Der Bayerische Landesbeauftragte
für den Datenschutz

# Die Datenschutz-Grundverordnung

## Ein Überblick

Stand: 25. Mai 2018

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

# Einleitung

Das Datenschutzrecht wurde zum 25. Mai 2018 europaweit grundlegend reformiert. Auch die bayerischen öffentlichen – insbesondere staatlichen und kommunalen – Stellen müssen sich auf diesem Gebiet mit einem geänderten normativen Handlungsrahmen vertraut machen.

Das neue Datenschutzrecht ist stark durch den Einfluss des Unionsrechts geprägt, sodass gewohnte Problemlösungen nicht unbesehen übernommen werden können. Das vorliegende Arbeitspapier legt daher besonderes Gewicht darauf, Kontinuität und Wandel im Datenschutzrecht anhand einzelner Regelungen zu erläutern. Einzelfragen der Rechtsanwendung, wie sie sich in der behördlichen Alltagspraxis stellen, kommen nur punktuell zur Sprache.

Der Bayerische Landesbeauftragte für den Datenschutz veröffentlicht auf seiner Homepage (https://www.datenschutz-bayern.de) in der Rubrik „Datenschutzreform 2018“ sukzessive Orientierungshilfen, Kurzpapiere und weitere Materialien, die den bayerischen öffentlichen Stellen die Arbeit mit dem neuen Datenschutzrecht erleichtern sollen. Hierzu wird auch ein RSS-Newsfeed angeboten (Näheres dazu finden Sie auf der Homepage unter dem Link „RSS“).

Die bereitgestellten Informationen sollen die bayerischen öffentlichen Stellen bei der Umstellung auf die Datenschutz-Grundverordnung unterstützen. Sie wollen einen Beitrag zum Verständnis des neuen Rechts leisten, nehmen aber keine Verbindlichkeit in Anspruch.

# Inhaltsverzeichnis

# I. Geltung und Anwendungsbereich

## 1. Inkrafttreten und unmittelbare Geltung der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO)[1] ist am 24. Mai 2016 in Kraft getreten. Sie beansprucht seit dem 25. Mai 2018 in der gesamten Europäischen Union (EU) – und damit auch im Freistaat Bayern – Geltung und hat die bisherige allgemeine Datenschutz-Richtlinie 95/46/EG ersetzt. Die Datenschutz-Grundverordnung hat zum **Ziel**, sowohl die Grundrechte und Grundfreiheiten natürlicher Personen – insbesondere deren Recht auf Schutz personenbezogener Daten – zu schützen als auch den freien Verkehr personenbezogener Daten zu gewährleisten (vgl. Art. 1 DSGVO).

Im Unterschied zu Richtlinien sind EU-Verordnungen in allen ihren Teilen verbindlich und **gelten unmittelbar** in jedem Mitgliedstaat (Art. 288 Vertrag über die Arbeitsweise der Europäischen Union – AEUV). Der europäische Gesetzgeber will mit dem Instrument der Verordnung eine Vollharmonisierung des Datenschutzrechts in Europa erreichen.

Die unmittelbare Geltung der Datenschutz-Grundverordnung hat dabei zum einen zur Folge, dass sie grundsätzlich ohne weitere Umsetzungsakte (siehe aber zu den sogenannten „Öffnungs- und Spezifizierungsklauseln“ sogleich unter 2.) Bestandteil der jeweiligen Rechtsordnung wird. Zum anderen kommt der Datenschutz-Grundverordnung aufgrund ihrer unmittelbaren Geltung ein **Anwendungsvorrang** gegenüber dem nationalen Recht zu. Dies bedeutet, dass nationales Recht, welches in Widerspruch zur Datenschutz-Grundverordnung steht, ab deren Geltungsbeginn nicht mehr zur Anwendung kommen darf.

Um die uneingeschränkte Anwendbarkeit der Datenschutz-Grundverordnung zu gewährleisten, müssen die Mitgliedstaaten daher ihr **nationales Recht** bis zum Geltungsbeginn an die Datenschutz-Grundverordnung **anpassen**. In Deutschland kommt diese Aufgabe in erster Linie dem Bundes- sowie den Landesgesetzgebern zu.

**Aber auch die Selbstverwaltungskörperschaften – insbesondere die Kommunen und die Hochschulen – haben ihr Satzungsrecht auf eventuellen Anpassungsbedarf hin zu überprüfen und gegebenenfalls mit der Datenschutz-Grundverordnung in Einklang zu bringen.**

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

## 2. Öffnungs- und Spezifizierungsklauseln der Datenschutz-Grundverordnung und das nationale Datenschutzrecht

Die Datenschutz-Grundverordnung ist eine untypische EU-Verordnung insoweit, als sie Ausnahmen von dem Grundsatz trifft, wonach eine Verordnung keiner weiteren Umsetzungsakte mehr bedarf (siehe bereits oben unter 1.). Stattdessen sieht sie eine Reihe von **Öffnungs- und Spezifizierungsklauseln** vor, die den mitgliedstaatlichen Gesetzgebern teils Gestaltungsspielräume eröffnen, teils Regelungsaufträge auferlegen.

Die Mehrzahl dieser Öffnungs- und Spezifizierungsklauseln betrifft die **Datenverarbeitung durch öffentliche Stellen**. Im öffentlichen Bereich ist der Vollharmonisierungsanspruch der Datenschutz-Grundverordnung damit von vornherein eingeschränkt.

Eine für den öffentlichen Bereich besonders bedeutsame Öffnungs- und Spezifizierungsklausel stellt Art. 6 Abs. 3 in Verbindung mit Abs. 1 UAbs. 1 Buchst. e DSGVO dar: Hiernach ist für Datenverarbeitungen bei der Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, die Rechtsgrundlage durch Unionsrecht oder mitgliedstaatliches Recht festzulegen. Die Mitgliedstaaten können in diesem Zusammenhang nach Maßgabe des Art. 6 Abs. 2 und Abs. 3 UAbs. 2 Satz 2 DSGVO zudem die Anwendung der Vorschriften der Datenschutz-Grundverordnung spezifischer regeln.

Weitere, für öffentliche Stellen bedeutsame Öffnungs- und Spezifizierungsklauseln betreffen beispielsweise die Verarbeitung besonderer Kategorien personenbezogener Daten (so etwa Gesundheitsdaten, Art. 9 DSGVO) oder die Einschränkung von Betroffenenrechten (Art. 12 ff. DSGVO in Verbindung mit Art. 23 DSGVO).

Die Neufassung des Bayerischen Datenschutzgesetzes (BayDSG)[2] nutzt diese Öffnungs- und Spezifizierungsklauseln ebenso wie das inzwischen angepasste bereichsspezifische bayerische Datenschutzrecht. Über die zwingend umzusetzenden Regelungsaufträge hinaus hatte der bayerische Gesetzgeber zu entscheiden, ob und in welchem Umfang er von den Gestaltungsmöglichkeiten Gebrauch macht, die ihm die Datenschutz-Grundverordnung einräumt.

**Seit Geltungsbeginn der Datenschutz-Grundverordnung ergibt sich das für die bayerischen öffentlichen Stellen maßgebliche Datenschutzrecht aus der Datenschutz-Grundverordnung und dem nationalen Recht, das diese ergänzt bzw. ausfüllt. Zur Beurteilung datenschutzrechtlicher Fragestellungen sind somit die Datenschutz-Grundverordnung und die Regelungen im allgemeinen sowie gegebenenfalls auch im bereichsspezifischen nationalen Datenschutzrecht (sei es im Landes-, sei es im Bundesrecht) im Zusammenhang zu lesen und anzuwenden.**

[2] Bayerisches Datenschutzgesetz vom 15. Mai 2018 (GVBl. S. 230, BayRS 204-1-I), geändert durch § 6 des Gesetzes vom 18. Mai 2018 (GVBl. S. 301).

## 3. Anwendungsbereich

Der Anwendungsbereich der Datenschutz-Grundverordnung umfasst nach Art. 2 Abs. 1 DSGVO die **ganz oder teilweise automatisierte Verarbeitung** personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Nicht hiervon erfasst sind nach Erwägungsgrund (ErwGr) 15 DSGVO lediglich „Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind". **Strukturierte Behördenakten** – gleich, ob sie elektronisch oder in Papierform geführt werden – unterfallen daher vollumfänglich den Regelungen der Datenschutz-Grundverordnung.

Die Datenschutz-Grundverordnung gilt allerdings nicht für Verarbeitungen im Rahmen von Tätigkeiten außerhalb des Anwendungsbereichs des Unionsrechts (Art. 2 Abs. 2 Buchst. a DSGVO). Dies betrifft etwa Verfassungsschutzbehörden oder die parlamentarische Tätigkeit des Landtags.

Vom Anwendungsbereich der Datenschutz-Grundverordnung ausgenommen sind ferner Datenverarbeitungen im Bereich der Strafjustiz (Art. 2 Abs. 2 Buchst. d DSGVO). Diesbezüglich hat der europäische Gesetzgeber flankierend zur Datenschutz-Grundverordnung die Datenschutz-Richtlinie für Polizei und Strafjustiz[3] erlassen.

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

# II. Begriffe und Grundsätze

## 1. Die Terminologie der Datenschutz-Grundverordnung

Eine Reihe zentraler Begriffe der Datenschutz-Grundverordnung ist in Art. 4 DSGVO definiert. Viele davon sind bereits aus dem bisherigen Datenschutzrecht bekannt und inhaltlich im Wesentlichen unverändert; teilweise ergeben sich jedoch Abweichungen.

Einige dieser Begrifflichkeiten werden im Folgenden – ohne Anspruch auf Vollständigkeit – kurz dargestellt:

(1) **„Personenbezogene Daten“** sind nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (sogenannte „betroffene Person“) beziehen. Inhaltlich entspricht dies dem gängigen Begriffsverständnis. Art. 4 Nr. 1 DSGVO führt im Weiteren ergänzend aus, wann eine natürliche Person als identifizierbar anzusehen ist.

(2) Der **Verarbeitungsbegriff** der Datenschutz-Grundverordnung reicht weiter als derjenige nach dem bisherigen Art. 4 Abs. 6 Satz 1 Bayerisches Datenschutzgesetz (BayDSG a. F.) und dem bisherigen § 3 Abs. 4 Bundesdatenschutzgesetz. Er umfasst nach Art. 4 Nr. 2 DSGVO grundsätzlich jeden Verarbeitungsvorgang im Zusammenhang mit personenbezogenen Daten einschließlich deren Erhebung. Die bislang im deutschen Datenschutzrecht gebräuchliche Begriffs-Trias „Erhebung, Verarbeitung und Nutzung“ wird daher durch den einheitlichen Begriff der Verarbeitung ersetzt. Dies schließt freilich nicht aus, dass einzelne Rechtsvorschriften – wie bislang auch – allein beispielsweise die Erhebung, Speicherung oder Löschung personenbezogener Daten regeln.

(3) Zentraler Adressat der materiellen Regelungen der Datenschutz-Grundverordnung ist der **„Verantwortliche“**. Nach Art. 4 Nr. 7 DSGVO ist „Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung „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.“ Damit trägt die **Leitung** der jeweiligen öffentlichen Stelle die Verantwortung für den Datenschutz in ihrem Zuständigkeitsbereich.

(4) Das Instrument der Datenverarbeitung im Auftrag eines Verantwortlichen (vgl. nur den bisherigen Art. 6 BayDSG a. F.) findet sich auch in der Datenschutz-Grundverordnung wieder. Der Auftragnehmer wird hierbei aber nicht mehr, wie bislang geläufig, als „Auftragsdatenverarbeiter“, sondern – kürzer – als **„Auftragsverarbeiter“** bezeichnet. Gemäß Art. 4 Nr. 8 DSGVO ist „Auftragsverarbeiter“ eine „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“.

(5) Art. 4 Nr. 11 DSGVO enthält eine Definition der **„Einwilligung“** im Sinne der Datenschutz-Grundverordnung. Hiernach muss die betroffene Person für einen bestimmten Fall unmissverständlich ihren Willen bekunden, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Eine besondere Form sieht diese Begriffsbestimmung dabei zunächst nicht vor. Die Einwilligung muss jedoch freiwillig und in informierter Weise erklärt werden.

**Zur ordnungsgemäßen Umsetzung der Datenschutz-Grundverordnung ist es unerlässlich, dass sich die bayerischen öffentlichen – insbesondere staatlichen und kommunalen – Stellen mit den (teilweise vom bisherigen Sprachgebrauch abweichenden) Begrifflichkeiten der Datenschutz-Grundverordnung vertraut machen. Besonderes Augenmerk ist in diesem Zusammenhang auf die in Art. 4 DSGVO enthaltenen Begriffsbestimmungen zu legen.**

## 2. Grundsätze der Datenschutz-Grundverordnung für die Verarbeitung personenbezogener Daten

Auch wenn die Datenschutz-Grundverordnung gegenüber dem bisherigen nationalen Datenschutzrecht insbesondere in formeller Hinsicht einige Neuregelungen trifft, hat sie materiell-rechtlich die **bekannten und vertrauten Datenschutzgrundsätze** im Wesentlichen beibehalten und fortentwickelt. Diese Grundsätze sind in Art. 5 DSGVO („Grundsätze für die Verarbeitung personenbezogener Daten“) aufgeführt und werden durch die weiteren Vorschriften der Datenschutz-Grundverordnung konkretisiert.

Im Einzelnen:

(1) Art. 5 Abs. 1 Buchst. a DSGVO normiert die Grundsätze der Rechtmäßigkeit der Verarbeitung personenbezogener Daten, der Verarbeitung nach **Verarbeitung nach Treu und Glauben** sowie der **Transparenz**. Personenbezogene Daten müssen hiernach „auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden“.

(2) Der Grundsatz der **Zweckbindung** ist in Art. 5 Abs. 1 Buchst. b DSGVO festgelegt. Personenbezogene Daten dürfen hiernach nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Eine Weiterverarbeitung ist unzulässig, wenn sie mit diesen Erhebungszwecken nicht zu vereinbaren ist.

(3) Nach Art. 5 Abs. 1 Buchst. c DSGVO müssen „personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“. Diese (sprachlich etwas unglückliche) Formulierung entspricht inhaltlich im Wesentlichen dem Erforderlichkeitsgrundsatz, der bereits das geltende Datenschutzrecht prägt. Die Datenschutz-Grundverordnung spricht in diesem Zusammenhang aber vom Grundsatz der **„Datenminimierung“**. Vor diesem Hintergrund hat der Verantwortliche insbesondere zu prüfen, ob ein bestimmter Verarbeitungszweck tatsächlich die Verarbeitung personenbezogener Daten erfordert oder ob nicht vielmehr die Verarbeitung anonymisierter Daten ausreichend ist.

(4) Personenbezogene Daten müssen nach Art. 5 Abs. 1 Buchst. d DSGVO sachlich richtig sein. Soweit erforderlich, müssen sie 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 (Grundsatz der **„Richtigkeit“**).

(5) Art. 5 Abs. 1 Buchst. e DSGVO regelt den Grundsatz der **„Speicherbegrenzung“**: Demnach müssen personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Verarbeitungszwecke erforderlich ist. Ausnahmen hiervon sieht diese Vorschrift unter bestimmten Voraussetzungen für Verarbeitungen vor, die ausschließlich für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Abs. 1 DSGVO erfolgen.

(6) Nach dem in Art. 5 Abs. 1 Buchst. f DSGVO normierten Grundsatz der **„Integrität und Vertraulichkeit“** müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Dies schließt den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen ein. Konkretisierende Vorgaben hierzu in technischer und organisatorischer Hinsicht finden sich insbesondere in Art. 32 DSGVO.

Die Einhaltung der dargestellten Grundsätze für die Verarbeitung personenbezogener Daten ist durch den Verantwortlichen nachzuweisen (sog. **Rechenschaftspflicht**, Art. 5 Abs. 2 DSGVO).

# III. Die rechtmäßige (Weiter-)Verarbeitung personenbezogener Daten

## 1. Rechtmäßigkeit und Transparenz der Verarbeitung personenbezogener Daten, „Verarbeitung nach Treu und Glauben“

### a) Voraussetzungen

Nach Art. 6 Abs. 1 DSGVO ist die Verarbeitung personenbezogener Daten **nur rechtmäßig**, wenn mindestens eine der in dieser Vorschrift genannten Bedingungen erfüllt ist. Die Datenschutz-Grundverordnung führt somit den bekannten Grundsatz fort, dass die Verarbeitung personenbezogener Daten verboten ist, sofern nicht ein entsprechender Erlaubnistatbestand vorliegt (sogenanntes **„Verbot mit Erlaubnisvorbehalt“**).

Für eine rechtmäßige Verarbeitung personenbezogener Daten muss gemäß Art. 6 Abs. 1 DSGVO mindestens eine der folgenden Bedingungen vorliegen:

- Die betroffene Person hat in die Verarbeitung ihrer Daten **eingewilligt** (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO). In diesem Zusammenhang ist insbesondere zu beachten, dass die Einwilligung – wie bislang auch – unter anderem freiwillig erteilt werden muss (Art. 4 Nr. 11 DSGVO, vgl. bereits II. 1. unter [5]). Dies ist in Fällen, in denen der für die Datenverarbeitung Verantwortliche eine öffentliche Stelle ist, vielfach zweifelhaft (vgl. ErwGr 43 DSGVO).

- Die Verarbeitung ist – vereinfacht ausgedrückt – für die Erfüllung eines **Vertrags** mit der betroffenen Person erforderlich (Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO).

- Die Verarbeitung ist zur Erfüllung einer **rechtlichen Verpflichtung** des Verantwortlichen erforderlich (Art. 6 UAbs. 1 Abs. 1 Buchst. c DSGVO). Die rechtliche Verpflichtung muss sich dabei gemäß Art. 6 Abs. 3 UAbs. 1 DSGVO aus dem Unionsrecht oder dem Recht des jeweiligen Mitgliedstaats ergeben.

- Die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen (Art. 6 Abs. 1 UAbs. 1 Buchst. d DSGVO).

- Die Verarbeitung ist erforderlich, um eine **Aufgabe** wahrzunehmen, die **im öffentlichen Interesse** liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO).

  Dies stellt für die öffentlichen Stellen den **zentralen Erlaubnistatbestand** zur Verarbeitung personenbezogener Daten dar. Die Rechtsgrundlage für die Verarbeitung ergibt sich jedoch nicht allein und unmittelbar aus dieser Vorschrift, sondern ist vielmehr gemäß

Art. 6 Abs. 3 UAbs. 1 DSGVO durch Unionsrecht oder das Recht des jeweiligen Mitgliedstaats festzulegen („Öffnungsklausel" für die nationalen Gesetzgeber, vgl. bereits I. 2.).

– Die Verarbeitung ist – bei Durchführung einer Interessenabwägung – zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich (Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO). Dieser Erlaubnistatbestand gilt allerdings **nicht** für Verarbeitungen, die Behörden in Erfüllung ihrer Aufgaben vornehmen, vgl. Art. 6 Abs. 1 UAbs. 2 DSGVO.

**Für eine rechtmäßige Verarbeitung personenbezogener Daten muss mindestens eine der in Art. 6 Abs. 1 UAbs. 1 DSGVO genannten Bedingungen vorliegen. Zentraler Erlaubnistatbestand für die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist dabei Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO in Verbindung mit den jeweiligen Rechtsgrundlagen im nationalen Recht (beispielsweise im Bayerischen Datenschutzgesetz oder in den jeweiligen Fachgesetzen).**

## b) Besondere Kategorien personenbezogener Daten

Die Datenschutz-Grundverordnung knüpft die Verarbeitung bestimmter, besonders sensibler Datenarten an zusätzliche Voraussetzungen. Diese **„besonderen Kategorien personenbezogener Daten"** sind in Art. 9 Abs. 1 DSGVO abschließend genannt. Es sind dies personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, ferner genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten sowie Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person.

Die Verarbeitung dieser besonderen Kategorien personenbezogener Daten ist grundsätzlich untersagt (Art. 9 Abs. 1 DSGVO) und **nur zulässig**, wenn neben einem Erlaubnistatbestand nach Art. 6 Abs. 1 UAbs. 1 DSGVO **zusätzlich** ein Fall des Art. 9 Abs. 2 DSGVO vorliegt, zum Beispiel, wenn die betroffene Person in die Verarbeitung **ausdrücklich** eingewilligt hat (Art. 9 Abs. 2 Buchst. a DSGVO).

Viele der Ausnahmetatbestände des Art. 9 Abs. 2 DSGVO bedürfen jedoch der Ergänzung durch mitgliedstaatliches Recht, enthalten also „Öffnungsklauseln" (siehe hierzu bereits I. 2.). Dies betrifft beispielsweise Verarbeitungen im Zusammenhang mit dem Arbeitsrecht (Art. 9 Abs. 2 Buchst. b DSGVO), aus Gründen eines erheblichen öffentlichen Interesses (Art. 9 Abs. 2 Buchst. g DSGVO) oder aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (Art. 9 Abs. 2 Buchst. i DSGVO), weiterhin Verarbeitungen für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 DSGVO (Art. 9 Abs. 2 Buchst. j DSGVO).

Die Datenschutz-Grundverordnung stellt an das mitgliedstaatliche Recht dabei besondere Anforderungen, um dem hohen Schutzbedarf dieser besonders sensiblen Datenkategorien gerecht zu werden.

**III. Die rechtmäßige (Weiter-)Verarbeitung**

**Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn neben einem Erlaubnistatbestand nach Art. 6 Abs. 1 UAbs. 1 DSGVO zusätzlich ein Fall des Art. 9 Abs. 2 DSGVO – gegebenenfalls in Verbindung mit dem einschlägigen nationalen Recht (etwa im Bayerischen Datenschutzgesetz oder im jeweiligen Fachrecht) – vorliegt.**

## c) Transparenz, Treu und Glauben

Die in Art. 5 Abs. 1 Buchst. a DSGVO normierten Grundsätze der Transparenz und der Verarbeitung nach Treu und Glauben (siehe hierzu bereits II. 2. unter [1]) werden insbesondere durch die Vorschriften zu den **Rechten der betroffenen Person** (Art. 12 ff. DSGVO) konkretisiert. Diese Regelungen umfassen insbesondere:

- **Informationspflichten** des Verantwortlichen gegenüber der betroffenen Person im Zusammenhang mit der Erhebung personenbezogener Daten (Art. 13 f. DSGVO),
- ein **Auskunftsrecht** der betroffenen Person bezüglich der sie betreffenden personenbezogenen Daten, die von dem jeweiligen Verantwortlichen verarbeitet werden (Art. 15 DSGVO),
- das Recht der betroffenen Person auf **Berichtigung** der sie betreffenden Daten (Art. 16 DSGVO),
- das Recht der betroffenen Person auf **Löschung** („Recht auf Vergessenwerden", Art. 17 DSGVO); dieses Recht gilt aber unter anderem nicht, soweit die Verarbeitung erforderlich ist zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Art. 17 Abs. 3 Buchst. b in Verbindung mit Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und 3 DSGVO),
- das Recht der betroffenen Person auf **Einschränkung** der Verarbeitung (Art. 18 DSGVO),
- das Recht der betroffenen Person auf **Datenübertragbarkeit** (Art. 20 DSGVO); dieses Recht gilt aber 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 (Art. 20 Abs. 3 Satz 2 in Verbindung mit Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und 3 DSGVO),
- ein **Widerspruchsrecht** der betroffenen Person gegen die Verarbeitung sie betreffender personenbezogener Daten (Art. 21 DSGVO),
- das Recht der betroffenen Person, 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 (Art. 22 DSGVO).

Zu beachten ist hierbei jedoch, dass diese Betroffenenrechte durch mitgliedstaatliches Recht **eingeschränkt** werden können, wenn dies zum Schutz der in Art. 23 Abs. 1 DSGVO genannten wichtigen Ziele des allgemeinen öffentlichen Interesses des Mitgliedstaats erforderlich ist.

**Der tatsächliche Umfang der Betroffenenrechte gegenüber öffentlichen Stellen ergibt sich somit erst aus der Zusammenschau zwischen Art. 12 ff. DSGVO und dem jeweils einschlägigen Bundes- oder Landesrecht.**

## 2. Zweckändernde Verarbeitung personenbezogener Daten (Weiterverarbeitung)

Art. 5 Abs. 1 Buchst. b DSGVO normiert, wie dargestellt, den sogenannten **Zweckbindungsgrundsatz** (siehe hierzu bereits II. 2. unter [2]).

Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden (in der Terminologie der Datenschutz-Grundverordnung als **„Weiterverarbeitung“** bezeichnet), setzt nach dem Regelungskonzept der Datenschutz-Grundverordnung (vgl. Art. 6 Abs. 4 DSGVO) voraus:

(1) Die Weiterverarbeitung beruht entweder auf der **Einwilligung** der betroffenen Person oder auf einer **Rechtsvorschrift** der Union oder eines Mitgliedstaates, welche die Weiterverarbeitung regelt. Eine solche Rechtsvorschrift muss die in Art. 6 Abs. 4 DSGVO aufgeführten spezifischen Anforderungen erfüllen.

(2) Liegt keine der unter (1) genannten Konstellationen vor, ist gemäß Art. 6 Abs. 4 DSGVO gesondert zu prüfen, ob die Verarbeitung zu einem anderen Zweck mit dem ursprünglichen Erhebungszweck vereinbar ist (sogenannte **„Kompatibilitätsprüfung“**). Art. 6 Abs. 4 DSGVO gibt dabei einige Kriterien vor, die bei dieser Kompatibilitätsprüfung zu berücksichtigen sind.

Zu beachten ist, dass eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Abs. 1 DSGVO kraft gesetzlicher Fiktion als vereinbar mit den ursprünglichen (Erhebungs-)Zwecken gilt (Art. 5 Abs. 1 Buchst. b DSGVO). Einer gesonderten Kompatibilitätsprüfung bedarf es in diesen Fällen nicht.

# IV. Verantwortlicher, Auftragsverarbeiter und Datenschutzbeauftragter

## 1. Der Verantwortliche nach der Datenschutz-Grundverordnung

Die Regelungen der Datenschutz-Grundverordnung richten sich in erster Linie an den „Verantwortlichen“ (zum Begriff vgl. Art. 4 Nr. 7 DSGVO sowie II. 1. unter [3]). Der Verantwortliche ist für die Einhaltung der datenschutzrechtlichen Vorgaben der Datenschutz-Grundverordnung verantwortlich. Ihm obliegt es somit, die Rechtmäßigkeit der von ihm verantworteten Verarbeitungen personenbezogener Daten zu gewährleisten. Bestehen hinsichtlich einer bestimmten Verarbeitung mehrere Verantwortliche („gemeinsam Verantwortliche“), sind die Bestimmungen des Art. 26 DSGVO zu beachten.

Die Datenschutz-Grundverordnung weist dem Verantwortlichen in diesem Zusammenhang insbesondere (keine abschließende Aufzählung!) die folgenden Pflichten zu:

(1) Der Verantwortliche ist für die Einhaltung der in Art. 5 Abs. 1 DSGVO normierten Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich. Er muss die Einhaltung dieser Grundsätze nachweisen können (**„Rechenschaftspflicht“**, Art. 5 Abs. 2 DSGVO). Vgl. zum Ganzen bereits II. 2.

(2) Der Verantwortliche ist **Adressat der Rechte der betroffenen Personen** nach Art. 12 ff. DSGVO (gegebenenfalls in Verbindung mit dem hierbei einschlägigen nationalen Recht, vgl. bereits III. 1. c). Er hat somit sicherzustellen, dass diese Rechte ordnungsgemäß wahrgenommen werden können.

(3) Nach Art. 24 DSGVO hat der Verantwortliche im Hinblick auf die jeweilige Verarbeitung und unter Berücksichtigung der mit ihr einhergehenden Risiken für die Rechte und Freiheiten natürlicher Personen **angemessene und geeignete technische und organisatorische Maßnahmen** umzusetzen. Diese Verpflichtung wird insbesondere durch die Vorgaben des Art. 25 DSGVO („Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“) und des Art. 32 DSGVO („Sicherheit der Verarbeitung“) näher konkretisiert.

(4) Der Verantwortliche hat ein **Verzeichnis aller Verarbeitungstätigkeiten**, die seiner Zuständigkeit unterliegen, zu führen (Art. 30 DSGVO). Dieses Verarbeitungsverzeichnis stellt zugleich einen wichtigen Bestandteil dar, um der in Art. 5 Abs. 2 DSGVO normierten Rechenschaftspflicht Genüge zu tun.

(5) **Verletzungen** des Schutzes personenbezogener Daten hat der Verantwortliche nach Maßgabe des Art. 33 DSGVO an die zuständige Aufsichtsbehörde zu **melden**. Unter den Voraussetzungen des Art. 34 DSGVO sind in einem solchen Fall zudem die betroffenen Personen durch den Verantwortlichen zu **benachrichtigen**.

(6) Bei bestimmten Verarbeitungsvorgängen, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, hat der Verantwortliche vorab eine **Datenschutz-Folgenabschätzung** durchzuführen (Art. 35 DSGVO).

(7) Öffentliche Stellen haben als Verantwortliche in jedem Fall einen **Datenschutzbeauftragten** zu benennen (Art. 37 Abs. 1 Buchst. a DSGVO).

**„Verantwortlicher" im Sinne der Datenschutz-Grundverordnung ist diejenige öffentliche Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Art. 3 Abs. 2 BayDSG konkretisiert dies dahin, dass Verantwortlicher die für die Verarbeitung zuständige öffentliche Stelle ist, soweit nichts anderes bestimmt ist. Damit trägt die Leitung der jeweiligen öffentlichen Stelle die Verantwortung für den Datenschutz in ihrem Zuständigkeitsbereich.**

**Der Verantwortliche hat zu gewährleisten, dass die datenschutzrechtlichen Vorgaben der Datenschutz-Grundverordnung eingehalten werden und die Verarbeitung personenbezogener Daten in seinem Verantwortungsbereich rechtmäßig erfolgt. Er muss die Einhaltung der Verarbeitungsgrundsätze nachweisen können.**

## 2. Der Auftragsverarbeiter nach der Datenschutz-Grundverordnung

Die wesentlichen Vorgaben zur Auftragsverarbeitung und zu den damit einhergehenden **Pflichten des Auftragsverarbeiters** (zum Begriff vgl. Art. 4 Nr. 8 DSGVO sowie Überblick II. 1. unter [4]) sind in Art. 28 DSGVO geregelt. Auch jenseits dieser Norm weist die Datenschutz-Grundverordnung dem Auftragsverarbeiter verschiedene Pflichten zu, die teilweise denjenigen des Verantwortlichen entsprechen oder den Verantwortlichen bei der Erfüllung seiner eigenen Verpflichtungen unterstützen sollen.

Insbesondere (keine abschließende Aufzählung!) hat auch der Auftragsverarbeiter ein **Verarbeitungsverzeichnis** zu führen (Art. 30 Abs. 2 DSGVO), die **Sicherheit der Verarbeitung** nach Maßgabe des Art. 32 DSGVO zu gewährleisten und unter den Voraussetzungen des Art. 37 DSGVO einen **Datenschutzbeauftragten** zu benennen.

## 3. Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung

Öffentliche Stellen haben in jedem Fall einen Datenschutzbeauftragten zu benennen (Art. 37 Abs. 1 Buchst. a DSGVO). Die maßgeblichen Vorschriften hierzu stellen die Art. 37 ff. DSGVO dar.

Die **Mindestaufgaben** des Datenschutzbeauftragten sind in Art. 39 Abs. 1 DSGVO geregelt. Durch die Datenschutz-Grundverordnung erfährt allerdings die innerbehördliche Stellung des Datenschutzbeauftragten eine **grundsätzliche Wesensveränderung**: Während es

nach Art. 25 Abs. 4 Satz 1 BayDSG a. F. Aufgabe der behördlichen Datenschutzbeauftragen ist, auf die Einhaltung der datenschutzrechtlichen Vorschriften hinzuwirken, weist ihnen Art. 39 Abs. 1 Buchst. b DSGVO nunmehr die entsprechende Überwachungsaufgabe zu. Wie bisher verbleibt die Verantwortung für die Einhaltung des Datenschutzes jedoch allein bei der Leitung der öffentlichen Stelle (siehe bereits oben IV. 1.).

Eine ergänzende landesrechtliche Bestimmung zu behördlichen Datenschutzbeauftragten trifft insbesondere **Art. 12 BayDSG**.