1. der Staatsregierung,
2. der kommunalen Spitzenverbände,
3. des Staatsministeriums für Gesundheit und Pflege aus dem Bereich der gesetzlichen Sozialversicherungsträger und
4. des Verbands freier Berufe in Bayern e.V.

[6]Für jedes Mitglied der Datenschutzkommission wird zugleich ein stellvertretendes Mitglied bestellt.

(2) Die Mitglieder der Datenschutzkommission werden jeweils für die Wahldauer des Landtags bestellt; sie sind in ihrer Tätigkeit an Aufträge und Weisungen nicht gebunden.

(3) [1]Die Datenschutzkommission tritt auf Antrag jedes ihrer Mitglieder oder des Landesbeauftragten zusammen. [2]Den Vorsitz führt ein Mitglied des Landtags. [3]Die Datenschutzkommission gibt sich eine Geschäftsordnung.

(4) [1]Die Mitglieder der Datenschutzkommission haben, auch nach ihrem Ausscheiden, über die ihnen bei ihrer Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. [2]Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

(5) Die Mitglieder der Datenschutzkommission erhalten vom Landesbeauftragten Reisekostenvergütung nach den Bestimmungen des Bayerischen Reisekostengesetzes wie Ehrenbeamte.

Abschnitt 2
Landesamt für Datenschutzaufsicht

Art. 18
Einrichtung und Aufgaben
(zu Art. 51 bis 58 und 85 DSGVO)

(1) [1]Das Landesamt für Datenschutzaufsicht (Landesamt) ist Aufsichtsbehörde nach Art. 51 DSGVO und nach § 40 des Bundesdatenschutzgesetzes für nicht öffentliche Stellen. [2]Im Anwendungsbereich des Art. 38 findet Art. 58 Abs. 1 Buchst. b, c, e und f sowie Abs. 2 Buchst. c bis j DSGVO keine Anwendung.

(2) Sitz des Landesamts ist Ansbach.

(3) Der Präsident des Landesamts ist Beamter auf Zeit und wird durch die Staatsregierung für die Dauer von fünf Jahren ernannt.

(4) [1]Das Landesamt kann Aufgaben der Personalverwaltung und Personalwirtschaft auf andere öffentliche Stellen des Freistaates Bayern übertragen, soweit dadurch seine Unabhängigkeit nicht beeinträchtigt wird. [2]Diesen Stellen dürfen personenbezogene Daten der beschäftigten Personen übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

Abschnitt 3
Unabhängigkeit und Zusammenarbeit der Aufsichtsbehörden

Art. 19
Unabhängigkeit und Rechtsstellung
(zu Art. 52 bis 54 DSGVO)

(1) [1]Zum Leiter einer Aufsichtsbehörde kann ernannt werden, wer

1. bei der Ernennung das 35. Lebensjahr vollendet hat,
2. die Voraussetzungen für den Einstieg in die vierte Qualifikationsebene erfüllt und
3. durch einschlägige Berufserfahrung die erforderlichen Kenntnisse des Datenschutzrechts nachweisen kann.

[2]Die Wiederernennung ist zulässig.

(2) [1]Wird ein Beamter oder Richter auf Lebenszeit zum Leiter einer Aufsichtsbehörde ernannt, gilt er für die Dauer der Amtszeit als ohne Bezüge beurlaubt. [2]Für Disziplinarmaßnahmen gegen den Leiter einer Aufsichtsbehörde gilt Art. 6 des Rechnungshofgesetzes entsprechend.

(3) [1]Die Stellen der Aufsichtsbehörden sind auf Vorschlag des Leiters der jeweiligen Aufsichtsbehörde zu besetzen. [2]Die Bediensteten können, sofern die Aufsichtsbehörde nicht selbst für diese Anordnungen zuständig ist, nur mit dessen Einvernehmen versetzt, abgeordnet oder umgesetzt werden. [3]Der Leiter einer Aufsichtsbehörde ist Dienstvorgesetzter der Bediensteten. [4]Die Bediensteten sind in ihrer Tätigkeit nur an dessen Weisungen gebunden und unterstehen ausschließlich seiner Dienstaufsicht. [5]Die Aufsichtsbehörde ist oberste Dienstbehörde im Sinne des § 96 der Strafprozessordnung (StPO), des Art. 6 Abs. 3 Satz 3 des Bayerischen Beamtengesetzes und des Art. 18 Abs. 2 Satz 1 des Bayerischen Disziplinargesetzes. [6]Der Leiter einer Aufsichtsbehörde kann die Disziplinarbefugnisse im Einzelfall teilweise oder vollständig auf die Landesanwaltschaft Bayern übertragen.

(4) [1]Der Leiter einer Aufsichtsbehörde darf

1. kein Gewerbe, keinen Beruf und kein anderes bezahltes Amt ausüben,
2. weder der Leitung noch dem Aufsichts- oder Verwaltungsrat eines auf Erwerb ausgerichteten Unternehmens angehören,
3. keiner Regierung, keiner gesetzgebenden Körperschaft des Bundes oder eines Landes und keinem kommunalen Vertretungsorgan angehören,

4. nicht gegen Vergütung als Schiedsrichter tätig sein, außergerichtliche Gutachten abgeben oder Vorträge halten und

5. keinerlei sonstige Tätigkeiten ausüben, die mit dem Amt nicht zu vereinbaren sind oder die Unabhängigkeit beeinträchtigen können.

[2]Satz 1 Nr. 5 gilt auch für ehemalige Leiter bis zum Ablauf von zwei Jahren nach dem Ausscheiden aus dem Amt.

(5) [1]Der Leiter einer Aufsichtsbehörde sowie deren Bedienstete unterliegen unabhängig von der jeweiligen Ausgestaltung ihres persönlichen Dienstverhältnisses den für Beamte geltenden Verschwiegenheitspflichten. [2]Der Leiter einer Aufsichtsbehörde entscheidet nach pflichtgemäßem Ermessen, ob und inwieweit er sowie die Bediensteten der Aufsichtsbehörde über Angelegenheiten, die dieser Verschwiegenheitspflicht unterliegen, vor Gericht oder außergerichtlich aussagen oder Erklärungen abgeben; wenn er nicht mehr im Amt ist, ist die Genehmigung des amtierenden Leiters der Aufsichtsbehörde erforderlich.

(6) [1]Die Erhebung von Kosten für Amtshandlungen der Aufsichtsbehörden bestimmt sich nach dem Kostengesetz. [2]Unbeschadet des Art. 57 Abs. 4 DSGVO sind Amtshandlungen für die betroffene Person und für den Datenschutzbeauftragten kostenfrei. [3]Die Aufsichtsbehörden unterliegen der Rechnungsprüfung durch den Obersten Rechnungshof nur, soweit ihre Unabhängigkeit hierdurch nicht beeinträchtigt wird.

Art. 20
Anrufung der Aufsichtsbehörden
(zu Art. 77 DSGVO)

(1) [1]Jeder kann sich an die Aufsichtsbehörden mit dem Vorbringen wenden, bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden zu sein. [2]Durch die Anrufung der Aufsichtsbehörden dürfen der betroffenen Person keine Nachteile entstehen.

(2) Auskunfts- oder Einsichtsrechte hinsichtlich Akten und Dateien der Aufsichtsbehörden bestehen nicht.

Art. 21
Zusammenarbeit
(zu Art. 51 DSGVO)

(1) [1]Die bayerischen Aufsichtsbehörden tauschen regelmäßig die in Erfüllung ihrer Aufgaben gewonnenen Erfahrungen aus und unterstützen sich gegenseitig bei ihrer

Aufgabenwahrnehmung. [2]Eine Aufsichtsbehörde ist berechtigt, zum Zwecke der Aufsicht personenbezogene Daten an andere Aufsichtsbehörden zu übermitteln.

(2) Soweit mehrere Aufsichtsbehörden für eine Angelegenheit des Europäischen Datenschutzausschusses zuständig sind, üben sie ihre Mitwirkungsrechte einvernehmlich aus.

Kapitel 6
Sanktionen

Art. 22
Geldbußen
(zu Art. 83 DSGVO)

Gegen öffentliche Stellen im Sinne des Art. 1 Abs. 1 und 2 dürfen Geldbußen nach Art. 83 DSGVO nur verhängt werden, soweit diese als Unternehmen am Wettbewerb teilnehmen.

Art. 23
Ordnungswidrigkeiten, Strafvorschrift
(zu Art. 84 DSGVO)

(1) Mit Geldbuße bis zu dreißigtausend Euro kann belegt werden, wer personenbezogene Daten, die durch eine öffentliche Stelle im Sinne des Art. 1 Abs. 1, 2 oder Abs. 4 verarbeitet werden und nicht offenkundig sind,

1. unbefugt
   a) speichert, verändert oder übermittelt,
   b) zum Abruf mittels automatisierten Verfahrens bereithält oder
   c) abruft oder sich oder einem anderen aus Dateien verschafft oder
2. durch unrichtige Angaben erschleicht.

(2) [1]Wer eine der in Abs. 1 bezeichneten Handlungen gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. [2]Die Tat wird nur auf Antrag verfolgt. [3]Antragsberechtigt sind die betroffene Person, der Verantwortliche, der Auftragsverarbeiter und die Aufsichtsbehörde.

(3) Gegen öffentliche Stellen im Sinne des Art. 1 Abs. 1 und 2 werden keine Geldbußen nach Abs. 1 verhängt.

(4) Eine Unterrichtung nach Art. 33 oder Art. 34 DSGVO darf in einem Straf- oder Ordnungswidrigkeitenverfahren gegen den Verantwortlichen oder einen seiner in § 52 Abs. 1 StPO bezeichneten Angehörigen nur mit seiner Zustimmung verwendet werden.

Kapitel 7
Besondere Verarbeitungssituationen

Art. 24
Videoüberwachung
(zu Art. 6 DSGVO)

(1) Die Verarbeitung personenbezogener Daten mit Hilfe von optisch-elektronischen Einrichtungen (Videoüberwachung) ist zulässig, wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist,

1. um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich im Bereich öffentlicher Einrichtungen, öffentlicher Verkehrsmittel, von Dienstgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder

2. um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Dienstgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen

zu schützen und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Personen beeinträchtigt werden.

(2) [1]Die Videoüberwachung ist durch geeignete Maßnahmen erkennbar zu machen. [2]Dabei ist der Verantwortliche anzugeben, soweit dieser nicht aus den Umständen hervorgeht.

(3) Die Daten dürfen für den Zweck verarbeitet werden, für den sie erhoben worden sind, für einen anderen Zweck nur, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung oder zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich ist.

(4) Die nach Abs. 1 erhobenen und gespeicherten Daten sowie daraus gefertigte Unterlagen sind spätestens zwei Monate nach der Erhebung zu löschen, soweit sie nicht zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung, zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden.

(5) Öffentliche Stellen haben ihrem behördlichen Datenschutzbeauftragten unbeschadet des Art. 35 Abs. 2 DSGVO rechtzeitig vor dem Einsatz einer Videoüberwachung den Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung, den betroffenen Personenkreis, die Maßnahmen nach Abs. 2 und die vorgesehenen Auswertungen mitzuteilen und ihm Gelegenheit zur Stellungnahme zu geben.

Art. 25
Verarbeitung zu Forschungszwecken
(zu Art. 89 DSGVO)

(1) Für Zwecke der wissenschaftlichen oder historischen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für diese Zwecke verarbeitet werden.

(2) [1]Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. [2]Bis dahin sind die Merkmale, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können, gesondert zu speichern. [3]Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(3) Die wissenschaftliche oder historische Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

(4) Die Art. 15, 16, 18 und 21 DSGVO sind nicht anzuwenden, soweit die Inanspruchnahme dieser Rechte voraussichtlich die Verwirklichung der wissenschaftlichen oder historischen Forschungszwecke unmöglich macht oder ernsthaft beeinträchtigt und diese Beschränkung für die Erfüllung der Forschungszwecke notwendig ist.

Art. 26
Verarbeitung zu Archivzwecken
(zu Art. 89 DSGVO)

(1) Personenbezogene Daten dürfen zu im öffentlichen Interesse liegenden Archivzwecken verarbeitet werden, soweit geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorgesehen werden.

(2) [1]Die Verarbeitung von Daten im Sinne des Art. 9 Abs. 1 DSGVO ist auch zulässig, soweit sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist. [2]Der

Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Rechte der betroffenen Person gemäß Art. 8 Abs. 2 vor.

(3) Ein Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO besteht nicht, soweit das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts ohne unverhältnismäßigen Aufwand ermöglichen.

(4) [1] Art. 16 DSGVO ist nicht anzuwenden. [2]Die betroffene Person kann verlangen, dass dem Archivgut, das sich auf ihre Person bezieht, eine Gegendarstellung beigefügt wird, wenn sie die Richtigkeit der sie betreffenden Informationen glaubhaft bestreitet. [3]Nach dem Tod der betroffenen Person kann die Beifügung einer Gegendarstellung von dem Ehegatten, dem Lebenspartner, den Kindern oder den Eltern verlangt werden, wenn sie ein berechtigtes Interesse daran glaubhaft machen können.

(5) Die Art. 18 Abs. 1 Buchst. a, b und d sowie Art. 20 und 21 DSGVO sind nicht anzuwenden, soweit diese Rechte voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und diese Beschränkung für die Erfüllung der Archivzwecke notwendig ist.

(6) Soweit öffentliche Stellen verpflichtet sind, Unterlagen einem öffentlichen Archiv zur Übernahme anzubieten, ist eine Löschung erst zulässig, nachdem die Unterlagen dem öffentlichen Archiv angeboten worden und von diesem nicht als archivwürdig übernommen worden sind oder über die Übernahme nicht fristgerecht entschieden worden ist.

Art. 27
Staatliche und kommunale Auszeichnungen und Ehrungen

(1) Zur Vorbereitung und Durchführung staatlicher oder kommunaler Auszeichnungen oder Ehrungen dürfen personenbezogene Daten, einschließlich der Daten nach Art. 9 Abs. 1 DSGVO, auch ohne Kenntnis der betroffenen Person verarbeitet werden.

(2) Andere öffentliche Stellen dürfen die zur Vorbereitung und Durchführung staatlicher oder kommunaler Auszeichnungen und Ehrungen erforderlichen personenbezogenen Daten, einschließlich der Daten nach Art. 9 Abs. 1 DSGVO, an die dafür zuständigen Stellen übermitteln.

(3) [1]Eine Verarbeitung der personenbezogenen Daten nach Abs. 1 für andere Zwecke ist nur mit Einwilligung der betroffenen Person zulässig. [2]Der Verantwortliche

sieht angemessene und spezifische Maßnahmen zur Wahrung der Rechte der betroffenen Person gemäß Art. 8 Abs. 2 vor.

(4) Soweit eine Verarbeitung ausschließlich für die in Abs. 1 genannten Zwecke erfolgt, sind die Art. 13 bis 16, 19 und 20 DSGVO nicht anzuwenden.

(5) [1]Die nach Abs. 1 gespeicherten personenbezogenen Daten sind zu löschen, sobald sie für den dort genannten Zweck nicht mehr erforderlich sind. [2]Eine Löschung von Name, Vorname, Geburtsdatum, Anschrift und Kommunikationsdaten kann unterbleiben.

(6) Abweichend von Art. 58 Abs. 2 DSGVO steht dem Landesbeauftragten bei der Überwachung der Anwendung von den Abs. 1 bis 5 nur das Beanstandungsrecht nach Art. 16 Abs. 4 zu.

Kapitel 8
Verarbeitungen im Anwendungsbereich der Richtlinie (EU) 2016/680

Art. 28
Anwendungsbereich dieses Kapitels

(1) [1]Die Vorschriften dieses Kapitels gelten, soweit nichts anderes bestimmt ist, für die Verarbeitung personenbezogener Daten durch

1. die Polizei,
2. die Gerichte in Strafsachen und die Staatsanwaltschaften,
3. die Strafvollstreckungs- und Justizvollzugsbehörden,
4. die Behörden des Maßregelvollzugs

zum Zwecke der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. [2]Die Vorschriften dieses Kapitels gelten auch für sonstige Behörden im Sinne des Art. 1 Abs. 1 Satz 1, soweit diese personenbezogene Daten verarbeiten, um Straftaten oder Ordnungswidrigkeiten zu verfolgen oder zu ahnden.

(2) [1]Unbeschadet anderer Rechtsvorschriften finden auf Verarbeitungen nach Abs. 1 abweichend von Art. 2 nur Anwendung:

1. aus dem Kapitel I DSGVO über allgemeine Bestimmungen Art. 4 DSGVO,

2. aus dem Kapitel II DSGVO über Grundsätze die Art. 5, 6 Abs. 1 Satz 1 Buchst. a und e, Art. 7 und 11 Abs. 1 DSGVO,
3. aus dem Kapitel IV DSGVO über Verantwortliche und Auftragsverarbeiter die Art. 24 Abs. 1 und 2, Art. 25 Abs. 1 und 2, Art. 28 Abs. 1 bis 4, 9 und 10, Art. 29, 31, 34, 36 Abs. 4, Art. 37 Abs. 1 und 3 bis 7, Art. 38 und 39 DSGVO,
4. aus dem Kapitel VI DSGVO über unabhängige Aufsichtsbehörden die Art. 51 bis 54, 55 Abs. 1 und 3 und Art. 59 DSGVO,
5. aus dem Kapitel VII DSGVO über Zusammenarbeit und Kohärenz Art. 61 Abs. 1 bis 7 und 9 DSGVO und
6. aus dem Kapitel VIII DSGVO über Rechtsbehelfe, Haftung und Sanktionen die Art. 77, 78 Abs. 1 bis 3 DSGVO.

[2]Im Übrigen finden aus dem Kapitel II DSGVO über Grundsätze Art. 9 Abs. 1 und 2, aus dem Kapitel IV DSGVO über Verantwortliche und Auftragsverarbeiter die Art. 26, 30, 32 und 33 DSGVO sowie aus dem Kapitel VI DSGVO über unabhängige Aufsichtsbehörden die Art. 57 und 58 DSGVO nach Maßgabe der nachfolgenden Vorschriften dieses Kapitels Anwendung.

(3) Unbeschadet anderer Rechtsvorschriften finden auf Verarbeitungen nach Abs. 1 keine Anwendung

1. aus Kapitel 2 über Grundsätze der Verarbeitung die Art. 6 Abs. 2 bis 4, Art. 7 und 8 Abs. 1,
2. das Kapitel 3 über Rechte der betroffenen Person,
3. aus Kapitel 4 über Verantwortliche und Auftragsverarbeiter Art. 14 Abs. 1 Nr. 1 und Abs. 2,
4. aus Kapitel 5 über unabhängige Aufsichtsbehörden Art. 18,
5. aus Kapitel 6 über Sanktionen Art. 22 und
6. aus Teil 3 über Meinungsäußerungs- und Informationsfreiheit Art. 38.

Art. 29
Verarbeitung zu anderen Zwecken und besonderer Kategorien personenbezogener Daten, DNA-Untersuchungen

(1) [1]Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen der in Art. 28 Abs. 1 genannten Zwecke handelt, der Verantwortliche

befugt ist, Daten zu diesem Zweck zu verarbeiten, und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist. [2]Die Verarbeitung personenbezogener Daten zu einem anderen, in Art. 28 Abs. 1 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist, die Voraussetzungen des Art. 9 Abs. 2 Buchst. c und e DSGVO vorliegen oder dies in einer Rechtsvorschrift vorgesehen ist.

(3) [1]Zur Vermeidung von DNA-Trugspuren können Personen, die regelmäßig Aufgaben im Rahmen polizeilicher oder strafprozessualer Ermittlungen wahrnehmen und dabei möglicherweise mit Spurenmaterial in Kontakt geraten, mit deren schriftlicher Zustimmung Körperzellen entnommen und molekulargenetisch untersucht werden, um hieraus gewonnene DNA-Identifizierungsmuster zu verarbeiten und mit Spurenmaterial automatisiert abzugleichen. [2]Die Entnahme der Körperzellen erfolgt mittels eines Mundschleimhautabstrichs oder eines hinsichtlich seiner Eingriffsintensität vergleichbaren Verfahrens. [3]Vor Erteilung der Zustimmung ist die betroffene Person über den Zweck der Verarbeitung sowie das Verfahren der Erkennung von DNA-Trugspuren zu belehren und darüber aufzuklären, dass sie die Zustimmung verweigern sowie jederzeit widerrufen kann. [4]Die Verwendung der entnommenen Körperzellen ist nur zur Feststellung des DNA-Identifizierungsmusters nach Satz 1, die Verarbeitung des DNA-Identifizierungsmusters nur zu den in Satz 1 genannten Zwecken zulässig.

(4) [1]Die DNA-Identifizierungsmuster werden in einer hierfür eingerichteten polizeilichen Datei gespeichert. [2]Eine Datenschutzfolgenabschätzung ist nicht erforderlich.

(5) [1]Die DNA-Identifizierungsmuster sind zu pseudonymisieren. [2]Abgleiche mit diesen sind zu protokollieren. [3]Die Protokolldaten sind eigenständig zu speichern und dürfen nur zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung verwendet werden. [4]Soweit die Protokolldaten hierfür nicht mehr benötigt werden, spätestens aber nach Ablauf des dritten Kalenderjahres, das dem Jahr der Protokollierung folgt, sind sie zu löschen.

(6) [1]Die nach Abs. 3 gewonnenen Körperzellen sind zu vernichten und die erhobenen Daten zu löschen, wenn sie für die genannten Zwecke nicht mehr erforderlich sind. [2]Die Vernichtung der Körperzellen und die Löschung der erhobenen Daten hat spätestens drei Jahre nach dem Zeitpunkt zu erfolgen, zu dem die betroffene Person letztmals mit Spurenmaterial in Kontakt treten konnte.

Art. 30
Gemeinsam Verantwortliche

[1]Die Angabe der Anlaufstelle für die betroffenen Personen nach Art. 26 Abs. 1 Satz 3 DSGVO ist verpflichtend. [2] Art. 26 Abs. 2 DSGVO findet keine Anwendung.

Art. 31
Verzeichnis von Verarbeitungstätigkeiten

[1]In dem Verzeichnis nach Art. 30 Abs. 1 DSGVO werden zusätzlich die Rechtsgrundlage der Verarbeitung sowie gegebenenfalls die Verwendung von Profiling aufgenommen. [2] Art. 30 Abs. 5 DSGVO findet keine Anwendung.

Art. 32
Anforderungen an die Sicherheit der Verarbeitung

(1) Art. 32 Abs. 3 und 4 DSGVO findet keine Anwendung.

(2) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche oder der Auftragsverarbeiter auf Grundlage einer Risikobewertung Maßnahmen zu ergreifen, die geeignet sind, um

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle),
3. zu verhindern, dass
   a) Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
   b) personenbezogene Daten unbefugt eingegeben werden sowie gespeicherte personenbezogene Daten unbefugt gelesen, verändert oder gelöscht werden (Speicherkontrolle),
   c) automatisierte Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),
   d) bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),

4. zu gewährleisten, dass

   a) die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),

   b) überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),

   c) nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in automatisierte Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),

   d) eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung),

   e) alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),

   f) gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),

   g) personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können (Auftragskontrolle).

Art. 33
Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Wenn Daten von oder an den Verantwortlichen eines anderen Mitgliedstaates übermittelt wurden, sind die Informationen nach Art. 33 Abs. 3 DSGVO unverzüglich auch an diesen zu melden.

Art. 34
Aufsicht durch den Landesbeauftragten für den Datenschutz

(1) [1] Art. 57 Abs. 1 Buchst. j bis s, u und v DSGVO sowie Art. 58 Abs. 1 Buchst. c, Abs. 2 Buchst. c bis j, Abs. 3 Buchst. c bis j DSGVO finden keine Anwendung. [2]Übt der Landesbeauftragte für die betroffene Person deren Rechte aus, hat er darüber hinaus die Rechtmäßigkeit der Verarbeitung zu überprüfen und die betroffene Person innerhalb

einer angemessenen Frist über das Ergebnis dieser Überprüfung zu unterrichten oder ihr die Gründe mitzuteilen, aus denen die Überprüfung nicht vorgenommen werden kann. [3]Die Mitteilung an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Auskunft zustimmt.

(2) [1]Die Aufsicht durch den Landesbeauftragten über die Erhebung personenbezogener Daten durch Strafverfolgungsbehörden bei der Ermittlung, Aufdeckung oder Verfolgung von Straftaten ist erst nach Abschluss des Strafverfahrens zulässig. [2]Sie erstreckt sich nicht auf eine Datenverarbeitung, die gerichtlich überprüft wurde. [3]Die Sätze 1 und 2 gelten für die Strafvollstreckung entsprechend.

(3) [1]Wird eine Beschwerde bei einer sachlich unzuständigen Aufsichtsbehörde eingereicht, gibt diese die Beschwerde unverzüglich an die sachlich zuständige Aufsichtsbehörde ab und unterrichtet die beschwerdeführende Person. [2]In diesem Fall hat die abgebende Stelle die betroffene Person über die Weiterleitung zu unterrichten und ihr auf Ersuchen weitere Unterstützung zu leisten.

Art. 35
Automatisierte Einzelentscheidungen

(1) Entscheidungen, die für die betroffene Person mit einer nachteiligen Rechtsfolge verbunden sind oder sie erheblich beeinträchtigen, einschließlich Profiling, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung gestützt werden, es sei denn, eine Rechtsvorschrift lässt dies ausdrücklich zu.

(2) Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Daten im Sinne des Art. 9 Abs. 1 DSGVO benachteiligt werden, ist verboten.

Art. 36
Vertrauliche Meldung von Datenschutzverstößen

[1]Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können. [2] Art. 12 Abs. 2 gilt für die zur Entgegennahme dieser Meldungen betraute Stelle entsprechend.

Art. 37
Schadenersatz

(1) [1]Hat eine öffentliche Stelle einer betroffenen Person durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz rechtswidrige Verarbeitung ihrer personenbezogenen Daten einen Schaden zugefügt, ist ihr Rechtsträger der betroffenen Person zum Ersatz dieses Schadens verpflichtet. [2]Die Ersatzpflicht entfällt, soweit bei einer nicht automatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist. [3]Sind bei einer Datei mehrere Stellen speicherungsberechtigt und sind Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

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

(3) Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(4) [1]Hat bei der Entstehung des Schadens ein Verschulden der betroffenen Person mitgewirkt, ist § 254 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden. [2]Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

(5) Vorschriften, nach denen Ersatzpflichtige in weiterem Umfang als nach dieser Vorschrift haften oder nach denen andere für den Schaden verantwortlich sind, bleiben unberührt.

(6) Der Rechtsweg vor den ordentlichen Gerichten steht offen.

Teil 3
Meinungsäußerungs- und Informationsfreiheit

Art. 38
Verarbeitung zu journalistischen, künstlerischen oder literarischen Zwecken (zu Art. 85 DSGVO)

(1) [1]Werden personenbezogene Daten zu journalistischen, künstlerischen oder literarischen Zwecken verarbeitet, stehen den betroffenen Personen nur die in Abs. 2 genannten Rechte zu. [2]Im Übrigen gelten für Verarbeitungen im Sinne des Satzes 1 Kapitel I, Art. 5 Abs. 1 Buchst. f, Art. 24 und 32, Kapitel VIII, X und XI DSGVO. [3] Art. 82 DSGVO gilt mit der Maßgabe, dass nur für unzureichende Maßnahmen nach Art. 5 Abs. 1 Buchst. f, Art. 24 und 32 DSGVO gehaftet wird.

(2) Führt die journalistische, künstlerische oder literarische Verarbeitung personenbezogener Daten zur Verbreitung von Gegendarstellungen, zu Verpflichtungserklärungen, gerichtlichen Entscheidungen oder Widerrufen, sind diese zu den gespeicherten Daten zu nehmen, dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst und bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln.

Art. 39
Allgemeines Auskunftsrecht
(zu Art. 86 DSGVO)

(1) [1]Jeder hat das Recht auf Auskunft über den Inhalt von Dateien und Akten öffentlicher Stellen, soweit ein berechtigtes, nicht auf eine entgeltliche Weiterverwendung gerichtetes Interesse glaubhaft dargelegt wird und

1. bei personenbezogenen Daten eine Übermittlung an nicht öffentliche Stellen zulässig ist und
2. Belange der öffentlichen Sicherheit und Ordnung nicht beeinträchtigt werden.

[2]Die Auskunft kann verweigert werden, soweit

1. Kontroll- und Aufsichtsaufgaben oder sonstige öffentliche oder private Interessen entgegenstehen,
2. sich das Auskunftsbegehren auf den Verlauf oder auf vertrauliche Inhalte laufender oder abgeschlossener behördeninterner Beratungen oder auf Inhalte aus nicht abgeschlossenen Unterlagen oder auf noch nicht aufbereitete Daten bezieht oder
3. ein unverhältnismäßiger Aufwand entsteht.

(2) Abs. 1 findet keine Anwendung auf Auskunftsbegehren, die Gegenstand einer Regelung in anderen Rechtsvorschriften sind.

(3) Ausgenommen von der Auskunft nach Abs. 1 sind

1. Verschlusssachen,
2. einem Berufs- oder besonderen Amtsgeheimnis unterliegende Datei- und Akteninhalte sowie
3. zum persönlichen Lebensbereich gehörende Geheimnisse oder Betriebs- und Geschäftsgeheimnisse, sofern die betroffene Person nicht eingewilligt hat.

(4) [1]Abs. 1 ist nicht anzuwenden auf

1. den Landtag, den Obersten Rechnungshof, die Staatlichen Rechnungsprüfungsämter, die Staatlichen Rechnungsprüfungsstellen der Landratsämter, den Kommunalen Prüfungsverband und die Aufsichtsbehörden im Sinne des Art. 51 DSGVO,
2. die obersten Landesbehörden in Angelegenheiten der Staatsleitung und der Rechtsetzung,
3. die Gerichte, Strafverfolgungs- und Strafvollstreckungsbehörden, Gerichtsvollzieher, Notare und die Landesanwaltschaft Bayern als Organe der Rechtspflege sowie die Justizvollzugsbehörden, die Disziplinarbehörden und die für Angelegenheiten der Berufsaufsicht zuständigen berufsständischen Kammern und Körperschaften des öffentlichen Rechts,
4. die Polizei und das Landesamt für Verfassungsschutz einschließlich der für ihre Aufsicht zuständigen Stellen,
5. Finanzbehörden in Verfahren nach der Abgabenordnung,
6. Universitätskliniken, Forschungseinrichtungen, Hochschulen, Schulen sowie sonstige öffentliche Stellen im Bereich von Forschung und Lehre, Leistungsbeurteilungen und Prüfungen,
7. die Landeskartellbehörde und die Regulierungskammer des Freistaates Bayern sowie die Industrie- und Handelskammern und die Handwerkskammern,
8. die kommunalen Spitzenverbände.

[2]Datei- und Aktenbestandteile der in Satz 1 genannten oder für Begnadigungsangelegenheiten zuständigen Stellen sind von der Auskunft nach Abs. 1 auch dann ausgenommen, wenn sie sich in Dateien oder Akten anderer öffentlicher Stellen befinden.

(5) Für die Auskunft werden Kosten nach Maßgabe des Kostengesetzes erhoben.

[Art. 39a bis 40: nicht abgedruckt]