

VORLESUNGSSKRIPT

Datenschutzrecht II – Rechtsgrundlagen, Pflichten & Betroffenenrechte

Art. 6 als Schaltzentrale, Einwilligung, sensible Daten,
Transparenz und die Rechte der Betroffenen

MODUL

**Governance, Risk, Compliance & Ethics – Teil
2**

SEMESTER

WS 26/27

VERSION

1.0

Prof. Dr. Markus Oermann

Dozent

markus.oermann@thws.de

Technische Hochschule Würzburg-Schweinfurt

Stand: 23.07.2026

Inhalt

1	Rechtsgrundlagen: Das Verbot mit Erlaubnisvorbehalt	3
2	Die Einwilligung in der Praxis	5
3	Höchste Warnstufe: Besonders sensible Daten	6
4	Transparenz durch Informationspflichten	8
5	Betroffenenrechte: Der Werkzeugkasten der Kontrolle	9
	5.1 Das Auskunftsrecht als Türöffner (Art. 15 DSGVO)	9
	5.2 Berichtigung, Löschung und die übrigen Rechte (Art. 16–21 DSGVO)	11
6	Quellen	12
	6.1 Literatur	12
	6.2 Normen & Standards	12
	6.3 Rechtsprechung	13

In der vorangegangenen Einheit haben wir das Fundament des Datenschutzrechts gelegt: den sachlichen und räumlichen Anwendungsbereich der DSGVO, den Begriff der personenbezogenen Daten (pbd) und die Rolle des Verantwortlichen, der über Zwecke und Mittel einer Verarbeitung entscheidet. Damit ist geklärt, *wann* das Datenschutzrecht überhaupt greift und *wer* in der Pflicht steht. Diese Einheit beantwortet die unmittelbar daran anschließende Frage: *Unter welchen Bedingungen* darf eine einmal als personenbezogen erkannte Datenverarbeitung tatsächlich stattfinden? Und welche Rechte stehen den betroffenen Personen dabei zu?

Wir bewegen uns dabei von den Erlaubnistatbeständen über die Pflichten des Verantwortlichen bis zu den durchsetzbaren Rechten der Betroffenen. Das ist kein Zufall, sondern spiegelt die innere Logik der DSGVO wider: Sie übersetzt den in der ersten Datenschutz-Einheit hergeleiteten Wert der informationellen Selbstbestimmung in ein System aus Erlaubnisvorbehalt, Transparenz und individuellen Kontrollrechten.

01

KAPITEL

Rechtsgrundlagen: Das Verbot mit Erlaubnisvorbehalt

Das Fundament des europäischen Datenschutzes beruht auf einem so simplen wie weitreichenden Prinzip: Jede Verarbeitung personenbezogener Daten ist zunächst einmal verboten. Erst wenn der Verantwortliche eine explizite gesetzlich vorgesehene Erlaubnis – eine Rechtsgrundlage – vorweisen kann, wird die Datenverarbeitung zulässig. Dieses System nennen Jurist/-innen „Verbot mit Erlaubnisvorbehalt“.

DEFINITION

Verbot mit Erlaubnisvorbehalt

Grundsätzliche Unzulässigkeit jeder Datenverarbeitung, es sei denn, eine gesetzliche Rechtsgrundlage (nach Art. 6 DSGVO) erlaubt sie ausdrücklich.

Die relevanten Erlaubnistatbestände finden sich in Art. 6 Abs. 1 DSGVO. Wenn nur eine der dort genannten Bedingungen erfüllt ist, leuchtet die datenschutzrechtliche Ampel grün. Die sechs Tatbestände der Buchstaben a bis f bilden gemeinsam die „Schaltzentrale“ des Datenschutzrechts: Jede Verarbeitung muss sich auf wenigstens einen von ihnen stützen lassen, sonst ist sie rechtswidrig.

DEEP DIVE Die sechs Erlaubnistatbestände des Art. 6 Abs. 1 DSGVO im Überblick

- **Einwilligung (lit. a):** Die betroffene Person hat den gesetzlichen Anforderungen entsprechend erklärt, mit der Verarbeitung einverstanden zu sein.
- **Vertragserfüllung (lit. b):** Die Verarbeitung ist objektiv notwendig, um einen Vertrag zu erfüllen. *Beispiel: Ein Online-Händler muss Ihre Adresse verarbeiten, um das Paket zu liefern; die Personalabteilung nutzt Ihre Kontodaten für die Gehaltszahlung.*
- **Rechtliche Verpflichtung (lit. c):** Der Verantwortliche muss ein Gesetz befolgen und dazu Daten verarbeiten (z. B. steuerrechtliche Aufbewahrungspflichten).
- **Schutz lebenswichtiger Interessen (lit. d):** Wenn es sprichwörtlich um Leben und Tod geht (z. B. Übermittlung von Blutgruppendaten an den Notarzt nach einem Unfall).
- **Aufgabenerfüllung im öffentlichen Interesse (lit. e):** Besonders wichtig für Behörden und staatliche Hochschulen: Wenn die Datenverarbeitungen für die Erfüllung einer gesetzlich festgelegten öffentlichen Aufgabe erforderlich ist. *Beispiel: Das Finanzamt darf Ihre steuerlich relevanten Daten verarbeiten.*
- **Berechtigtes Interesse (lit. f):** Die Verarbeitung ist zur Wahrung legitimer Interessen eines Unternehmens erforderlich und die Interessen der Betroffenen überwiegen nicht. *Achtung: Auf diese Rechtsgrundlage dürfen sich Behörden in Erfüllung ihrer öffentlichen Aufgaben nicht stützen.*

Zwei dieser Tatbestände verdienen besondere Aufmerksamkeit, weil sie eine detaillierte Prüfung erfordern. Die **Vertragserfüllung (lit. b)** trägt nur, soweit die Verarbeitung für den Vertrag *objektiv erforderlich* ist – die bloße Bequemlichkeit oder ein bloßer zusätzlicher Werbezweck reichen nicht. Das **berechtigte Interesse (lit. f)** ist die flexibelste, aber auch anspruchsvollste Grundlage: Es verlangt eine dreistufige Prüfung: (1) Ein legitimes Interesse des Verantwortlichen, (2) die Erforderlichkeit der Verarbeitung für die Wahrung dieses Interesses und (3) eine Abwägung, bei der die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen dürfen. Gerade weil lit. f keinen festen Katalog liefert, ist die saubere Dokumentation dieser Abwägung in der Praxis entscheidend.

In Praxis prüfen Sie stets, welche dieser Grundlagen einschlägig ist. Eine doppelte Absicherung ist dabei weder nötig noch sinnvoll: Eine einzige belastbare Rechtsgrundlage genügt vollauf. Wer mehrere Rechtsgrundlagen „auf Vorrat“ benennt, signalisiert eher Unsicherheit als Sorgfalt.

ÜBUNG · BEGRIFFE

Das Datenschutzrecht folgt dem Grundsatz des Verbots mit **Erlaubnisvorbehalt**: Die Verarbeitung ist nur legal, wenn mindestens eine Bedingung aus Art. 6 DSGVO erfüllt ist. Unternehmen können sich dabei auf ihr **berechtigtes Interesse** stützen, sofern die Rechte der Betroffenen nicht überwiegen.

02

KAPITEL

Die Einwilligung in der Praxis

Die Praxis neigt dazu, die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) als datenschutzrechtlichen „Freibrief“ zu missverstehen. Dabei ist die Einwilligung – legaldefiniert in Art. 4 Nr. 11 DSGVO und ausgestaltet in Art. 7 DSGVO – an strenge Wirksamkeitsvoraussetzungen geknüpft. Wer versucht, Datenschutzprobleme durch pauschales Abnicken durch die Betroffenen zu „heilen“, begibt sich auf juristisches Glatteis.

DEFINITION

Einwilligung (Consent)

Jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung.

Ein zentraler Pfeiler für eine wirksame Einwilligung ist die **Freiwilligkeit**. Die betroffene Person muss eine echte, unbeeinflusste Wahl haben. Ist diese Wahl aufgrund eines Machtgefälles eingeschränkt, wie es zum Beispiel im Arbeitsverhältnis zwischen Arbeitgeber und beschäftigter Person anzutreffen ist, gelten extrem strenge Maßstäbe (§ 26 Abs. 2 BDSG; zur unionsrechtlich umstrittenen Reichweite des § 26 BDSG vgl. EuGH, Ur. v. 30.03.2023 – C-34/21). Auch die Koppelung der Einwilligung an den Abschluss eines Vertrags unterminiert die Freiwilligkeit, wenn diese Daten für die Erfüllung des Vertrags gar nicht zwingend notwendig wären (vgl. Art. 7 Abs. 4 DSGVO). Hier ist allerdings vieles strittig.

Darüber hinaus erfordert eine Einwilligung zwingend eine aktive Handlung (**Opt-In**). Bloßes Still-schweigen, Untätigkeit oder gar vorausgefüllte Kästchen am Ende eines Webseiten-Formulars (Opt-Out) genügen den Anforderungen der DSGVO nicht. Das Einholen einer Zustimmung zur Nutzung von Analysetools wie Webtracking verlangt dieses aktive Opt-In, bevor der erste Datenfluss ausgelöst wird.

Zusätzlich müssen **Informiertheit und Bestimmtheit** gewahrt bleiben. Betroffene müssen vor der Datenerhebung in einfacher, präziser Sprache aufgeklärt werden, wer verarbeitet, was verarbeitet wird und vor allem wozu. Schließlich ist die **Widerruflichkeit** integraler Bestandteil des Konzepts: Jede rechtswirksame Einwilligung muss von der betroffenen Person jederzeit und so einfach wie die Abgabe widerrufen werden können. Dieser Widerruf wirkt jedoch nur für die Zukunft (*ex nunc*, also „von jetzt an“): Die bis zum Widerruf gestützt auf die Einwilligung erfolgte Verarbeitung bleibt rechtmäßig und wird nicht nachträglich rechtswidrig.

Eine eigene Schwelle gilt für **Minderjährige**: Beziehen sich Verarbeitungen auf Angebote von Diensten der Informationsgesellschaft (sprich alle internetbaiserten Dienste), die einem Kind direkt gemacht werden, ist die Einwilligung des Kindes nur rechtmäßig, wenn es das 16. Lebens-jahr vollendet hat (Art. 8 Abs. 1 DSGVO). Andernfalls bedarf es der Einwilligung oder Zustimmung

der Träger der elterlichen Verantwortung. Die Mitgliedstaaten dürfen diese Altersgrenze bis auf 13 Jahre absenken; Deutschland hat von dieser Öffnung keinen Gebrauch gemacht, sodass es bei 16 Jahren bleibt.

QUICK-CHECK

Welches Verhalten bei einem Cookie-Banner auf einer Website ist datenschutzrechtlich **unzulässig**?

Ein Banner mit einem Button für „Alles akzeptieren“ und einem gleichrangigen Button für „Alles ablehnen“.

Ein Banner, das ein vorausgefülltes Kästchen zur Zustimmung enthält oder nur einen „Alles akzeptieren“-Button anbietet, ohne eine einfache Ablehnung auf gleicher Ebene zu ermöglichen.

Ein Banner, das den Nutzer detailliert informiert und ihn aktiv seine Präferenzen auswählen lässt (Opt-In).

03

KAPITEL

Höchste Warnstufe: Besonders sensible Daten

Bestimmte Informationen im Leben eines Menschen sind von Natur aus derart sensibel, dass die herkömmlichen Rechtsgrundlagen des Art. 6 DSGVO und die sonstigen allgemeinen Pflichten der DSGVO schlicht nicht ausreichen, um sie angemessen zu schützen. Art. 9 DSGVO spannt daher einen deutlich rigideren Schutzschild auf.

Das Konzept unterscheidet zwischen „gewöhnlichen“ personenbezogenen Daten und solchen besonderer Kategorien. Die Norm statuiert für die Verarbeitung dieser sensiblen Daten in Absatz 1 erst einmal ein rigoroses und prinzipielles Verbot.

■ DEEP DIVE **Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO)**

Zu diesen besonders geschützten Informationen zählen Daten, aus denen Folgendes hervorgeht: - Rassistische und ethnische Herkunft - Politische Meinungen, religiöse oder weltanschauliche Überzeugungen - Gewerkschaftszugehörigkeit - Genetische Daten und biometrische Daten zur eindeutigen Identifizierung - Gesundheitsdaten sowie Daten zum Sexualleben oder zur sexuellen Orientierung

Natürlich sind auch hier Ausnahmen vom Verbot der Verarbeitung vorgesehen – sie sind jedoch deutlich enger gefasst. Eine Verarbeitung ist nur ausnahmsweise dann gestattet, wenn ganz spezifische, noch strengere Erlaubnistatbestände aus Art. 9 Abs. 2 DSGVO herangezogen werden können. Dies wäre beispielsweise eine **ausdrückliche**, isolierte Einwilligung exakt für diese extrem sensiblen Daten oder die Erfüllung zwingender Vorschriften aus dem Arbeits- und Sozialrecht. Der gesteigerte Maßstab – „ausdrücklich“ statt nur „unmissverständlich“ – verdeutlicht: Wer sensible Daten auf eine Einwilligung stützen will, muss diese gesondert, klar abgegrenzt und gezielt für genau diese Kategorie einholen.

Wenden Sie diese Systematik praktisch an und klassifizieren Sie die typischen Datenarten in die jeweilige rechtliche Schutzkategorie:

Wie sich diese Unterscheidung in der unternehmerischen Praxis äußern kann, zeigt das folgende Fallbeispiel.

FALLSTUDIE

Fall: Das Tattoo-Studio und der Instagram-Account

Ein angesagtes Tattoo-Studio lässt seine Kunden vor dem Stechen des Tattoos routinemäßig ein Formular unterschreiben. Inmitten eines langen Fließtextes auf Seite zwei verbirgt sich folgende Klausel: „Wir erheben mit dieser Erklärung Gesundheitsdaten von Ihnen (z. B. zu Infektionen), um das Tattoo sicher stechen zu können. Zudem fertigen wir im Anschluss Vorher-Nachher-Fotos des Werks für unseren Instagram-Kanal an.“

Lösung. **Lösung:** Hier offenbaren sich erhebliche rechtliche Mängel. Die ausdrückliche Abfrage von Gesundheitszuständen (z. B. Infektionen) erhebt Gesundheitsdaten und fällt damit in den Anwendungsbereich von Art. 9 DSGVO.

Die pauschale, in einem Fließtext versteckte Einwilligung ohne klare optische und inhaltliche Trennung der völlig unterschiedlichen Zwecke (medizinisch-gesundheitliche Vorbereitung der Behandlung versus Social-Media-Werbung im Internet) verfehlt die grundlegenden Anforderungen an die Informiertheit und Bestimmtheit. Eine ausdrückliche, spezifisch getrennte Zustimmung exakt für diese sensiblen Gesundheitsdaten fehlt. Die Einwilligung in dieser undifferenzierten Form ist höchstwahrscheinlich vollumfänglich unwirksam.

ÜBUNG · BEGRIFFE

Die Verarbeitung von sensiblen Daten, wie beispielsweise **Gesundheitsdaten**, unterliegt einem prinzipiellen Verbot gemäß **Art. 9 DSGVO**. Ausnahmen sind nur unter strengen Bedingungen möglich, etwa einer **ausdrücklichen** Einwilligung, die klar vom restlichen Text **abgehoben** erteilt werden muss.

04

KAPITEL

Transparenz durch Informationspflichten

Geheimnisvolles hat im Leben seinen Reiz, im Datenschutzrecht hingegen ist es hochproblematisch. Wer personenbezogene Daten verarbeitet, muss die Karten auf den Tisch legen. Transparenz ist nicht bloß eine höfliche Geste, sondern eine hart sanktionierte Rechtspflicht, die den Betroffenen überhaupt erst in die Lage versetzt, seine Rechte geltend zu machen.

Das **Transparenzgebot** des Art. 5 Abs. 1 lit. a DSGVO fordert unmissverständlich, dass Datenverarbeitungen für die betroffenen Personen nachvollziehbar sein müssen. Um dieses Ziel operativ sicherzustellen, statuiert die DSGVO ein engmaschiges Netz an Informationspflichten. Diese sind gemäß Art. 12 Abs. 1 DSGVO in präziser, transparenter und verständlicher Form sowie in einfacher Sprache bereitzustellen. Juristisches Kauderwelsch genügt den Anforderungen in der EU also ausdrücklich nicht.

Die Systematik der DSGVO unterscheidet bei der Informationserteilung zwischen zwei grundlegenden Erhebungskonstellationen:

DEFINITION

Direkterhebung (Art. 13 DSGVO)

Die Daten werden unmittelbar bei der betroffenen Person erhoben (z. B. Ausfüllen eines Online-Formulars). Die Information muss zwingend zum Zeitpunkt der Erhebung erfolgen.

DEFINITION

Dritterhebung (Art. 14 DSGVO)

Die Daten stammen aus anderen Quellen (z. B. Adresskauf, Web-Scraping). Hier müssen zusätzlich die Datenquelle und die genaue Kategorie der verarbeiteten Daten mitgeteilt werden.

Vergleichen Sie die inhaltlichen Unterschiede der Informationspflichten je nach Art der Datenerhebung im folgenden interaktiven Schaubild:

In der praktischen Umsetzung manifestieren sich diese Pflichten typischerweise in der allgegenwärtigen Datenschutzerklärung. Doch was gehört zwingend in dieses Dokument? Neben dem Namen und den Kontaktdaten des Verantwortlichen müssen die konkreten Zwecke und Rechtsgrundlagen der Verarbeitung offengelegt werden. Ebenso entscheidend sind die Speicherdauer (oder zumindest die Kriterien für deren Festlegung), potentielle Empfänger der Daten sowie etwaige Übermittlungen in Länder außerhalb der EU (sog. Drittländer). Nicht zuletzt bedarf es

einer unmissverständlichen Aufklärung über die Betroffenenrechte und das Beschwerderecht bei der zuständigen Aufsichtsbehörde.

■ DEEP DIVE Der Datenschutzbeauftragte in der Datenschutzerklärung

Ein interessantes Detail aus der Praxis: Muss der Datenschutzbeauftragte eigentlich namentlich in der Datenschutzerklärung aufgeführt werden? Nein, befand der Bundesgerichtshof. Es reicht aus, wenn ausreichende und leicht zugängliche Wege zur Kontaktaufnahme (wie eine Funktions-E-Mail-Adresse) zur Verfügung gestellt werden.

■ BGH, Urt. v. 14.05.2024 – VI ZR 370/22

Die Informationspflichten sind indes nicht uferlos. Sie entfallen beispielsweise dann, wenn die betroffene Person bereits über das entsprechende Wissen verfügt (Art. 13 Abs. 4 DSGVO). Auch der nationale Gesetzgeber kann Ausnahmen normieren. Das Bundesdatenschutzgesetz (BDSG) greift diese Ermächtigung auf und lässt Informationspflichten entfallen, wenn zwingende Geheimhaltungsinteressen, der Quellenschutz von Journalisten oder Belange der öffentlichen Sicherheit entgehen (§§ 29, 32, 33 BDSG).

ÜBUNG · BEGRIFFE

Werden Daten unmittelbar bei der Person erhoben, greift die **Direkterhebung** nach Art. 13 DSGVO. Fließen die Daten aus fremden Quellen zu, spricht man von der **Dritterhebung** gemäß Art. 14 DSGVO, wobei hier zwingend die **Quelle** der Daten mitgeteilt werden muss.

05

KAPITEL

Betroffenenrechte: Der Werkzeugkasten der Kontrolle

Wo Transparenz herrscht, wachsen auch die Kontrollmöglichkeiten. Sobald Daten verarbeitet werden, rüstet die DSGVO die betroffene Person mit einem beachtlichen juristischen Werkzeugkasten an Kontrollrechten aus (Art. 15 bis 21 DSGVO). Diese Rechte sind kein bloßer Anhang, sondern das durchsetzbare Gegenstück zu den Pflichten des Verantwortlichen. So wird die informationelle Selbstbestimmung individuell durchsetzbar.

5.1 Das Auskunftsrecht als Türöffner (Art. 15 DSGVO)

Ein scharfes Schwert im Repertoire des Betroffenen ist das Auskunftsrecht (Art. 15 DSGVO). Es dient als unerlässlicher **Türöffner**, um die Rechtmäßigkeit einer Verarbeitung überhaupt über-

prüfen zu können. Wer nicht weiß, was über ihn gespeichert ist, kann auch nichts korrigieren oder löschen lassen. Das Recht umfasst die Bestätigung, ob Daten verarbeitet werden, sowie eine detaillierte Auskunft über Zwecke, Empfänger und Speicherdauer.

Die Brisanz des Auskunftsanspruchs zeigt sich in der weiten Auslegung durch die Rechtsprechung. Der Anspruch ist nicht auf simple Stammdaten beschränkt. Der Bundesgerichtshof zieht den Kreis denkbar weit: Auch interne Vermerke, Telefonnotizen, Gesprächsprotokolle und E-Mails können personenbezogene Daten enthalten und sind dann vollumfänglich auskunftspflichtig.

Zudem ist das Motiv für das Auskunftersuchen in der Regel unbedeutend.

DEFINITION

Fehlendes Rechtsschutzbedürfnis beim Auskunftsanspruch?

Das Auskunftsrecht setzt kein spezifisches „Rechtsschutzbedürfnis“ voraus. Selbst wenn das primäre Ziel des Betroffenen völlig datenschutzfremd ist (z. B. Vorbereitung einer arbeitsrechtlichen Klage oder Überprüfung von Provisionsabrechnungen), steht dies dem Anspruch nach herrschender Rechtsprechung grundsätzlich nicht entgegen.

Darüber hinaus sichert Art. 15 Abs. 3 DSGVO das Recht auf eine **kostenlose Erstkopie** der verarbeiteten personenbezogenen Daten. Der BGH hat auch hier klargestellt, dass dies durchaus die Herausgabe tatsächlicher Dokumentenkopien (wie von Briefen oder E-Mails) bedeuten kann, sofern dies zum Verständnis der Daten erforderlich ist.

Diese weitreichenden Ansprüche finden ihre Grenze erst dort, wo sie mit den Rechten und Freiheiten anderer Personen kollidieren (Art. 15 Abs. 4 DSGVO), etwa wenn berechtigte Geschäftsgeheimnisse tangiert sind. Auch bei exzessiven Anträgen, also offenkundig unbegründeten oder häufig wiederholten Anträgen, kann der Verantwortliche die Auskunft verweigern oder ein angemessenes Entgelt verlangen.

FALLSTUDIE

Fall: Die misslungene Pflichtfachprüfung

Ein Jura-Student ist bei der staatlichen Pflichtfachprüfung in Nordrhein-Westfalen durchgefallen. Um Ansatzpunkte für eine Prüfungsanfechtung zu finden, fordert er vom zuständigen Prüfungsamt unter Berufung auf Art. 15 DSGVO die unentgeltliche Übersendung einer Kopie seiner gesamten Klausuren (stolze 348 Seiten) inklusive der handschriftlichen Gutachten und Randbemerkungen der Prüfer. Das Amt weigert sich aufgrund des Umfangs und der Rechte der Prüfer.

Lösung. Lösung: Der Anspruch nach Art. 15 DSGVO besteht tatsächlich vollumfänglich. Die schriftlichen Aufsichtsarbeiten des Studenten sowie die darauf bezogenen Prüfungsgutachten der Korrektoren stellen personenbezogene Daten dar. Auch die Rechte Dritter (Art. 15 Abs. 4 DSGVO) – hier die der Prüfer – stehen der Herausgabe nicht entgegen, da Prüfer ihre Korrekturanmerkungen ohnehin in dem Bewusstsein anfertigen, dass sie dem Prüfling im Rahmen der Akteneinsicht zugänglich gemacht werden müssen. Das Bundesverwaltungsgericht gab dem klagenden Studenten in letzter Instanz Recht. Das

Datenschutzrecht hebt hier faktisch die strengen Regularien des Verwaltungsverfahrenrechts aus.

BVerwG, Urt. v. 30.11.2022, 6 C 10.21 - Auskunft über Prüfungsunterlagen, Art. 15 DSGVO

Das Auskunftsrecht entwickelt sich in der Praxis zunehmend zur universellen Allzweckwaffe. Für Unternehmen und Behörden bedeutet das einen enormen organisatorischen Druck, Anfragen binnen des gesetzlichen Monats beauskunften zu können. Wer IT-Systeme nicht so baut, dass sie auf Knopfdruck vollständige Datenkopien auswerfen, manövriert sich unweigerlich in ein Compliance-Risiko.

QUICK-CHECK

Welche Aussage zum Auskunftsrecht nach Art. 15 DSGVO ist korrekt?

Das Auskunftsrecht kann vom Verantwortlichen verweigert werden, wenn der Betroffene die Informationen nutzen will, um eine arbeitsrechtliche Kündigungsschutzklage vorzubereiten. Der Auskunftsanspruch beschränkt sich auf strukturierte Stammdaten wie Name, Anschrift und Geburtsdatum in einer Datenbank.

Auch handschriftliche Vermerke, E-Mails und Prüfungsgutachten können einen Anspruch auf Herausgabe einer Kopie begründen, solange die Rechte anderer nicht überwiegen.

5.2 Berichtigung, Löschung und die übrigen Rechte (Art. 16–21 DSGVO)

Auf den durch die Auskunft geöffneten Zugang bauen die weiteren Rechte auf. Ist ein Datensatz inkorrekt, greift Art. 16 DSGVO mit dem Recht auf unverzügliche **Berichtigung**. Sind die Zwecke der Verarbeitung erfüllt oder widerruft die Person ihre zuvor erteilte Einwilligung, aktiviert sich das „Recht auf Vergessenwerden“ (**Recht auf Löschung**) nach Art. 17 DSGVO. Die Idee, dass digitale Daten nicht ewig fortbestehen sollten, hatte der Jurist Viktor Mayer-Schönberger als „Tugend des Vergessens“ beschrieben. Die DSGVO hat dieses Anliegen in einen durchsetzbaren Anspruch übersetzt.

Die Artikel 18 und 20 flankieren dieses Arsenal mit dem Recht auf **Einschränkung der Verarbeitung** sowie dem Recht auf **Datenübertragbarkeit**, welches der drohenden Monopolisierung von Nutzerdaten durch große Plattformen entgegenwirken soll. In der Praxis ist das Übertragbarkeitsrecht allerdings bislang kaum wirksam geworden.

Besondere strategische Relevanz entfaltet das Recht auf **Widerspruch** gemäß Art. 21 DSGVO. Es richtet sich vor allem gegen Verarbeitungen, die auf das **berechtigte Interesse** (Art. 6 Abs. 1 lit. f) gestützt werden, und kehrt die Beweislast um: Nach einem Widerspruch muss der Verantwortliche zwingende schutzwürdige Gründe nachweisen, die die Interessen der betroffenen Person überwiegen. Andernfalls hat er die Verarbeitung einzustellen. Gegen Direktwerbung ist der Widerspruch sogar voraussetzungslos möglich.

FALLSTUDIE**Fall: KI-Training durch Tech-Giganten**

Social-Media-Konzerne wie Meta (Facebook, Instagram) greifen für das Training ihrer hauseigenen generativen KI-Modelle zunehmend auf die massenhaft verfügbaren öffentlichen Beiträge, Fotos und Kommentare ihrer Nutzerschaft zurück.

Lösung. Lösung: Hier greift das Recht auf Widerspruch aus Art. 21 DSGVO. Nutzerinnen und Nutzer können der Verwendung ihrer datenschutzrechtlich relevanten Posts für das KI-Training widersprechen. Das Unternehmen muss die Verarbeitung dann einstellen, es sei denn, es kann zwingende schutzwürdige Gründe nachweisen, welche die Interessen der Betroffenen überwiegen. Eine Hürde, die bei massenhaftem KI-Training schwerlich pro Einzelperson zu nehmen ist.

Das Datenschutzrecht fordert Sie kontinuierlich auf, Datenkategorien zu unterscheiden und das Zusammenspiel von Einwilligung, Transparenz und Betroffenenrechten sauber, granular und präzise auszugestalten. Zielen Sie immer auf informierte Entscheidungen statt auf verschleierte Zustimmungsfällen.

Die fundierte rechtliche Begründung einer Datenverarbeitung ist keine nebensächliche Formalie für Legal-Nerds, sondern das essenzielle Fundament, ohne das fast jedes digitale Geschäftsmodell zur Compliancefalle werden kann. Damit ist der materielle Kern des Datenschutzrechts beschrieben: Wir wissen nun, *wann* (Anwendungsbereich, vorige Einheit), *unter welchen Bedingungen* (Rechtsgrundlagen, Art. 6/7/9) und *mit welchen Pflichten und Rechten* (Art. 12–21) verarbeitet werden darf. Die nächste Einheit wendet sich der Frage zu, wie diese Vorgaben technisch-organisatorisch abgesichert und durchgesetzt werden: Datensicherheit, Datenschutz-Folgenabschätzung, Privacy by Design, die Rolle des Datenschutzbeauftragten sowie Haftung, Bußgeld und Schadensersatz.

06

KAPITEL

Quellen

6.1 Literatur

- Mayer-Schönberger, V. (2010): *Delete. Die Tugend des Vergessens in digitalen Zeiten* (übersetzt von Frank Lachmann). Berlin University Press, Berlin.

6.2 Normen & Standards

- Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO), insb. Art. 4 Nr. 11, Art. 5 Abs. 1 lit. a, Art. 6, Art. 7, Art. 8, Art. 9, Art. 12–14, Art. 15–21. <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679>

- Bundesdatenschutzgesetz (BDSG), insb. § 26 Abs. 2, §§ 29, 32, 33. https://www.gesetze-im-internet.de/bdsg_2018/

6.3 Rechtsprechung

- BGH, Urt. v. 14.05.2024 – VI ZR 370/22 (namentliche Nennung des Datenschutzbeauftragten in der Datenschutzerklärung nicht zwingend).
- BVerwG, Urt. v. 30.11.2022 – 6 C 10.21 (Auskunftsanspruch nach Art. 15 DSGVO über Prüfungsklausuren und Korrekturgutachten).
- EuGH, Urt. v. 30.03.2023 – C-34/21 (zur unionsrechtlich umstrittenen Reichweite nationaler Beschäftigtendatenschutz-Normen, hier § 23 HDSIG / parallel § 26 BDSG).
- EuGH, Urt. v. 19.10.2016 – C-582/14 (Breyer; dynamische IP-Adresse als personenbezogenes Datum); fortgeführt durch BGH, Urt. v. 16.05.2017 – VI ZR 135/13.