



***Leitfaden zum Datenschutzrecht  
2. Auflage***

Ein Leitfaden für Mitglieder

## Impressum

### Autoren:

#### **Rechtsanwalt Dr. Oliver Hornung**

SKW Schwarz Rechtsanwälte

T +49 69 630001-65

[o.hornung@skwschwarz.de](mailto:o.hornung@skwschwarz.de)

### Bearbeitet von:

#### **Katharina Dietrich**

HESSENMETALL

Frankfurt am Main

T +49 69 95808-169

F +49 69 95808-126

[katharina.dietrich@hessenmetall.de](mailto:katharina.dietrich@hessenmetall.de)

### Herausgeber:

#### **HESSENMETALL**

Verband der Metall- und Elektro-Unternehmen Hessen e. V.

Emil-von-Behring-Straße 4, 60439 Frankfurt am Main

T +49 69 95808-0

F +49 69 95808-126

[info@hessenmetall.de](mailto:info@hessenmetall.de)

[www.hessenmetall.de](http://www.hessenmetall.de)

Dieser Leitfaden ist mit großer Sorgfalt erstellt worden. Er ersetzt gleichwohl die Beratung im Einzelfall nicht. Mit der Bitte um Verständnis wird darauf hingewiesen, dass keinerlei Haftung übernommen wird. Alle Angaben dieser Publikation beziehen sich grundsätzlich auf alle Geschlechter. Aus Gründen der einfacheren Sprache und ohne jede Diskriminierungsabsicht wurde auf eine Bezeichnung mit dem Genderstern \* verzichtet.

## Vorwort

Seit dem 25. Mai 2018 gelten in der gesamten Europäischen Union (EU) die Bestimmungen der Datenschutz-Grundverordnung (DS-GVO). Die DS-GVO stellt sicher, dass in allen Mitgliedstaaten der EU ein einheitlicher Datenschutzstandard besteht und die Rechte und Freiheiten der betroffenen Personen gewahrt werden.

Die Verarbeitung personenbezogener Daten kann in einer Vielzahl relevanter Geschäftsprozesse eine Rolle spielen – von der Personalverwaltung bis hin zu Stammdatenpflege von Geschäftskunden. Auch Unternehmen in der Metall- und Elektroindustrie müssen daher sicherstellen, dass sie alle notwendigen Anforderungen der DS-GVO umsetzen und über eine ausreichende Dokumentation zum Datenschutz verfügen.

Der Leitfaden, der aktuell in 2. Auflage erscheint, soll einen Überblick über die Anforderungen der DS-GVO liefern und hierbei die wichtigsten Fragestellungen für die Praxis aufzeigen. Um einen möglichst großen Mehrwert zu liefern, ist der Leitfaden mit einer Vielzahl an Beispielen und Links zu weiterführenden Informationen versehen, die in der betrieblichen Praxis herangezogen werden können. Es wurde beim Entwurf des Leitfadens bewusst darauf verzichtet, sämtliche Spezialprobleme zum Datenschutz aufzugreifen, sondern lediglich die für die Praxis relevantesten Themenfelder in der gebotenen Kürze aufzuzeigen. Ziel ist es somit, einen ersten Beitrag für eine solide Datenschutz-Compliance im Unternehmen bereitzustellen.

Eine abschließende und verbindliche rechtliche Beratung kann der vorliegende Leitfaden jedoch nicht bieten, weshalb für spezifische Fragen stets die Rechtsexperten hinzugezogen werden sollten.

Der Leitfaden ist von SKW Schwarz Rechtsanwälte für HESSENMETALL erstellt worden und wurde der VhU zur Verfügung gestellt, dafür bedanken wir uns sehr herzlich.

Dirk Pollert

Prof. Dr. Franz-Josef Rose

April 2026

# INHALTSVERZEICHNIS

Impressum .....	2
A. Wichtige Begriffsbestimmungen .....	6
B. Grundlagen der DS-GVO .....	6
Zielsetzung der DS-GVO .....	6
Anwendungsbereich der DS-GVO .....	7
1. Sachlicher Anwendungsbereich .....	7
2. Persönlicher Anwendungsbereich .....	8
Erlaubnis zur Verarbeitung personenbezogener Daten .....	8
1. Gesetzliche Erlaubnistatbestände mit Beispielen .....	9
2. Anforderungen an eine Einwilligung .....	10
Datenschutzgrundsätze aus Art. 5 DS-GVO .....	12
Rechtmäßigkeit, Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a) DS-GVO) .....	12
Zweckbindung (Art. 5 Abs. 1 lit. b) DS-GVO) .....	12
Datenminimierung (Art. 5 Abs. 1 lit. c) DS-GVO) .....	13
Richtigkeit (Art. 5 Abs. 1 lit. d) DS-GVO) .....	13
Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DS-GVO) .....	13
Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DS-GVO) .....	13
Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) .....	13
C. Pflichten aus der DS-GVO .....	13
Rechte der betroffenen Personen (einschl. Maßnahmen zur Transparenz) .....	14
1. Überblick zu Betroffenenrechten .....	14
2. Maßnahmen zur Transparenz .....	15
3. Das Auskunftsrecht gemäß Art. 15 DS-GVO .....	17
Formelle Pflichten der DS-GVO .....	19
1. Einbeziehung Dritter in die Datenverarbeitung .....	19
2. Verzeichnis von Verarbeitungstätigkeiten .....	21
3. Verletzung des Schutzes personenbezogener Daten .....	22
4. Datenschutz-Folgenabschätzung .....	25
5. Der Datenschutzbeauftragte .....	27
6. Drittlandtransfer .....	29
Technische und organisatorische Maßnahmen .....	31
1. Allgemeine Anforderungen .....	31

<b>2. Sonderfall: Vorhalten eines Löschkonzepts.....</b>	<b>32</b>
<b>Relevante Sonderkonstellationen .....</b>	<b>33</b>
<b>1. Videoüberwachung auf dem Betriebsgelände .....</b>	<b>33</b>
<b>2. Webseite und Social-Media .....</b>	<b>34</b>
<b>3. E-Mail und Internetnutzung im Unternehmen.....</b>	<b>36</b>

## A. Wichtige Begriffsbestimmungen

Um die nachstehenden Ausführungen verständlicher zu gestalten, sollen zunächst einige relevante Definitionen der DS-GVO aufgezeigt werden. Im weiteren Verlauf des Leitfadens werden die Begrifflichkeiten verwendet, ohne diese nochmal explizit zu definieren. Soweit eine weitergehende Erläuterung der jeweiligen Begriffe erforderlich ist, wird dies themenspezifisch im Rahmen des jeweiligen Gliederungspunktes vorgenommen.

**Personenbezogene Daten (Art. 4 Nr. 1 DS-GVO):** *Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche 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.*

**Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO):** *Personenbezogene 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.*

**Betroffene Person:** *Natürliche Person, deren Daten verarbeitet werden.*

**Verantwortlicher (Art. 4 Nr. 7 DS-GVO):** *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.*

**Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO):** *Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.*

**Verarbeitung (Art. 4 Nr. 2 DS-GVO):** *Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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.*

## B. Grundlagen der DS-GVO

### Zielsetzung der DS-GVO

Die DS-GVO zielt darauf ab, die Grundrechte und -freiheiten natürlicher Personen, insbesondere den Schutz personenbezogener Daten, zu gewährleisten. Gleichzeitig soll die Verordnung den freien Verkehr dieser Daten ermöglichen. Die DS-GVO balanciert diese auf den ersten Blick konträren Schutzziele, indem sie einerseits spezifische Rechte für betroffene Personen bereithält, andererseits jedoch klare Erlaubnistatbestände für die Verarbeitung personenbezogener Daten aufstellt. Für den betrieblichen Kontext kann man sich daher merken,

dass personenbezogene Daten bei Vorliegen einer Rechtsgrundlage verarbeitet werden dürfen, dies jedoch mit einer Vielzahl rechtlicher und formeller Verpflichtungen einhergeht.

## Anwendungsbereich der DS-GVO

Damit die Anforderungen der DS-GVO überhaupt zur Anwendung kommen, muss stets der Anwendungsbereich der Verordnung eröffnet sein.

### 1. Sachlicher Anwendungsbereich

Nach Art. 2 Abs. 1 DS-GVO gilt die Verordnung für die automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Für die betriebliche Praxis ist somit entscheidend,

- ob eine Verarbeitung stattfindet,
- ob die jeweiligen Daten als „personenbezogen“ anzusehen sind und
- ob ausnahmsweise auch eine nicht automatisierte Verarbeitung unter den Anwendungsbereich der DS-GVO fällt.

## Verarbeitung von Daten

Der Begriff der Verarbeitung umfasst alle Formen des Umgangs mit personenbezogenen Daten - von der Erhebung bis zur endgültigen Vernichtung. Man kann sich also merken, dass letztlich jeder Umgang mit personenbezogenen Daten auch eine Datenverarbeitung i. S. d. DS-GVO darstellt.

**Beispiele:** Kontaktdatenpflege im CRM-System, Veröffentlichung von Mitarbeiterfotos auf Social-Media, Videoüberwachung auf dem Betriebsgelände sowie das Durchführen eines BEM-Verfahrens.

## Personenbezug der Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Identifizierbar ist eine Person immer dann, wenn sie direkt oder indirekt (also mit den zur Verfügung stehenden Informationen) identifiziert werden kann. Typische Beispiele für personenbezogene Daten sind:

- Name
- Adresse
- Telefonnummer und E-Mail-Adresse
- Geburtsdatum und Geburtsort
- Staatsangehörigkeit

Daneben zählen auch finanzbezogene, gesundheitsbezogene, berufsbezogene sowie soziale und persönliche Merkmale als personenbezogene Daten, soweit sie einer natürlichen Person zugeordnet werden können.

Abschließend sollte man sich merken, dass auch gewisse „Exoten“ existieren, deren Einordnung als personenbezogene Daten ggf. nicht auf den ersten Blick ersichtlich ist. So ist z. B. auch die IP-Adresse als personenbezogenes Datum anzusehen, da sie unter Zuhilfenahme weiterer Informationen (des Internet-Providers) einer natürlichen Person zugeordnet werden kann. Die Frage der Identifizierbarkeit einer Person kann daher nicht nur auf Basis derjenigen Informationen beurteilt werden, die dem Verantwortlichen selbst zur Verfügung stehen. Auch das Zusatzwissen Dritter ist zu berücksichtigen, soweit dies mit verhältnismäßigen Mitteln für den Verantwortlichen erreichbar ist.

## Nicht automatisierte Datenverarbeitung

Automatisierte Datenverarbeitung ist die Verarbeitung personenbezogener Daten mithilfe von technischen Systemen, wie Computern oder Softwareprogrammen, die Vorgänge automatisch ausführen, ohne dass eine manuelle Eingabe erforderlich ist. Beispiele sind das Speichern, Abrufen, Ändern, Löschen oder Übermitteln von Daten durch digitale Systeme. Diese Verarbeitungsvorgänge unterfallen stets der DS-GVO.

Die nicht automatisierte Datenverarbeitung bezieht sich demgegenüber auf die manuelle Verarbeitung von personenbezogenen Daten, z. B. durch das Führen von Papierakten oder handgeschriebenen Listen. Nicht automatisierte Datenverarbeitungen fallen nur dann unter die DS-GVO, wenn die personenbezogenen Daten in einem strukturierten Dateisystem gespeichert sind oder gespeichert werden sollen. Ein strukturiertes Dateisystem ist hierbei eine Sammlung von Daten, die nach bestimmten Kriterien organisiert und zugänglich sind.

**Beispiel:** Alphabetisch geordnete Kundenlisten sowie in Papierform geführte Personalakten von Beschäftigten.

## 2. Persönlicher Anwendungsbereich

Die DS-GVO adressiert primär den sog. Verantwortlichen. In der betrieblichen Praxis wird es im absoluten Regelfall darauf hinauslaufen, dass das jeweilige Unternehmen personenbezogene Daten als Verantwortlicher verarbeitet. Dies gilt jedenfalls bei den typischen Verarbeitungsszenarien, etwa im Zusammenhang von Beschäftigten, Kunden und Geschäftspartnern. Daraus folgt, dass das jeweilige Unternehmen (nicht primär die Beschäftigten des Unternehmens!) die datenschutzrechtlichen Vorgaben der DS-GVO umsetzen müssen.

Soweit sich im Einzelfall einmal Abgrenzungsfragen stellen, z. B. da weitere Dienstleister bei der Datenverarbeitung hinzugezogen werden, werden diese spezifischen Fragen in eigenen Abschnitten des Leitfadens dargestellt.

## Erlaubnis zur Verarbeitung personenbezogener Daten

Die Verarbeitung von personenbezogenen Daten ist (nur) zulässig, wenn eine gesetzliche Vorschrift es erlaubt oder die betroffene Person in die Nutzung ihrer Daten eingewilligt hat. Die DS-GVO folgt dem etwas sperrigen Begriff des „Verbots mit Erlaubnisvorbehalt“, welcher jedoch nicht weiter irritieren sollte. Soweit eine Rechtsgrundlage zur Verarbeitung personenbezogener Daten vorliegt, dürfen die jeweiligen Daten auch verarbeitet werden.

## 1. Gesetzliche Erlaubnistatbestände mit Beispielen

Die gesetzlichen Vorschriften für eine erlaubte Datenverarbeitung finden sich hauptsächlich in Art. 6 DS-GVO.

Hiernach ist eine Datenverarbeitung auch **ohne Einwilligung** der betroffenen Person erlaubt, wenn:

- die Verarbeitung zur Erfüllung eines Vertrags erforderlich ist (z. B. Stammdaten, Zahlungsdaten und die Kundenadresse für eine Auftragsausführung), vgl. Art. 6 Abs. 1 lit. b) DS-GVO
- die Verarbeitung zur Durchführung vorvertraglicher Maßnahmen erforderlich ist (z. B. die E-Mail-Adresse für den Versand eines Kostenvoranschlags), vgl. Art. 6 Abs. 1 lit. b) DS-GVO
- die Verarbeitung zur Erfüllung rechtlicher Verpflichtungen erforderlich ist (z. B. die Einhaltung handels- und steuerrechtlicher Aufbewahrungspflichten), vgl. Art. 6 Abs. 1 lit. c) DS-GVO
- die Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen der betroffenen Person nicht überwiegen (z. B. die Videoüberwachung auf der Außenfläche des Betriebsgeländes), vgl. Art. 6 Abs. 1 lit. f) DS-GVO

### **Praxishinweis:**

Zur Rechtsgrundlage des Art. 6 Abs. 1 lit. f) DS-GVO sollte man sich jedoch merken, dass die Interessenabwägung in jedem Fall **zu dokumentieren** ist. Nur auf diese Weise kann der Verantwortliche sicherstellen und auch nachweisen, dass alle relevanten Abwägungskriterien berücksichtigt wurden. Die Umsetzung dieser Pflicht mag zunächst als bloße „Förmelei“ wirken, wird von Seiten der Datenschutzaufsichtsbehörden jedoch äußerst ernst genommen.

Die Verarbeitung von **Arbeitnehmer- oder Bewerberdaten** ist insbesondere zulässig, wenn sie:

- zur Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist (z. B. das Führen einer Personalakte und das Durchführen eines Bewerbungsverfahrens)
- zur Ausübung der Interessenvertretung der Beschäftigten erforderlich ist (z. B. die Weiterleitung von Arbeitnehmerdaten an den Betriebsrat)
- zur Aufdeckung von Straftaten erfolgt und zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat (z. B. bei begründetem Verdacht eines Diebstahls)
- zur Kontrolle der Einhaltung dienstlicher Weisungen und Vorschriften erforderlich ist (z. B. zur Kontrolle der Nutzung von dienstlichem Equipment)

**Praxishinweis:**

Ohne zu tief in die juristischen Einzelheiten einsteigen zu wollen, soll dennoch der ausdrückliche Hinweis angebracht werden, dass eine Betriebsvereinbarung **keine** eigenständige Rechtsgrundlage zur Datenverarbeitung darstellt. Auch wenn dies gegenläufig in § 26 Abs. 4 BDSG festgehalten wird und bislang auch die vielseitig gelebte Praxis darstellte, wurde dieser Vorgehensweise durch den Europäischen Gerichtshof (EuGH) nunmehr eine klare Absage erteilt (vgl. *Urteil vom 19. Dezember 2024 – Az. C-65/23*).

**Besondere Kategorien personenbezogener Daten** gelten in allen Verarbeitungsszenarien als besonders schutzwürdig und unterliegen daher gesonderten Anforderungen (Art. 9 DS-GVO). Für die betriebliche Praxis bedeutet das, dass z. B. die Verarbeitung von Gesundheitsdaten (z. B. Krankmeldungen) von Beschäftigten einer eigenständigen Rechtsgrundlage bedarf. Im konkreten Beispiel könnte auf die Vorschrift des Art. 9 Abs. 2 lit. b) DS-GVO abgestellt werden, wonach eine entsprechende Datenverarbeitung dann erlaubt ist, soweit der Arbeitgeber seinen aus dem Arbeitsrecht resultierenden Pflichten nachkommen muss. Da die Verarbeitung der Krankmeldung ohne Weiteres erforderlich ist, damit der Arbeitgeber den Anforderungen des Entgeltfortzahlungsgesetzes (EntgFG) nachkommen kann, ist auch eine entsprechende Datenverarbeitung erlaubt.

**Praxishinweis:**

Eine detaillierte Darstellung aller einschlägigen Verarbeitungsszenarien und Rechtsgrundlagen würde den Rahmen des vorliegenden Leitfadens überschreiten. Ebenfalls existieren (insbesondere im Beschäftigtendatenschutz) weiterführende Regelungen im Bundesdatenschutzgesetz (BDSG), deren Anwendbarkeit durch eine komplexe Rechtsprechung teils in Frage steht. Für eine erste Einordnung ist es jedoch ausreichend, sofern man die allgemeinen Rechtsgrundlagen zur Datenverarbeitung kennt und auch eine gewisse Sensibilität für die Verarbeitung besonderer Kategorien personenbezogener Daten entwickelt. Bei Zweifelsfragen ist stets der Datenschutzbeauftragte bzw. der Datenschutzkoordinator einzubeziehen, der sodann in eine detaillierte Prüfung einsteigt.

## 2. Anforderungen an eine Einwilligung

In einigen Fällen bedarf es einer Einwilligung der betroffenen Personen, um ihre personenbezogenen Daten verarbeiten zu dürfen. Dies ist immer dann der Fall, wenn keine gesetzliche Erlaubnis zur Datenverarbeitung vorliegt. Ein praktisch relevantes Beispiel ist etwa die Veröffentlichung von Mitarbeiterfotos auf Social-Media sowie die Nutzung von Tracking- und Analysetools auf der Webseite des Unternehmens.

Damit eine Einwilligung rechtswirksam ist, müssen die gesetzlichen Anforderungen der Art. 6 Abs. 1 lit. a) und 7 DS-GVO erfüllt sein. Bei der Prüfung und Ausgestaltung einer Einwilligung müssen daher jedenfalls die nachfolgenden Kriterien geprüft und umgesetzt werden.

### a) Freiwilligkeit der Einwilligung

Eine Einwilligung ist immer nur dann rechtmäßig, wenn sie freiwillig erteilt wurde. Jede Form von Druck, Zwang oder Verpflichtung führt zur Unwirksamkeit der Einwilligung. Eine Einwilligung gilt unter anderem bereits dann als unfreiwillig, wenn der Abschluss eines Vertrags oder die Erbringung einer Leistung von der Abgabe der Einwilligungserklärung abhängig gemacht wird und die betroffene Person keine Möglichkeit hat, die Leistung auch auf andere Weise zu erlangen.

Auch im Beschäftigungsverhältnis spielt die Freiwilligkeit der Einwilligung eine entscheidende Rolle. Aufgrund des Über- und Unterordnungsverhältnis zwischen Arbeitgeber und Arbeitnehmer muss die Freiwilligkeit der Einwilligung in diesen Fällen besonders gründlich geprüft werden. Probleme können immer dann auftreten, wenn die Gefahr besteht, dass der jeweilige Beschäftigte lediglich aufgrund eines gefühlten Zwangs handelt. Eine Freiwilligkeit ist demgegenüber dann anzunehmen, wenn der Beschäftigte einen Vorteil erlangt, oder Arbeitgeber und Arbeitnehmer zumindest gleichgelagerte Interessen verfolgen.

**Beispiel:** Aufnahme des Geburtsdatums in eine Geburtstagsliste.

## **b) Form der Einwilligung**

Einwilligungen müssen grundsätzlich nicht schriftlich erklärt werden; eine mündliche Einwilligung ist ebenso wirksam. Aus Beweis- und Dokumentationsgründen sollte die Einwilligungserklärung dennoch stets in Textform eingeholt werden.

## **c) Inhalt der Einwilligung**

Die DS-GVO stellt klare Mindestanforderungen an die Wirksamkeit einer Einwilligung auf. Eine Einwilligungserklärung muss daher jedenfalls folgende Informationen enthalten:

- Identität des Verantwortlichen (Angabe des Namens bzw. der Firma).
- Information zu den verarbeiteten Daten (z. B. Adresdaten, Kontodaten).
- Information zu den Zwecken der Datenverarbeitung (z. B. Werbung, Weitergabe an Dritte).
- Hinweis auf das Widerrufsrecht: Der Einwilligende hat das voraussetzungslose Recht, die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Es ist daher anzugeben, in welcher Form (Textform) und an welche Adresse (Postanschrift, E-Mail-Adresse) der Widerruf zu richten ist.

## **d) Optische Gestaltung**

Die Einwilligungserklärung muss optisch so gestaltet sein, dass sie direkt ins Auge fällt und vom Einwilligenden als solche wahrgenommen wird. Dieses Merkmal ist besonders wichtig, wenn die Einwilligungserklärung zusammen mit anderen Informationen, wie Allgemeinen Geschäftsbedingungen (AGB), in einem Text vorgelegt wird. Eine optische Abhebung kann z. B. durch Einrahmung, Fettdruck, andere Farben oder die Schriftgröße erreicht werden.

## **e) Aktive Erklärung erforderlich**

Die Einwilligung muss zudem aktiv erklärt werden und sollte durch eine eindeutige bestätigende Handlung erfolgen. Eine aktive Erklärung kann z. B. durch Anklicken eines Kästchens auf einer Webseite geschehen. Stillschweigen, das bloße Hinnehmen bereits angekreuzter Kästchen oder Untätigkeit der betroffenen Person stellen keine Einwilligung dar. Soll die datenschutzrechtliche Einwilligung gemeinsam mit weiteren Erklärungen abgegeben werden, sollte für jede Erklärung eine gesonderte Unterzeichnung oder ein gesondertes Anklicken vorgesehen werden.

## f) Gültigkeitsdauer

Eine Einwilligung ist trotz fehlender gesetzlicher Vorgaben nicht unbeschränkt gültig. Sie gilt immer nur so lange, wie die betroffene Person vernünftigerweise mit der Verarbeitung ihrer Daten rechnen muss. Wann ein solcher Zeitraum überschritten ist, muss am jeweiligen Einzelfall und nach Art und Umfang der Datenverarbeitung bewertet werden.

### **Weiterführende Informationen:**

Kurzpapier Nr. 20 (DSK) – Die Einwilligung nach der DS-GVO

Ratgeber zum Beschäftigtendatenschutz (LfDI Baden-Württemberg)

Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten im Lichte des EuGH-Urteils vom 30. März 2023 Rs. C-34/21 (Hessischer Beauftragter für Datenschutz und Informationsfreiheit)

## **Datenschutzgrundsätze aus Art. 5 DS-GVO**

In Art. 5 Abs. 1 und 2 DS-GVO werden die allgemeinen Datenschutzgrundsätze der DS-GVO geregelt. Die Grundsätze ziehen sich wie ein roter Faden durch die gesamte DS-GVO, weshalb deren Verständnis ein elementarer Bestandteil zum Aufbau einer Datenschutz-Compliance im Unternehmen ist.

### **Rechtmäßigkeit, Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a) DS-GVO**

In Art. 5 Abs. 1 lit. a) DS-GVO werden mehrere Datenschutzgrundsätze gebündelt. Jede Verarbeitung personenbezogener Daten muss auf einer rechtmäßigen Grundlage erfolgen, etwa auf Basis einer Einwilligung oder einer gesetzlichen Erlaubnis. Die Verarbeitung muss darüber hinaus fair ausgestaltet sein und für die betroffene Person in transparenter Weise erfolgen.

**Beispiel:** Ein Webseitenbesucher erteilt seine Einwilligung zur Verarbeitung seiner E-Mail-Adresse für die Zusendung eines Newsletters. In der Einwilligungserklärung muss der Kunde über Art, Umfang und Zwecke der Datenverarbeitung transparent und leicht verständlich aufgeklärt werden.

### **Zweckbindung (Art. 5 Abs. 1 lit. b) DS-GVO**

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden. Die Zwecke zur Datenverarbeitung sind vor der erstmaligen Erhebung der jeweiligen Daten zu bestimmen.

**Beispiel:** Ein Online-Shop erhebt personenbezogene Daten wie Name, Adresse und Zahlungsinformationen eines Kunden, um eine Bestellung abzuwickeln und die Waren zu versenden. Diese Daten dürfen grundsätzlich nicht für andere Zwecke, wie beispielsweise zur Versendung von Werbung, verwendet werden. Möchte das Unternehmen die Kundendaten (anders als ursprünglich vorgesehen) nunmehr auch für Werbezwecke verwenden, handelt es sich um eine sog. Zweckänderung, die weitere rechtliche Prüfschritte erfordert (vgl. Art. 6 Abs. 4 DS-GVO).

### Datenminimierung (Art. 5 Abs. 1 lit. c) DS-GVO)

Es dürfen nur diejenigen personenbezogenen Daten verarbeitet werden, die für den jeweiligen Zweck notwendig sind.

**Beispiel:** Ein Unternehmen erfasst nur die Adresse sowie Kontakt- und Zahlungsdaten des Kunden, nicht aber dessen Geburtsdatum, wenn die Angabe des Geburtstages zur Auftragserfüllung nicht erforderlich ist.

### Richtigkeit (Art. 5 Abs. 1 lit. d) DS-GVO)

Personenbezogene Daten müssen richtig und aktuell sein. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige Daten berichtigt oder gelöscht werden.

**Beispiel:** Ein Kunde meldet eine Adressänderung, weshalb das Unternehmen die Kundendaten sofort in seinem CRM-System aktualisiert.

### Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DS-GVO)

Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, notwendig ist.

**Beispiel:** Ein Unternehmen löscht die Daten ehemaliger Kunden und Beschäftigten nach Ablauf der gesetzlichen Aufbewahrungsfristen.

### Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DS-GVO)

Personenbezogene Daten müssen durch geeignete technische und organisatorische Maßnahmen geschützt werden, um die Sicherheit der Daten zu gewährleisten.

**Beispiel:** Ein Unternehmen verwendet verschlüsselte Datenübertragung und sichere Passwörter, um Kundendaten vor unbefugtem Zugriff zu schützen.

### Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO)

Der Verantwortliche muss in der Lage sein, die Einhaltung der DS-GVO nachzuweisen und entsprechende Maßnahmen und Verfahren dokumentieren. Die Rechenschaftspflicht ist einer der zentralen Grundsätze der DS-GVO, da die Umsetzung aller formellen Pflichten der DS-GVO häufig im besonderen Fokus der Datenschutzaufsichtsbehörden steht.

**Beispiel:** Ein Unternehmen führt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO und dokumentiert alle datenschutzrelevanten Prozesse sorgfältig.

## C. Pflichten aus der DS-GVO

Nachdem die Grundbegriffe der DS-GVO geklärt wurden, soll der Fokus nun auf die konkreten Pflichten für Unternehmen gelegt werden. Pflichten aus der DS-GVO lassen sich in vier unterschiedliche Themengebiete unterteilen:

- Pflichten, welche zur **Prüfung und Umsetzung von sog. Betroffenenrechten** umgesetzt werden. Die DS-GVO gibt Betroffenen eine ganze Palette an Rechten an die Hand, etwa zur Auskunft, zur Berichtigung oder zur Löschung personenbezogener Daten. Gleichsam fordert die DS-GVO **Maßnahmen zur Transparenz** gegenüber Betroffenen.
- **Formelle Pflichten der DS-GVO**, welche in einem engen Zusammenhang zur Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO stehen. Hiervon sind sämtliche Pflichten aus der DS-GVO betroffen, die eine Dokumentation der ergriffenen Maßnahmen zum Datenschutz darstellen. Die Erfahrung aus der Praxis zeigt, dass gerade diese formellen Pflichten gerne unterschätzt werden, obwohl die Datenschutzaufsichtsbehörden einen besonderen Fokus hierauf legen.
- Pflichten, welche den **technischen und organisatorischen Datenschutz** betreffen. Die entsprechenden Pflichten werden in den Art. 24, 25 und 32 DS-GVO abgebildet und adressieren den eigentlich Schutz personenbezogener Daten. Hier geht es also insbesondere um die Frage, welche Maßnahmen im Unternehmen ergriffen werden müssen, um ein dem jeweiligen Risiko angemessenes Datenschutzniveau zu gewährleisten. Als Sonderfall kann hierbei auch das Vorhalten eines **Löschkonzepts** im Unternehmen genannt werden, da auch ein Löschkonzept die Umsetzung technischer und organisatorischer Maßnahmen voraussetzt.
- Pflichten, die aus **relevanten Sonderkonstellationen** herrühren. Hierbei geht es weniger um allgemeine datenschutzrechtliche Anforderungen, sondern um die Darstellung praxisrelevanter Datenverarbeitungsvorgänge, die in einer Vielzahl von Unternehmen häufiger vorkommen.

## Rechte der betroffenen Personen (einschl. Maßnahmen zur Transparenz)

Das Datenschutzrecht gewährt Personen, deren Daten von Unternehmen genutzt werden, zahlreiche Rechte. Die Rechte sollen sicherstellen, dass die betroffenen Personen Einfluss auf die Nutzung und Verbreitung ihrer Daten nehmen können und sind in den Art. 12 bis 22 der DS-GVO festgelegt. Ergänzende Regelungen finden sich zudem in den §§ 32 bis 37 BDSG.

Das in Art. 12 DS-GVO verankerte Transparenzgebot legt hierbei zunächst fest, wie Informationen und Anfragen von Betroffenen zu behandeln sind und in welcher Form diese ausgestaltet werden müssen. Der Verantwortliche muss den Betroffenen alle Informationen und Mitteilungen präzise, transparent, verständlich, leicht zugänglich und in einer klaren und einfachen Sprache zukommen lassen. Obwohl mündliche Informationen grundsätzlich zulässig sind, wird aus Beweisgründen stets die schriftliche Form empfohlen, unabhängig davon, ob diese auf Papier oder elektronisch übermittelt wird.

### 1. Überblick zu Betroffenenrechten

Die DS-GVO sieht folgende Pflichten zur Transparenz sowie Betroffenenrechte vor:

- **Informationspflichten (Art. 13 und 14 DS-GVO):** Art. 13 DS-GVO definiert, welche Informationen der Verantwortliche dem Betroffenen erteilen muss, wenn Daten direkt

bei ihm erhoben werden. Art. 14 DS-GVO regelt demgegenüber die Informationspflichten, wenn die Daten von Dritten stammen, also nicht direkt bei der betroffenen Person erhoben werden.

- **Auskunftsrecht (Art. 15 DS-GVO):** Betroffene haben das Recht, vom datenverarbeitenden Unternehmen eine Bestätigung darüber zu verlangen, ob personenbezogene Daten über sie gespeichert und verarbeitet werden. Falls dies der Fall ist, muss das Unternehmen Auskunft über diese Daten, deren Herkunft und weitere Informationen erteilen. Auf Wunsch der betroffenen Person ist ihr zudem eine sog. „Kopie“ zu erteilen.
- **Recht auf Berichtigung (Art. 16 DS-GVO):** Sind personenbezogene Daten fehlerhaft, veraltet oder unvollständig, haben Betroffene gemäß Art. 16 DS-GVO das Recht auf Berichtigung.
- **Recht auf Löschung (Art. 17 DS-GVO):** Art. 17 DS-GVO gewährt den Betroffenen das Recht, die Löschung ihrer Daten zu verlangen, wenn einer der gesetzlich festgelegten Lösungsgründe vorliegt.
- **Recht auf Vergessenwerden (Art. 17 DS-GVO):** Das „Recht auf Vergessenwerden“ ist eine spezielle Form des Lösungsanspruchs, die sich auf veröffentlichte Daten bezieht und hierbei insbesondere auf Veröffentlichungen im Internet abzielt.
- **Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO):** Mit dem Recht auf Einschränkung der Verarbeitung können Betroffene in bestimmten Fällen erreichen, dass ihre Daten gesperrt und nicht weiterverarbeitet werden.
- **Recht auf Datenübertragbarkeit (Art. 20 DSGVO):** Das Recht auf Datenübertragbarkeit gibt Betroffenen unter bestimmten Bedingungen das Recht, eine Kopie ihrer personenbezogenen Daten in einem üblichen Dateiformat zu erhalten. Dadurch können sie ihre Daten von einem Anbieter zu einem anderen mitnehmen. Die Regelung soll den Wechsel zu einem anderen Anbieter, insbesondere bei sozialen Netzwerken oder Verträgen mit Energieversorgern, Banken und Versicherungen, erleichtern. Für Unternehmen in der Metall- und Elektroindustrie wird dieses Recht keine große praktische Relevanz haben.
- **Widerspruchsrecht (Art. 21 DSGVO):** Betroffene haben das Recht, der Verarbeitung ihrer Daten in gewissen Fällen zu widersprechen. Obwohl die Nutzung von Daten z. B. für Direktwerbung erlaubt ist, können Betroffene jederzeit und ohne Angabe von Gründen dagegen Widerspruch erheben.
- **Das Recht, nicht einer automatisierten Entscheidung unterworfen zu werden (Art. 22 DS-GVO):** Dies betrifft z. B. Fälle, in denen ein Bewerber automatisiert (etwa unter Einsatz von Künstlicher Intelligenz) abgelehnt wird, ohne dass ein Mensch die Entscheidung nochmal überprüft.

## 2. Maßnahmen zur Transparenz

Personen, deren Daten von einem Verantwortlichen verarbeitet werden, müssen vor Beginn der Datenverarbeitung informiert werden. Es stellt ein Grundprinzip der DS-GVO dar, dass Betroffene genau wissen sollen, welche Daten über sie verarbeitet werden und zu welchem Zweck dies erfolgt. Um Transparenz zu gewährleisten, sind Verantwortliche verpflichtet, den

Betroffenen umfassende Informationen über die geplante Nutzung ihrer Daten zu erteilen. Die spezifischen Informationen, die mitgeteilt werden müssen, sind in den Art. 13 und 14 DS-GVO sowie in den §§ 32 und 33 BDSG festgelegt.

Es gibt drei unterschiedliche Situationen, die bei der Erteilung von Informationen zu unterscheiden sind:

- Daten werden direkt bei der betroffenen Person erhoben. Da diese Konstellation den Regelfall einnimmt, soll hierauf nachstehend der Fokus gelegt werden.
- Daten werden nicht bei der betroffenen Person selbst, sondern bei einem Dritten erhoben.
- Der Verantwortliche hat die Daten bereits erhoben und möchte sie zu einem anderen Zweck nutzen als ursprünglich vorgesehen.

Wenn personenbezogene Daten direkt bei der betroffenen Person erhoben werden, wie z. B. bei Kunden oder Besuchern von Webseiten, müssen folgende Informationen gemäß Art. 13 Abs. 1 DS-GVO bereitgestellt werden:

- Identität des Verantwortlichen: Name und Kontaktdaten.
- Kontaktdaten des Datenschutzbeauftragten (DSB): Falls ein DSB bestellt ist, müssen dessen Kontaktdaten bereitgestellt werden.
- Verarbeitungszweck der Datennutzung: Beispielsweise für Werbemaßnahmen oder zur Vertragsabwicklung.
- Rechtsgrundlage der Datenverarbeitung: Entweder die gesetzliche Grundlage für die Datenerhebung oder die Einwilligung des Betroffenen. Bei der Einwilligung muss auch auf das Widerrufsrecht hingewiesen werden.
- Empfänger oder Kategorien von Empfängern der Daten: Falls Daten an Dritte weitergeleitet werden, beispielsweise an Dienstleister oder konzernverbundene Unternehmen.
- Dauer der Verarbeitung oder Datenspeicherung: Es ist möglichst genau darüber zu informieren, für welchen Zeitraum die jeweilige Datenverarbeitung erfolgt.
- Rechte der Betroffenen: Zum Beispiel das Recht auf Auskunft, Berichtigung und Löschung.
- Hinweis auf das Beschwerderecht bei der Aufsichtsbehörde.
- Hinweis, ob die Bereitstellung der Daten für den Abschluss oder die Abwicklung eines Vertrags erforderlich ist.

Vergleichbare Informationen müssen auch dann bereitgestellt werden, sofern die jeweiligen Daten bei einem Dritten erhoben wurden (vgl. Art. 14 Abs. 1 DS-GVO) oder sofern eine sog. Zweckänderung vorliegt (vgl. Art. 13 Abs. 3 DS-GVO).

**Zeitpunkt der Information:** Bei der direkten Erhebung von Daten bei der betroffenen Person müssen die Informationen zum Zeitpunkt der Datenerhebung mitgeteilt werden. Wenn die Daten nicht direkt bei der betroffenen Person erhoben werden, muss der Verantwortliche die Informationen innerhalb einer angemessenen Frist, spätestens jedoch nach einem Monat, bereitstellen.

**Ausnahmen von der Informationspflicht:** Die Information der betroffenen Person ist dann nicht erforderlich, wenn sie bereits Kenntnis über die relevanten Informationen hat. Wenn die Daten bei einem Dritten erhoben werden, kann die Information unterbleiben, wenn die Bereitstellung der Informationen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde. Die Ausnahmen werden im absoluten Regelfall nicht eingreifen, sodass der Grundsatz gilt: Informieren!

**Formvorschriften:** Die Informationen müssen gemäß Art. 12 Abs. 1 DS-GVO präzise, transparent, verständlich und leicht zugänglich in einer klaren und einfachen Sprache bereitgestellt werden. Bei der Erteilung der jeweiligen Informationen sollte ein sog. „Medienbruch“ vermieden werden. Besucher der Webseite eines Unternehmens sollten die jeweiligen Informationen daher in einem digitalen Format auf der Webseite einsehen können.

**Weiterführende Informationen:**

[Kurzpapier Nr. 10 \(DSK\) – Informationspflichten bei Dritt- und Direkterhebung](#)

[Themenseite zu Informationspflichten mit weitergehenden Mustern und Links \(LDA Bayern\)](#)

### 3. Das Auskunftsrecht gemäß Art. 15 DS-GVO

Das Auskunftsrecht der betroffenen Personen aus Art. 15 DS-GVO ist das zentrale Recht, um bei Bedarf gezielt weitere Rechte, z. B. das Recht auf Berichtigung oder Löschung, geltend zu machen. Die betroffene Person kann von dem Verantwortlichen eine Bestätigung darüber verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Sofern dies der Fall ist, hat die betroffene Person bezüglich dieser Daten ein Recht auf Auskunft.

Das hat zur Folge, dass der betroffenen Person konkret mitzuteilen ist, welche Daten verarbeitet werden. Grundvoraussetzung hierfür ist zunächst, dass eine lückenlose Kenntnis über die jeweils verarbeiteten Daten besteht. Das setzt voraus, dass sämtliche relevanten IT-Systeme sowie händische Verarbeitungsvorgänge herausgearbeitet und die dabei verarbeiteten personenbezogenen Daten bestimmt werden. Als erster Anhaltspunkt kann insoweit das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DS-GVO herangezogen werden. Die eigentliche Auskunft betrifft sodann z. B. Name, Adresse, Geburtsdatum, Beruf und sämtliche weiteren Informationen zum Verhältnis zur betroffenen Person. Die Art und Anzahl der bereitzustellenden Informationen muss natürlich am jeweiligen Einzelfall bewertet werden und ist kontextbezogen zu bestimmen. Im Regelfall wird es darum gehen, der betroffenen Person „genügend“ Information zur Verfügung zu stellen, sodass sie die ihr aus der DS-GVO zustehenden Rechte umsetzen kann.

Die Auskunftserteilung erstreckt sich darüber hinaus auf die folgenden Angaben:

- Zwecke für die Verarbeitung der personenbezogenen Daten
- Kategorien personenbezogener Daten, die verarbeitet werden
- Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (insb. Empfänger in Drittländern oder int. Organisationen)
  - **Wichtig:** Es wurde bereits mehrfach gerichtlich geurteilt und stellt das einheitliche Meinungsbild der Datenschutzaufsichtsbehörden dar, dass der Betroffene

die namhafte Benennung aller Datenempfänger fordern kann! Für Unternehmen bedeutet das, dass alle Datenempfänger tatsächlich bekannt sein müssen, um den gesetzlichen Anforderungen des Art. 15 Abs. 1 DS-GVO entsprechen zu können.

- geplante Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- Bestehen eines Rechts auf Berichtigung, Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchs gegen die Verarbeitung
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- Informationen über die Herkunft der Daten (soweit die Daten nicht bei der betroffenen Person erhoben werden)
- Bestehen einer automatischen Entscheidungsfindung einschließlich Profiling gem. Art. 22 Abs. 1, 4 DS-GVO 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
- Bezeichnung der geeigneten Garantien gem. Art. 46 DS-GVO zur Wahrung eines angemessenen Datenschutzniveaus bei Übermittlungen in Drittländer oder an internationale Organisationen

**Erteilung einer Kopie:** Der betroffenen Person ist darüber hinaus auf Wunsch eine Kopie der sie betreffenden personenbezogenen Daten auszuteilen. Das Unternehmen hat der betroffenen Person eine originalgetreue und verständliche Reproduktion sämtlicher sie betreffende personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen. Der betroffenen Person ist darüber hinaus eine Kopie von Auszügen aus Dokumenten oder Datenbanken, die ihre personenbezogenen Daten enthalten, zu gewähren, sofern dies für die wirksame Ausübung der durch die DS-GVO verliehenen Rechte erforderlich ist. Der Anspruch auf Erhalt einer Kopie bezieht sich daher nicht originär auf die jeweiligen Dokumente selbst, sondern auf die darin enthaltenen personenbezogenen Daten. Die Herausgabe entsprechender Dokumente wird jedoch immer dann erforderlich sein, sofern eine Kontextualisierung der verarbeiteten Daten erforderlich ist und so die Verständlichkeit der Auskunft gewährleistet wird. Der EuGH spricht „insbesondere“ von Angaben in Freitextfeldern, die regelmäßig die Bereitstellung des jeweiligen Dokuments erfordern.

**Beachtung Rechte Dritter:** Bei der Erfüllung des Auskunftsanspruchs muss zudem darauf geachtet werden, dass keine Rechte und Freiheiten Dritter beeinträchtigt werden. Das betrifft sowohl Rechte wie Geschäftsgeheimnisse oder das Urheberrecht, als auch sämtliche Rechte anderer betroffener Personen, deren personenbezogene Daten vom Unternehmen verarbeitet werden. Ggf. kann es daher erforderlich sein, Schwärzungen an vorzulegenden Dokumenten vorzunehmen.

**Form der Auskunft:** Die Auskunftserteilung an die betroffene Person kann grundsätzlich schriftlich, elektronisch oder auf Wunsch der betroffenen Person auch mündlich erfolgen. Stellt die betroffene Person ihren Antrag z. B. elektronisch, so ist ihr die Auskunft in einem gängigen elektronischen Format (z. B. PDF) zur Verfügung zu stellen. Hierbei ist in jedem Fall sicherzustellen, dass eine sichere (also hinreichend verschlüsselte) Datenübermittlung stattfindet.

**Frist zur Auskunftserteilung:** Unternehmen müssen unverzüglich tätig werden, sobald die betroffene Person Rechte nach den Art. 15 ff. DS-GVO geltend macht. Spätestens innerhalb eines Monats muss der Antragsstellung bzw. dem Begehren der betroffenen Person beim Vorliegen der gesetzlichen Voraussetzungen entsprochen werden. Die Monatsfrist kann auf bis zu drei Monate verlängert werden, soweit die Komplexität und die Anzahl der Anträge es erforderlich machen. Die betroffene Person muss über die Verlängerung der Frist und über die entsprechenden Gründe innerhalb eines Monats benachrichtigt werden.

**Weiterführende Informationen:**

[Kurzpapier Nr. 6 \(DSK\) – Auskunftsrecht der betroffenen Personen, Art. 15 DS-GVO](#)

[Themenseite zur Auskunft gemäß Art. 15 DS-GVO mit weitergehenden Mustern und Links \(LDA Bayern\)](#)

## Formelle Pflichten der DS-GVO

Die Umsetzung aller Anforderungen der DS-GVO setzt in weiten Teilen auch die Einhaltung formeller Pflichten voraus. Da die DS-GVO eine Vielzahl entsprechender Pflichten vorsieht, sollen die für die Praxis relevantesten Fälle nachstehend aufgezeigt werden.

### 1. Einbeziehung Dritter in die Datenverarbeitung

Datenschutzrechtliche Pflichten können zunächst aufkommen, sofern Dritte in die Datenverarbeitung einbezogen werden. Im Kern lassen sich hierbei zwei Konstellationen voneinander unterscheiden:

- Einbeziehung von Dienstleistern (z. B. IT-Support oder Hosting)
- Einbeziehung weiterer (ggf. auch konzernverbundener) Unternehmen, die arbeitsteilig bei der Datenverarbeitung zusammenwirken

Aus datenschutzrechtlicher Sicht entfaltet die Einbindung weiterer Unternehmen insoweit eine Relevanz, als die jeweiligen Rollen zwischen den Beteiligten zu klären sind. Es ist insbesondere zu prüfen, ob eine getrennte oder gemeinsame Verantwortlichkeit besteht, oder ob der Dritte als Auftragsverarbeiter i. S. d. Art. 28 DS-GVO anzusehen ist.

### Auftragsverarbeitung

Eine Auftragsverarbeitung liegt vor, wenn ein Unternehmen personenbezogene Daten für seine eigenen Zwecke nutzt, die tatsächliche Verarbeitung und Aufbereitung der Daten jedoch nicht selbst durchführt, sondern an einen Dienstleister auslagert. Der Dienstleister verarbeitet die Daten im Auftrag und auf strikte Weisung des Verantwortlichen. Das ist beispielsweise der Fall bei Cloud-Anbietern, die Daten auf ihren Servern für das Unternehmen speichern, oder bei Dienstleistern, die sich zu Zwecken des IT-Supports per Fernwartung auf die Server des Verantwortlichen einwählen.

Der wichtigste Aspekt bei der Auftragsverarbeitung ist die Verpflichtung, einen den Anforderungen des Art. 28 DS-GVO entsprechenden Vertrag zur Auftragsverarbeitung mit dem Dienstleister abzuschließen.

**Form des Vertrags zur Auftragsverarbeitung:** Art. 28 DS-GVO schreibt keine spezielle Form vor. Aus Gründen der Dokumentation und Beweisführung ist es jedoch ratsam, einen Vertrag in Textform abzuschließen. Der Vertrag kann dabei in elektronischer Form (z. B. pdf) oder schriftlich auf Papier geschlossen werden.

**Inhalt des Vertrags zur Auftragsverarbeitung:** Artikel 28 DS-GVO legt zahlreiche Mindestanforderungen für den Inhalt einer Auftragsverarbeitung fest. Dazu gehören insbesondere folgende Punkte:

- Gegenstand des Auftrags
- Dauer des Auftrags
- Zweck der Datenverarbeitung
- Art der zu verarbeitenden Daten
- Kategorien der betroffenen Personen
- Ergreifung der erforderlichen technischen und organisatorischen Maßnahmen
- Genehmigte Unterauftragsverarbeiter
- Umfang der Weisungsbefugnisse
- Rückgabe von Datenträgern nach Beendigung des Auftrags

**Wichtig:** Der Europäische Datenschutzausschuss (EDSA) fordert, dass Unternehmen im Falle des Einsatzes von Auftragsverarbeitern Kenntnis über die gesamte Verarbeitungskette haben. Unternehmen müssen daher prüfen, welche weiteren Unterauftragsverarbeiter eingesetzt werden und ob hierbei z. B. ein Drittlandtransfer i. S. d. Art. 44 ff. DS-GVO stattfindet. Auch bei einer Auslagerung der Datenverarbeitung an Dritte bleibt es bei dem Grundsatz: Verantwortlich heißt verantwortlich – und zwar in der gesamten Verarbeitungskette!

**Weiterführende Informationen:**

[Kurzpapier Nr. 13 \(DSK\) - Auftragsverarbeitung](#)

[Muster für einen Vertrag zur Auftragsverarbeitung \(Hessischer Beauftragter für Datenschutz und Informationsfreiheit\)](#)

[Muster für einen Vertrag zur Auftragsverarbeitung \(LfDI Baden-Württemberg\)](#)

### **Gemeinsame Verantwortlichkeit**

Eine gemeinsame Verantwortlichkeit liegt gemäß Art. 26 DS-GVO vor, wenn mehrere Unternehmen gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden. Typische Beispiele hierfür sind:

- Gemeinsamer Betrieb eines Bewerberportals im Konzern
- Gemeinsamer Betrieb eines Online-Shops durch mehrere Unternehmen
- Gemeinsame Nutzung eines CRM-Systems im Konzern

Wie den vorgenannten Fällen entnommen werden kann, spielt die gemeinsame Verantwortlichkeit für Unternehmen in der Metall- und Elektroindustrie regelmäßig (nur) dann eine Rolle, wenn konzernverbundene Unternehmen bei der Verarbeitung personenbezogener Daten zusammenwirken.

Wie auch bei der Auftragsverarbeitung, muss auch im Falle einer gemeinsamen Verantwortlichkeit ein Vertrag zwischen allen (gemeinsam) Verantwortlichen abgeschlossen werden, der die Anforderungen des Art. 26 DS-GVO abbildet.

**Inhalt des Vertrags:** Ein Vertrag zur gemeinsamen Verantwortlichkeit muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Die Verantwortlichen müssen insbesondere klären, wer von ihnen welche Verpflichtung gemäß der DS-GVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß Art. 13 und 14 DS-GVO nachkommt. Das Wesentliche der Vereinbarung ist den betroffenen Personen als erweiterte Information zur Verfügung zu stellen.

**Weiterführende Informationen:**

Kurzpapier Nr. 16 (DSK) – Gemeinsame Verantwortlichkeit

Muster für einen Vertrag zur gemeinsamen Verantwortlichkeit sowie Muster zur Informationserteilung an Betroffene (LfDI Baden-Württemberg)

## 2. Verzeichnis von Verarbeitungstätigkeiten

Unternehmen, die personenbezogene Daten verarbeiten, müssen alle Verarbeitungsprozesse im sogenannten „Verzeichnis von Verarbeitungstätigkeiten“ (kurz auch „VVT“) gemäß Art. 30 DS-GVO dokumentieren. Das VVT dient dazu, eine klare Übersicht über alle datenschutzrelevanten Abläufe im Unternehmen zu schaffen und letztlich bei der Einhaltung der datenschutzrechtlichen Vorschriften zu unterstützen.

Die Verpflichtung zur Dokumentation der Datenverarbeitungsprozesse und die spezifischen Anforderungen an die Dokumentation sind in Art. 30 DS-GVO festgelegt. Gemäß Art. 30 DS-GVO müssen alle Tätigkeiten dokumentiert werden, bei denen personenbezogene Daten verarbeitet werden. Solche Tätigkeiten können in verschiedenen betrieblichen Kontexten auftreten, wie beispielsweise bei der Erstellung und Veränderung einer Kundendatei, der Verwaltung von Mitarbeiterdaten oder der Nutzung einer Videoüberwachung auf dem Betriebsgelände.

Die Pflichtangaben in einem VVT sind:

- Name und Kontaktdaten des Verantwortlichen
- Name und Kontaktdaten des Datenschutzbeauftragten (DSB), falls ein DSB bestellt wurde
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen (z. B. Kunden, Mitarbeiter, Zulieferer)
- Beschreibung der Kategorien personenbezogener Daten (z. B. einfache Adressdaten oder besonders sensible Daten)
- Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt wurden oder werden (z. B. Weitergabe an eingesetzte IT-Dienstleister)

- Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- Wenn möglich, eine Beschreibung der technischen und organisatorischen Maßnahmen

**Praxishinweis:**

Das VVT ist nicht selten die erste Anlaufstelle im Falle einer aufsichtsbehördlichen Prüfung. Eine entsprechende Dokumentation kann daher als das „Herzstück“ der Datenschutz-Compliance im Unternehmen angesehen werden. Eine sorgsame Pflege sowie die regelmäßige Aktualisierung des VVT sollten daher mit höchster Priorität im Unternehmen behandelt werden!

Um die Pflege und Aktualisierung des VVT sicherzustellen, sollte im Unternehmen daher ein klarer Ablaufplan etabliert und an alle Beschäftigten kommuniziert werden. Wer ist z. B. für die Meldung eines neuen IT-Systems verantwortlich und welche Informationen werden hierbei benötigt?

**Weiterführende Informationen:**

[Kurzpapier Nr. 1 \(DSK\) – Verzeichnis von Verarbeitungstätigkeiten](#)

[Hinweise zum Verzeichnis von Verarbeitungstätigkeiten \(DSK\)](#)

[Mustervorlage für ein Verarbeitungsverzeichnis nach Artikel 30 DS-GVO mit Löschkonzept nach Art. 17 Abs. 1 DS-GVO \(LfDI Baden-Württemberg\)](#)

[Muster für ein Verzeichnis von Verarbeitungstätigkeiten \(Hessischer Beauftragter für Datenschutz und Informationsfreiheit\)](#)

**3. Verletzung des Schutzes personenbezogener Daten**

Bei einer Verletzung des Schutzes personenbezogener Daten (auch „Datenpanne“ genannt) besteht für den Verantwortlichen die Pflicht, die zuständige Aufsichtsbehörde sowie ggf. die betroffene(n) Person(en) über den Vorfall zu informieren. Das gilt nur dann nicht, sofern der Vorfall voraussichtlich nicht zu einem (hohen) Risiko für die Rechte und Freiheiten der betroffenen Person(en) führt. Ob ein Risiko oder gar ein hohes Risiko erforderlich ist, um entsprechende Pflichten des Verantwortlichen auszulösen, muss im Hinblick auf die Meldung gegenüber der Aufsichtsbehörde sowie die Benachrichtigung der betroffenen Person(en) unterschiedlich bewertet werden.

**Was ist eine Datenschutzverletzung?** Eine Verletzung des Schutzes personenbezogener Daten ist gem. Art. 4 Nr. 12 DS-GVO 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. Regelmäßig werden hierbei drei unterschiedliche Kategorien von Datenschutzverletzungen unterschieden:

- Die Verletzung der Vertraulichkeit, d. h. die unbefugte oder (un)beabsichtigte Preisgabe von oder Einsichtnahme in personenbezogene Daten

- die Verletzung der Integrität, d. h. die unbefugte oder (un)beabsichtigte Änderung personenbezogener Daten
- die Verletzung der Verfügbarkeit, d. h. der unbefugte oder (un)beabsichtigte Verlust des Zugangs zu personenbezogenen Daten oder die (un)beabsichtigte oder unrechtmäßige Vernichtung personenbezogener Daten

### **Beispiele für Datenschutzverletzungen:**

- Hackerangriff auf die IT-Systeme und Abzug von Daten
- versehentlicher elektronischer Versand einer unverschlüsselten Liste mit Daten an einen unrechtmäßigen Empfänger
- versehentlicher postalischer Versand von Dokumenten an den falschen Adressaten
- fehlerhafte Verteilung von Zugriffsberechtigungen auf Laufwerke
- Verwendung von geschäftlichen Daten für private Zwecke
- Verlust oder Diebstahl des Laptops oder eines anderen Datenträgers, wenn die Daten darauf nicht oder nicht ausreichend verschlüsselt sind
- Verlust oder Diebstahl einer Videokamera und des Aufzeichnungsmaterials
- Veröffentlichungen von Daten im Internet aufgrund eines technischen Fehlers

**Meldepflicht gegenüber der Datenschutzaufsichtsbehörde:** Eine Datenschutzverletzung muss der Aufsichtsbehörde innerhalb von 72 Stunden gemeldet werden, es sei denn, dass die Datenschutzverletzung „voraussichtlich nicht zu einem Risiko für die betroffene Person“ führt. Ein „einfaches Risiko“ reicht – es muss keine schwerwiegende Beeinträchtigung drohen. Bei den meisten Fällen wird nicht auszuschließen sein, dass irgendein denkbares Risiko besteht, sodass nahezu immer eine Meldung an die Aufsichtsbehörde erfolgen muss.

Die Meldung an die Aufsichtsbehörde muss enthalten:

- eine Beschreibung des konkreten Vorfalls (Art der Datenpanne)
- die Kategorien von betroffenen Personen (beispielsweise Adressdaten, E-Mail-Adressen, Bankverbindung, Geburtstag, Steuermerkmale, Bonitätsdaten)
- die Anzahl der Betroffenen
- die Anzahl der Datensätze
- die Einschätzung der wahrscheinlichen Folgen für die betroffenen Personen
- Ergriffene oder vorgeschlagene Maßnahmen zur Behebung oder Abmilderung der Verletzung (Ursachenbeseitigung und Schadensbegrenzung), beispielsweise die Information von irrtümlichen Empfängern unter Aufforderung zur Datenlöschung

- der Name und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Information

**Berechnung der Meldefrist:** Die in Art. 33 DS-GVO geregelte Meldefrist (72 Stunden) beginnt nicht schon bei einem bloßen Verdacht einer Datenschutzverletzung. Sie muss aber auch nicht mit Sicherheit festgestellt worden sein. Vielmehr müssen dem Verantwortlichen tatsächliche Anhaltspunkte bekannt werden, die eine hohe Wahrscheinlichkeit einer Datenschutzverletzung indizieren. Hierbei gilt es insbesondere zu beachten, dass etwaige innerbetriebliche Beschwerden nicht berücksichtigt werden. Maßgeblich wird darauf abgestellt, wann die tatsächliche Möglichkeit zu einer Meldung bestand. Ist es dem Verantwortlichen nicht möglich, vor Ablauf der Meldefrist sämtliche Informationen bereitzustellen, so sieht die DS-GVO eine schrittweise Meldung vor. Der zuständigen Aufsichtsbehörde sollten daher jedenfalls diejenigen Informationen zur Verfügung gestellt werden, die dem Verantwortlichen zum jeweiligen Zeitpunkt bekannt sind.

Wichtig hierbei ist insbesondere, dass die aufgeführte Frist auch dann (weiter) läuft, sofern eine Datenschutzverletzung z. B. erst an einem Freitagabend bekannt wird. Wochenend- oder Feiertage verlängern die in der DS-GVO vorgesehenen Fristen nicht. Soweit die 72 Stunden überschritten werden, muss die Verzögerung im Rahmen des Meldeschreibens begründet werden.

**Benachrichtigungspflicht der betroffenen Personen:** Bedeutet die Datenschutzverletzung voraussichtlich ein „hohes Risiko“ für die persönlichen Rechte und Freiheiten der von der Datenschutzverletzung betroffenen Personen, müssen auch die Betroffenen unverzüglich von der Datenschutzverletzung benachrichtigt werden. Während eine Meldung gegenüber der Aufsichtsbehörde der Regelfall sein wird, bedarf es neu der Pflicht zur Benachrichtigung der Betroffenen einer intensiveren Prüfung.

**Beispiel:** Ein Unternehmen versendet einen Auszug der Personalakte eines Beschäftigten (mit Informationen zu Krankmeldungen und Gehaltsdaten) versehentlich an die gesamte Belegschaft. Da der Vorfall voraussichtlich ein hohes Risiko für die betroffene Person zur Folge hat, muss die Aufsichtsbehörde eingeschaltet und die betroffene Person benachrichtigt werden. Die Pflichtinformationen an eine entsprechende Benachrichtigung werden in Art. 34 Abs. 2 DS-GVO festgehalten.

**Ausnahmen von der Benachrichtigungspflicht:** Unter bestimmten Voraussetzungen ist die Benachrichtigung der betroffenen Person – trotz eines hohen Risikos für deren persönliche Rechte und Freiheiten – entbehrlich. Gemäß Art. 34 Abs. 3 DS-GVO ist das in den folgenden Konstellationen der Fall:

- Der Verantwortliche hat technische und organisatorische Vorkehrungen getroffen, die einen Drittzugriff ausschließen (z. B. durch Verschlüsselung).
- Der Verantwortliche hat durch nachträgliche Maßnahmen dafür gesorgt, dass das hohe Risiko für die betroffene Person nicht mehr besteht.
- Eine Benachrichtigung ist bei unverhältnismäßigem Aufwand entbehrlich. In einem solchen Fall kann der Verantwortliche eine öffentliche Bekanntmachung machen oder ähnlich wirksame Maßnahmen treffen.

Ob eine der vorbezeichneten Konstellationen im Einzelfall ausnahmsweise vorliegt, sollte stets in enger Abstimmung mit dem Datenschutzbeauftragten entschieden werden.

**Dokumentationspflichten?** Unabhängig von einer Meldepflicht an die Aufsichtsbehörde besteht für Datenschutzverletzungen eine Dokumentationspflicht nach Art. 33 Abs. 5 DS-GVO. Die jeweiligen Dokumentationen sollten jedenfalls für einen Zeitraum von 3 Jahren aufbewahrt werden.

**Weiterführende Informationen:**

Formular und Eingabemaske zur Meldung von Verletzungen des Schutzes personenbezogener Daten in Hessen (mit weitergehenden Mustern und Links)

Flyer zur Verletzung des Schutzes personenbezogener Daten (LDA Bayern)

Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten (EDSA)

#### 4. Datenschutz-Folgenabschätzung

Für bestimmte Datenverarbeitungsvorgänge muss eine sog. Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO durchgeführt werden. Das ist immer dann der Fall, sofern aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen anzunehmen ist. Die Prüfung gliedert sich hierbei in zwei Schritte:

- Klärung der Frage, ob eine Datenverarbeitung ein hohes Risiko zur Folge haben kann (sog. Schwellwertanalyse)
- Ggf. Durchführen einer Datenschutz-Folgenabschätzung

**Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung:** Eine Datenschutz-Folgenabschätzung ist immer dann durchzuführen, wenn eine bestimmte Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt. In Art. 35 Abs. 3 DS-GVO werden hierzu einige exemplarische Fälle benannt:

- 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
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

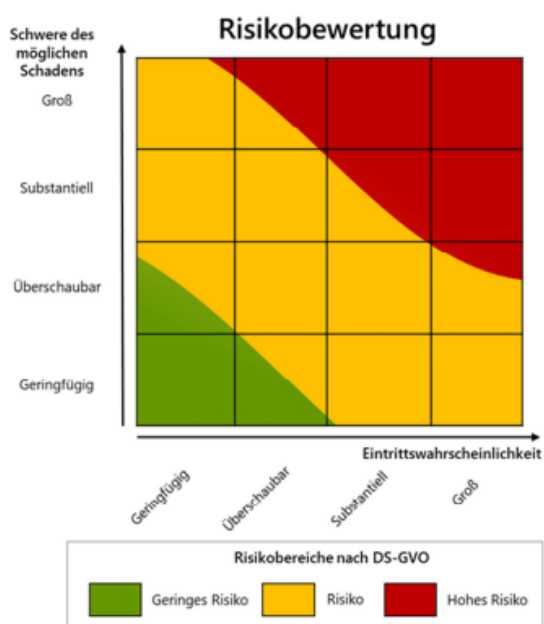
Daneben veröffentlichen die Datenschutzaufsichtsbehörden gemäß Art. 35 Abs. 4 DS-GVO eine sog. „Muss-Liste“, in welcher konkrete Datenverarbeitungsvorgänge benannt sind, bei denen zwingend eine Datenschutz-Folgenabschätzung durchzuführen ist. Ein Beispiel ist der Einsatz künstlicher Intelligenz, soweit hierbei die Interaktion mit natürlichen Personen gesteuert wird (z. B. KI-gestützte Chatbots).

**Systematik einer Datenschutz-Folgenabschätzung:** Eine Datenschutz-Folgenabschätzung muss gemäß Art. 35 Abs. 7 DS-GVO die folgenden Mindestinhalte aufweisen:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- 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

**Die Risikobewertung:** Unter einem Risiko versteht man „das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann“. Gemäß Erwägungsgrund 75 der DS-GVO sind hierbei psychische, materielle und immaterielle Schäden denkbar.

Ein Risiko bemisst sich immer aus einer Korrelation zwischen der Schwere eines (denkbaren) Schadens und dessen Eintrittswahrscheinlichkeit. Zur Bewertung der bestehenden Risiken sollten sich Unternehmen an der eigens hierfür geschaffenen Matrix der Datenschutzkonferenz (DSK) in Kurzpapier Nr. 18 orientieren.<sup>1</sup>



<sup>1</sup> Abrufbar unter: [https://www.datenschutzkonferenz-online.de/media/kp/dsk\\_kpnr\\_18.pdf](https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf)

Bei der Durchführung der Datenschutz-Folgenabschätzung ist stets der Rat des Datenschutzbeauftragten einzuholen.

#### **Weiterführende Informationen:**

[Kurzpapier Nr. 5 \(DSK\) – Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO](#)

[Themenseite zur DS-FA mit weitergehenden Mustern und Links \(LDA Bayern\)](#)

[Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO \(LfDI Baden-Württemberg\)](#)

## **5. Der Datenschutzbeauftragte**

Da der Datenschutzbeauftragte in vielen Unternehmen eine wichtige Rolle einnimmt, sollen die relevantesten Punkte hierzu bereits an dieser Stelle behandelt werden. Die Anforderungen an die Benennung eines Datenschutzbeauftragten sind in den Art. 37 bis 39 der DS-GVO sowie in § 38 BDSG festgelegt.

**Pflicht zur Benennung eines Datenschutzbeauftragten:** Ein Datenschutzbeauftragter ist erforderlich, wenn mindestens 20 Personen im Betrieb ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Automatisierte Verarbeitung umfasst beispielsweise die Nutzung digitaler Kundendateien oder die Verwendung von Kundendaten auf Tablets oder Smartphones. Als „ständig befasst“ gelten Mitarbeiter, deren Hauptaufgabe die Datenverarbeitung ist, wie in der Lohnbuchhaltung oder Personalabteilung. Mitarbeiter, die Daten nur zur Ausübung ihrer gewöhnlichen Tätigkeit benötigen, fallen nicht unter diese Regelung.

Für mehrere Standorte eines Unternehmens kann ein einziger Datenschutzbeauftragter bestellt werden, solange er seine Aufgaben weiterhin angemessen erfüllen kann.

**Anforderungen an den Datenschutzbeauftragten:** Ein Datenschutzbeauftragter kann entweder ein interner Mitarbeiter des Unternehmens oder ein externer Dienstleister sein. Unabhängig davon, ob es sich um einen internen oder externen Datenschutzbeauftragten handelt, müssen folgende Anforderungen erfüllt sein:

- Fachliche Qualifikationen im Bereich Datenschutz (Kenntnisse im Datenschutzrecht und IT-Fachwissen)
- Keine Interessenkonflikte bei der Aufgabenwahrnehmung (Interessenkonflikte bestehen z. B. für Mitglieder der Geschäftsführung oder Leiter der IT- oder Personalabteilung, da diese Personen für die Datenverarbeitung mitverantwortlich sind und sich selbst kontrollieren müssten)

**Stellung des Datenschutzbeauftragten:** Der Datenschutzbeauftragte muss bei der Erfüllung seiner Aufgaben unabhängig sein und direkt an die Geschäftsführung berichten. Er muss frühzeitig in alle datenschutzrechtlichen Themen eingebunden werden. Ein interner Datenschutzbeauftragter darf wegen seiner Aufgaben weder abberufen noch benachteiligt werden. Ihm müssen die notwendige Zeit und Unterstützung (z. B. Fortbildungen und Ausstattung) zur Ver-

fügung gestellt werden. Zudem genießt ein interner Datenschutzbeauftragter besonderen Kündigungsschutz: Das Arbeitsverhältnis darf während seiner Tätigkeit als DSB und für ein Jahr danach nicht gekündigt werden, außer aus wichtigem Grund.

**Aufgaben des Datenschutzbeauftragten:** Ein Datenschutzbeauftragter hat insbesondere folgende Aufgaben:

- Unterrichtung und Beratung der Geschäftsführung und der Mitarbeiter in Datenschutzfragen
- Überwachung der Einhaltung der Datenschutzvorschriften
- Sensibilisierung und Schulung der Mitarbeiter
- Beratung und Überwachung der Durchführung von Datenschutz-Folgenabschätzungen
- Zusammenarbeit mit der Datenschutzaufsichtsbehörde
- Ansprechpartner für externe und interne Betroffene bei Fragen zur Verarbeitung ihrer personenbezogenen Daten

Der Datenschutzbeauftragte ist jedoch nur für die ordnungsgemäße Erfüllung seiner eigenen gesetzlichen Aufgaben verantwortlich. Weitergehende Pflichten oder Haftungen bestehen nicht, insbesondere nicht für die Einhaltung der datenschutzrechtlichen Vorschriften im Unternehmen. Die Geschäftsführung bleibt trotz Benennung eines Datenschutzbeauftragten für das rechtmäßige Handeln des Unternehmens in Datenschutzangelegenheiten verantwortlich. Der Datenschutzbeauftragte hat lediglich die Pflicht zur ordnungsgemäßen Beratung.

**Formelle Anforderungen:** Es gibt keine gesetzlich vorgeschriebene Form oder Dauer für die Bestellung eines Datenschutzbeauftragten. Aus Nachweisgründen sollte die Bestellung jedoch schriftlich erfolgen. Nach der Bestellung müssen folgende Informationspflichten beachtet werden:

- Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten (z. B. E-Mail-Adresse, Durchwahlnummer) auf der Webseite des Betriebs
- Meldung der Kontaktdaten des Datenschutzbeauftragten an die zuständige Landesdatenschutzbehörde. Es ist lediglich erforderlich, die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen, nicht zwingend seinen Namen

**Weiterführende Informationen:**

[Kurzpapier Nr. 12 \(DSK\) – Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern](#)

[Formular zur Meldung eines Datenschutzbeauftragten in Hessen](#)

[Handreichung zum behördlichen und betrieblichen Datenschutzbeauftragten \(Hessischer Beauftragter für Datenschutz und Informationsfreiheit\)](#)

## 6. Drittlandtransfer

In gewissen Fällen kann es vorkommen, dass personenbezogene Daten nicht ausschließlich innerhalb der EU verarbeitet werden. So werden Daten entweder in das außereuropäische Ausland übermittelt bzw. dort gespeichert oder es wird ein entsprechender Zugriff auf Daten ermöglicht (etwa im Falle eines Fernzugriffs). Ein Drittlandtransfer spielt sowohl bei der Einbindung von Dienstleistern als auch bei der Mitwirkung konzernverbundener Unternehmen eine Rolle.

Die DS-GVO sieht für solche Datenübermittlungen besondere Regelungen in den Art. 44 ff. DS-GVO vor. Bei jedem Drittlandtransfer hat daher eine zweistufige Prüfung zu erfolgen:

- Prüfung und Umsetzung der allgemeinen datenschutzrechtlichen Pflichten
- Prüfung und Umsetzung der besonderen Anforderungen der Art. 44 ff. DS-GVO

**Anforderungen an einen Drittlandtransfer:** Jeder Drittlandtransfer, also jede Verlagerung personenbezogener Daten außerhalb der EU, muss den Anforderungen der Art. 44 ff. DS-GVO entsprechen. Die zweite Stufe der Prüfung meint hierbei nichts anderes, als dass ein eigenständiger Erlaubnistatbestand für die Verlagerung der Datenverarbeitung in ein Drittland aufgefunden werden muss. Grundsätzlich bestehen die folgenden Instrumente, auf deren Basis ein entsprechender Drittlandtransfer möglich ist:

- Es existiert ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 Abs. 3 DS-GVO
- Es werden geeignete Garantien i. S. d. Art. 46 Abs. 2 DS-GVO ergriffen (z. B. Standardvertragsklauseln oder Binding Corporate Rules)
- Es existiert eine Ausnahme für bestimmte Fälle gemäß Art. 49 Abs. 1 DS-GVO (z. B. die betroffene Person hat in den Drittlandtransfer eingewilligt)

**Was ist ein Angemessenheitsbeschluss?** Ein Angemessenheitsbeschluss ist die Aussage der Europäischen Kommission, dass in einem Drittland ein angemessenes Datenschutzniveau existiert. Das bedeutet im Ergebnis, dass grundsätzlich keine weiteren Prüfschritte nach den Art. 44 ff. DS-GVO durchgeführt werden müssen. Die Datenverarbeitung wird so behandelt, als würde sie in der EU stattfinden.

Derzeit existieren Angemessenheitsbeschlüsse für folgende Drittländer:

- Andorra
- Argentinien
- Kanada
- Färöer-Inseln
- Guernsey
- Israel
- Isle of Man
- Japan
- Jersey
- Neuseeland
- Republik Korea (Südkorea)

- Schweiz
- Uruguay
- Vereinigtes Königreich (UK)
- Vereinigte Staaten von Amerika (USA)

**Wichtig:** In Ausnahmefällen (so z. B. für **Datenübermittlungen in die USA**) müssen sich Datenimporteure (also Datenempfänger in einem Drittland) dem jeweiligen Angemessenheitsbeschluss ausdrücklich unterwerfen, damit der Drittlandtransfer ohne weitere Prüfschritte durchgeführt werden kann. Ein Angemessenheitsbeschluss gilt daher nicht immer voraussetzungslos in dem gesamten Drittland, sondern muss ggf. branchen- oder unternehmensbezogen geprüft werden.

Die aktuellen Zertifizierungen unter dem EU-US Data Privacy Agreement können auf einer hierfür eingerichteten Webseite<sup>2</sup> eingesehen werden. Hierbei ist jedoch wichtig, dass sich die jeweilige Zertifizierung **nur auf den Datenimporteur selbst** bezieht. Werden z. B. weitere Unterauftragsverarbeiter eingesetzt, muss für jedes weitere Unterauftragsverarbeitungsverhältnis geprüft werden, ob die Anforderungen der Art. 44 ff. DS-GVO eingehalten werden (können)!

**Praxishinweis:**

Gerade in Bezug auf Datenübermittlungen in die USA ändert sich die Rechtslage in mehr oder weniger regelmäßigen Abständen. Die beiden Vorgänger des derzeit (noch) gültigen Angemessenheitsbeschlusses wurden bereits infolge von Urteilen des EuGH aufgehoben. Dreh- und Angelpunkt ist hierbei immer wieder die Frage, ob Geheimdienstaktivitäten in den USA sowie fehlende Rechtsschutzmöglichkeiten für betroffene Personen einem angemessenen Datenschutzniveau im Wege stehen. Auch der aktuelle Angemessenheitsbeschluss steht erneut in der Kritik, sodass mit einem weiteren Verfahren vor dem EuGH zu rechnen ist!

Man kann sich also merken, dass gerade Datenübermittlungen in die USA in regelmäßigen Abständen auf den Prüfstand gestellt werden sollten. Häufig wird die Empfehlung ausgesprochen, auch unabhängig vom Vorliegen des Angemessenheitsbeschlusses, Standardvertragsklauseln mit dem Datenempfänger zu vereinbaren, um vor einer (erneuten) Anpassung der Rechtslage gewappnet zu sein. Viele der namhaften US-Anbieter sehen eine entsprechende Vorgehensweise ohnehin vor, um die jeweiligen Datenübermittlungen auch künftig abzusichern.

**Geeignete Garantien für einen Drittlandtransfer:** In Art. 46 Abs. 2 DS-GVO finden sich weitere Instrumente, auf deren Basis ein Drittlandtransfer durchgeführt werden kann. Am praxisrelevantesten sind die sog. Standardvertragsklauseln. Hierbei handelt es sich um die vertragliche Zusicherung des Datenimporteurs in einem Drittland, dass er vertragliche, technische und organisatorische Maßnahmen ergreift, um ein dem europäischen Niveau vergleichbares Datenschutzniveau sicherzustellen.

Bei der Vereinbarung von Standardvertragsklauseln ist stets darauf zu achten, dass die aktuell gültigen Formulare der Europäischen Kommission verwendet werden und die jeweiligen Muster – abseits von vorgesehenen Anpassungen – nicht abgeändert werden. Ebenfalls ist zu beachten, dass die bloße Vereinbarung von Standardvertragsklauseln nicht ausreicht, um einen Drittlandtransfer nach den Vorgaben der DS-GVO zu legitimieren. Es ist stets ein sog. Transfer Impact Assessment (TIA) durchzuführen, mit welchem die aus dem Drittlandtransfer

<sup>2</sup> Abrufbar unter: <https://www.dataprivacyframework.gov/s/participant-search>

resultierenden Risiken zu prüfen sind. Der Europäische Datenschutzausschuss (EDSA) hat Empfehlungen zur Vorgehensweise bei einem TIA veröffentlicht, an denen sich Unternehmen streng orientieren sollten. (Nur) Sofern diese Anforderungen entsprechend umgesetzt werden, können die Daten auch ohne Vorliegen eines Angemessenheitsbeschlusses in ein Drittland übermittelt werden.

#### **Weiterführende Informationen:**

[Kurzpapier Nr. 4 \(DSK\) – Datenübermittlung in Drittländer](#)

[Handreichung zu Drittlandtransfers unter der DS-GVO \(LfDI Baden-Württemberg\)](#)

## **Technische und organisatorische Maßnahmen**

### **1. Allgemeine Anforderungen**

Gemäß den Art. 24, 25 und 32 DS-GVO sind Unternehmen dazu verpflichtet, technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit zu ergreifen. Die hierbei verfolgten Schutzziele können u. a. durch die nachfolgenden Maßnahmen umgesetzt werden:

- **Maßnahmen zur Vertraulichkeit der Datenverarbeitung** (z. B. Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle): Maßnahmen, die sicherstellen, dass Unbefugte keinen Zugang zu Datenverarbeitungsanlagen erhalten, in denen personenbezogene Daten verarbeitet werden. Ein Beispiel hierfür wäre das Abschließen des Serverraums, um den Zugang zu den Servern zu kontrollieren. Ein weiteres Beispiel ist die Implementierung eines strikten Rechte- und Rollenkonzepts, um zu gewährleisten, dass nur befugte Personen Zugriff auf die jeweiligen Daten erhalten.
- **Maßnahmen zur Gewährleistung der Integrität der Datenverarbeitung** (z. B. Eingabekontrolle, Verarbeitungskontrolle): Maßnahmen, die sicherstellen, dass nachträglich überprüft werden kann, wer personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt hat. Dies kann durch die Verwendung individueller Benutzernamen ermöglicht werden, um die Aktivitäten der Nutzer nachvollziehbar zu machen.
- **Maßnahmen zur Verfügbarkeitskontrolle**: Maßnahmen, die gewährleisten, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind und dass diese Daten im Störfall wiederhergestellt werden können. Ein Beispiel hierfür ist die Installation von Geräten zur Überwachung der Temperatur und Feuchtigkeit in Serverräumen, um die physische Sicherheit der Daten zu gewährleisten.

Die vorstehende Liste ist natürlich nicht abschließend, sondern soll lediglich einen ersten Eindruck zu Art und Umfang der jeweiligen Maßnahmen ermöglichen. Die konkret zu ergreifenden Maßnahmen müssen stets am jeweiligen Verarbeitungskontext und den daraus resultierenden Risiken bewertet werden. Zudem müssen alle ergriffenen Maßnahmen dem Stand der Technik entsprechen.

## Weiterführende Informationen:

[Hinweise zum sicheren Umgang mit Passwörtern \(LfDI Baden-Württemberg\)](#)

[Good Practice bei technischen und organisatorischen Maßnahmen \(LDA Bayern\)](#)

## 2. Sonderfall: Vorhalten eines Löschkonzepts

Die DS-GVO legt als besondere Voraussetzung fest, dass personenbezogene Daten gelöscht werden müssen, sobald sie nicht mehr für den Zweck benötigt werden, zu dem sie ursprünglich erhoben wurden. Die Pflicht hierzu kann unmittelbar dem den betroffenen Personen zustehenden Anspruch auf Löschung aus Art. 17 DS-GVO entnommen werden und wird gleichzeitig durch den Grundsatz der Speicherbegrenzung in Art. 5 Abs. 1 lit. e) DS-GVO festgehalten. Da das Vorhalten eines Löschkonzepts als besonders praxisrelevant anzusehen ist, sollen die Kernelemente nachstehend überblicksartig dargestellt werden.

**Beispiel:** Ein Kunde bittet um einen Kostenvoranschlag für eine bestimmte Leistung oder ein bestimmtes Produkt. Das Unternehmen muss hierzu den Namen, die Anschrift und gegebenenfalls weitere Kontaktdaten des Kunden erfassen. Wenn nach dem Kostenvoranschlag jedoch kein Vertrag zustande kommt, werden die Daten nicht mehr benötigt und müssen grundsätzlich gelöscht werden.

**Einzelfallbetrachtung:** Im Allgemeinen liegt es im Ermessen des Verantwortlichen zu entscheiden, wann die Aufbewahrung von personenbezogenen Daten nicht mehr erforderlich ist. In der Praxis haben sich jedoch bestimmte Fristen etabliert, die sich häufig aus Verjährungsfristen ergeben und nach deren Ablauf die Daten in der Regel nicht mehr benötigt werden. Daneben gibt es gesetzliche Regelungen, die vorschreiben, dass bestimmte Daten für einen festgelegten Zeitraum aufbewahrt oder zu einem bestimmten Zeitpunkt gelöscht werden müssen. Hierzu gehören beispielsweise steuerrelevante Daten wie Rechnungen, die jedenfalls für zehn Jahre aufzubewahren sind.

Während des gesetzlich vorgeschriebenen Aufbewahrungszeitraums dürfen personenbezogene Daten nicht gelöscht werden. Nach Ablauf der gesetzlichen Frist dürfen die jeweiligen Daten gelöscht werden, müssen jedoch nicht zwingend gelöscht werden. Die Pflicht zur Löschung ergibt sich aus dem allgemeinen Grundsatz der DS-GVO, wonach Daten nach Ablauf der Aufbewahrungsfrist gelöscht werden müssen, sofern sie nicht mehr für den ursprünglichen Zweck erforderlich sind.

**Beispiel:** Kundendaten werden nach Ablauf der Gewährleistungsfristen und der steuerrechtlichen Aufbewahrungspflichten – also nach zehn Jahren – nicht mehr zur Vertragsabwicklung benötigt. Die Daten könnten jedoch für die weitere Geschäftsbeziehung und Kundenbindung erforderlich sein und dürfen für diese Zwecke weiterhin aufbewahrt werden.

**Vorhalten eines Löschkonzepts:** Um den vorgenannten Anforderungen entsprechen zu können, muss im Unternehmen ein Löschkonzept erarbeitet werden. Ein Löschkonzept bedeutet, dass jedes Unternehmen eine Dokumentation darüber verfügen muss, welche Daten auf welchen Systemen gespeichert sind und wann die Daten unter Berücksichtigung der jeweils einschlägigen Regelungen gelöscht werden müssen.

Löschung bedeutet nichts anderes als die tatsächliche Vernichtung der Daten. Papierdokumente sollten geshreddert oder anderweitig vernichtet werden. Bei digitaler Speicherung müssen Daten unwiderruflich vom Datenträger gelöscht werden (z. B. Festplatte, USB-Stick). Datenträger, die keine digitale Löschung ermöglichen (z. B. CDs), müssen physisch zerstört werden.

Für die ordnungsgemäße Löschung und Entsorgung werden häufig Dienstleister beauftragt. Die Löschung durch Dienstleister stellt eine Auftragsverarbeitung dar und erfordert den Abschluss eines Vertrags zur Auftragsverarbeitung gemäß Art. 28 DS-GVO.

**Löschprotokoll:** Wie bei allen Pflichten der DS-GVO muss auch bei der Datenlöschung nachgewiesen werden, dass die Pflicht ordnungsgemäß erfüllt wurde (Art. 5 Abs. 2 DS-GVO). Es ist daher zu empfehlen, ein Löschprotokoll anzufertigen. Das Protokoll muss keine besondere Form aufweisen, sollte jedoch keine personenbezogenen Daten enthalten, sondern lediglich dokumentieren, dass eine Löschung vorgenommen wurde.

## Relevante Sonderkonstellationen

Einige Konstellationen spielen in der betrieblichen Praxis eine besondere Rolle, können jedoch keiner der vorherigen Pflichtenkategorien zugeordnet werden. Im vorliegenden Leitfaden sollen daher die folgenden Konstellationen näher in den Blick genommen werden:

- Videoüberwachung auf dem Betriebsgelände
- Betrieb einer Webseite und Social-Media-Kanäle
- E-Mail und Internetnutzung im Unternehmen

### 1. Videoüberwachung auf dem Betriebsgelände

Der Einsatz von Videokameras auf Betriebsgeländen und in Betriebsräumen ist weit verbreitet. Die Zulässigkeit einer solchen Videoüberwachung hängt davon ab, ob der überwachte Bereich öffentlich zugänglich ist, zu welchen Zwecken die Videoüberwachung erfolgt und welche Personen aufgenommen werden. Je nachdem, ob Kunden, unbeteiligte Dritte oder Beschäftigte des Unternehmens überwacht werden, ergeben sich unterschiedliche rechtliche Anforderungen.

**Öffentlich zugängliche Räume:** In öffentlich zugänglichen Bereichen, wie beispielsweise Parkplätzen, Geschäfts-, Empfangs- und Verkaufsräumen, können Videokameras im Regelfall ohne Einwilligung der überwachten Personen eingesetzt werden. Es ist lediglich darauf zu achten, dass tatsächlich ein berechtigtes Interesse des Unternehmens besteht und dokumentiert wird (Art. 6 Abs. 1 lit. f) DS-GVO). Ein solches Interesse kann z. B. die Aufklärung von Diebstählen oder Sachbeschädigungen sein.

Das berechtigte Interesse eines Unternehmens an der Videoüberwachung muss stets gegen das Schutzinteresse der gefilmten Personen abgewogen werden. Dabei ist zu unterscheiden, wer gefilmt wird:

- Kunden: Kunden haben in der Regel kein höheres Schutzinteresse, da sie das Betriebsgelände freiwillig und in Kenntnis der Videoüberwachung betreten. Dies gilt jedenfalls dann, sofern eine ordnungsgemäße Beschilderung angebracht wird (hierzu sogleich).

- **Passanten:** Passanten, die nicht das Betriebsgelände betreten, sondern auf öffentlichen Wegen daran vorbeigehen oder sich dort aufhalten, haben ein höheres Schutzinteresse. Zudem besteht in diesen Fällen kein berechtigtes Interesse am Betrieb einer Videoüberwachung. Kameras dürfen nur das Betriebsgelände erfassen und nicht darüber hinaus auf öffentliche Straßen, Wege und Plätze gerichtet sein. Sie sollten also so ausgerichtet werden, dass sie ausschließlich das Betriebsgelände filmen.
- **Beschäftigte:** Beschäftigte haben ein höheres Schutzinteresse, wenn sie dauerhaft gefilmt werden, da eine solche Vorgehensweise einer unzulässigen Dauerüberwachung gleichkommt. Die Kameras sollten daher so ausgerichtet sein, dass Beschäftigte entweder gar nicht oder nur gelegentlich erfasst werden.

**Nicht öffentlich zugängliche Räume:** In Betriebsräumen, die ausschließlich für Beschäftigte zugänglich sind, wie Materiallager, Büros oder Werkstätten, ist der Einsatz von Kameras grundsätzlich nicht erlaubt, wenn Beschäftigte gefilmt werden. Das gilt auch dann, wenn die Beschäftigten nur gelegentlich und nicht dauerhaft aufgenommen werden. Das Filmen von Beschäftigten in nicht öffentlich zugänglichen Räumen ist im Regelfall nur dann zulässig, wenn ein berechtigter Zweck (z. B. Aufklärung von Diebstählen oder Sachbeschädigungen) verfolgt wird und die Beschäftigten in die Videoüberwachung eingewilligt haben. Eine Einwilligung ist jedoch nur für eine gelegentliche Überwachung möglich, eine dauerhafte Videoüberwachung ist stets unzulässig.

**Hinweis zur Videoüberwachung:** Personen, die von einer Kamera aufgenommen werden, müssen spätestens zum Zeitpunkt der Videoüberwachung darüber informiert werden. Die Pflicht hierzu ergibt sich aus den Informationspflichten der DS-GVO (Art. 13 DS-GVO) und ermöglicht den betroffenen Personen zu entscheiden, ob sie sich im überwachten Bereich aufhalten möchten oder nicht.

Die Datenschutzaufsichtsbehörden der Bundesländer empfehlen einen Aushang mit Piktogramm und weitergehenden Informationen. Dieser oder ein vergleichbarer Aushang sollte am Ort der Videoüberwachung an einer gut sichtbaren Stelle platziert werden.

**Löschfristen:** Videoaufnahmen müssen gelöscht werden, wenn sie zur Erreichung des ursprünglichen Zwecks, meist die Aufklärung von Straftaten, nicht mehr notwendig sind.

Die Datenschutzaufsichtsbehörden halten eine Speicherdauer von 72 Stunden grundsätzlich für ausreichend, um die Verfolgung von Straftaten zu ermöglichen.

**Weiterführende Informationen:**

[Orientierungshilfe Videoüberwachung \(DSK\) mit Mustern für Datenschutzhinweise](#)

[Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte \(EDSA\)](#)

**2. Webseite und Social-Media**

Weitere datenschutzrechtliche Fragen stellen sich regelmäßig auch beim Betrieb einer Unternehmens-Webseite sowie beim Einsatz von Social-Media-Kanälen.

**Cookies und Analyse-Tools:** Eines der relevantesten Themenfelder im Online-Bereich ist das Setzen von Cookies und Analyse-Tools. Bei Cookies handelt es sich um Textdateien, die vorübergehend im Browser des Nutzers deponiert werden und Informationen über diesen erheben. Häufig werden Cookies eingesetzt, um den Nutzern mehr Komfort beim Surfen zu bieten (z. B. Warenkorbfunktion oder Speicherung der Sprachauswahl). Dabei handelt es sich um sogenannte technisch notwendige Cookies, die die fehlerfreie Funktion einer Webseite erst ermöglichen. Die dazugehörigen Vorschriften sind in § 25 Telekommunikation- Digitale-Dienste-Datenschutz-Gesetz (TDDDG) abgebildet und gelten unabhängig davon, ob tatsächlich personenbezogene Daten verarbeitet werden oder nicht. Das bloße Setzen eines Cookies oder Analyse-Tools muss somit den Anforderungen des TDDDG entsprechen.

Das Vorhalten technisch notwendiger Cookies bedarf keiner datenschutzrechtlichen Einwilligung, da die Bereitstellung der Webseite und/oder einzelner Funktionen ohne diese nicht möglich ist. Die im Regelfall hiermit einhergehende Verarbeitung personenbezogener Daten (z. B. die IP-Adresse) kann sodann auf Art. 6 Abs. 1 lit. f) DS-GVO gestützt werden.

Darüber hinaus können jedoch auch Cookies/Tools verwendet werden, um geräteübergreifende Nutzerprofile oder sonstige Analysen über das Nutzerverhalten zu erstellen. Dabei können die Cookies unterschiedliche Arten von Daten enthalten – neben statistischen auch personenbezogene Nutzerdaten etwa in Form der vollständigen IP-Adresse. Diese Tools bedürfen – entgegen der weit verbreiteten Meinung – im Regelfall der vorherigen Einwilligung des Nutzers und können nicht auf Basis einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f) DS-GVO eingesetzt werden.

**Anforderungen an Datenschutzhinweise:** Auf der Webseite müssen zunächst sämtliche auf der Webseite genutzten Cookies aufgeführt werden, welche als technisch notwendig anzusehen sind. Hierbei sollte zumindest aufgezeigt werden, zu welchen Zwecken der Cookie genutzt wird, um welchen Cookie-„Typ“ es sich handelt (z. B. HTTP, HTML, etc.) und wie lange die jeweiligen Daten gespeichert werden (z. B. reine Session-Cookies oder längere Aufbewahrung?). Wie bereits aufgezeigt, bedarf es für den Einsatz dieser Cookies keiner Einwilligungserklärung der Nutzer.

Einwilligungsbedürftige Cookies/Tools sind sodann ebenfalls in den Datenschutzhinweisen abzubilden. Hier ist genau darzustellen, zu welchen Zwecken die jeweiligen Tools eingesetzt werden, welche Daten hierbei verarbeitet werden und wer der Anbieter des jeweiligen Tools ist. Ebenfalls ist darauf hinzuweisen, ob beim Einsatz des Tools ein Drittlandtransfer i. S. d. Art. 44 ff. DS-GVO stattfindet.

**Cookie-Banner:** Schlussendlich ist ein Cookie-Banner vorzuhalten, welcher – je nach eingesetztem Cookie – die Abgabe einer Einwilligung oder eine Ablehnung der Nutzung von optionalen Cookies ermöglicht. Die Einwilligung des Nutzers muss eingeholt werden, **bevor** das Cookie aktiviert und die jeweiligen Daten verarbeitet werden. Der Cookie-Banner sollte aus diesem Grund unmittelbar bei Aufruf der Webseite erscheinen.

Wichtig bei der Ausgestaltung eines Cookie-Banners ist jedenfalls, dass der Nutzer der Webseite die freie Wahl zwischen einer Zustimmung, einer individuellen Anpassung und/oder einer Ablehnung von Cookies hat. Dies muss auch anhand der optischen Ausgestaltung des Cookie-Banners erkennbar sein. Sog. „Dark-Patterns“, welche eine Ablehnung der Nutzung von Cookies z. B. dunkel hinterlegen, sind rechtswidrig.

Ebenfalls ist es wichtig, dass nur technisch notwendige Cookies „vorangekreuzt“ sind. Jeder darüberhinausgehende Einsatz von Cookies muss auf der freiwilligen Entscheidung des Nutzers beruhen und darf nicht voreingestellt sein.

**Social-Media:** Von nahezu allen Unternehmen genutzt und dennoch gerne unterschätzt, wird auch das Themenfeld Social-Media. Sei es die Facebook-Fanpage oder der Instagram-Kanal – in allen Fällen tun sich datenschutzrechtliche Fragen auf, deren Handhabung Unternehmen vor einige praktische Schwierigkeiten stellen kann:

Der EuGH hat für den Einsatz einer Facebook-Fanpage per Urteil vom 5. Juni 2018 (Az. C-210/16) festgehalten, dass META (ehemals Facebook) und der jeweilige Fanpage-Betreiber als gemeinsame Verantwortliche i. S. d. Art. 26 DS-GVO anzusehen sind. Auch wenn bislang keine weiteren Urteile zu dieser Fragestellung existieren, vertreten die Datenschutzaufsichtsbehörden die Ansicht, dass diese Einschätzung auch auf andere Social-Media-Kanäle übertragbar ist.

Häufig ist Unternehmen nicht wirklich bekannt, welche (personenbezogenen) Daten vom jeweiligen Anbieter der Social-Media-Plattform verarbeitet werden. Zwar werden den Fanpage-Betreibern sog. „Insights“ zur Verfügung gestellt, die Unternehmen einen Einblick über das Nutzerverhalten auf ihrer Fanpage bieten. Woher diese Daten konkret kommen, wie sie erhoben und weiterverarbeitet wurden, ist jedoch nicht ohne Weiteres klar. Meta verarbeitet die Daten der Nutzenden jedenfalls nicht ausschließlich zum Zweck der Bereitstellung eines sozialen interaktiven Netzwerks, sondern auch zu Werbezwecken, die auf feingranularen Profilen der Nutzenden aufsetzen, um für sie „passgenaue“ Werbung im Auftrag von Unternehmen, Verbänden, Parteien etc. schalten zu können. Aufgrund der gemeinsamen Verantwortlichkeit sind Unternehmen aber auch für diese Datenverarbeitung (mit-)verantwortlich.

Aufgrund der vorgenannten Fragestellungen wurde bereits die ausdrückliche Aussage einiger Datenschutzaufsichtsbehörden getroffen, dass der datenschutzkonforme Einsatz einer Facebook-Fanpage nicht möglich sei. Letztlich stellt es eine Entscheidung der Geschäftsführung des Unternehmens dar, ob Social-Media-Kanäle trotz der bestehenden datenschutzrechtlichen Bedenken eingesetzt werden sollten oder nicht. Um Risiken so weit wie möglich zu minimieren, sollten jedenfalls die bereitgestellten Verträge mit den Anbietern der Social-Media-Plattformen abgeschlossen und möglichst transparente Informationen zu deren Nutzung auf der Webseite vorgesehen werden.

#### **Weiterführende Informationen:**

[FAQ zu Cookies und Tracking \(LfDI Baden-Württemberg\)](#)

[FAQ zu Facebook Fanpages \(DSK\)](#)

### **3. E-Mail und Internetnutzung im Unternehmen**

Spannend wird es schlussendlich auch bei der Frage, welche datenschutzrechtlichen Anforderungen zu beachten sind, soweit der Arbeitgeber seinen Beschäftigten die private Nutzung von Internet und E-Mail im Unternehmen gestattet. Dreh- und Angelpunkt der Frage ist immer, ob eine entsprechende Nutzung unter das Fernmeldegeheimnis in § 3 TDDDG fällt.

Bislang wurde der Arbeitgeber, sofern er die private Nutzung von Internet und E-Mail im Unternehmen erlaubt hat, nach dem wohl überwiegenden Meinungsbild der Datenschutzaufsichtsbehörden als Telekommunikationsanbieter eingestuft. Eine „Erlaubnis“ ist grundsätzlich

auch dann anzunehmen, sofern eine entsprechende Nutzung lediglich im Unternehmen geduldet und nicht ausdrücklich untersagt wird. Dies hatte zur Folge, dass für den Arbeitgeber die Regelungen aus dem TDDDG (vormals TKG) insbesondere das Fernmeldegeheimnis gelten. Insofern musste der Arbeitgeber stets eine Einwilligung der Betroffenen einholen, wenn er auf die Protokolldaten oder E-Mails der Beschäftigten zugreifen wollte.

Dieses Meinungsbild ist jedoch längst nicht mehr „in Stein gemeißelt“. Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) hat in ihrem letzten Tätigkeitsbereich z. B. ausdrücklich angeführt, dass die Bereitstellung von Internet und E-Mail im Unternehmen zu privaten Zwecken **nicht** dem Fernmeldegeheimnis unterliege. Nach Ansicht der LDI NRW fehle es dem Arbeitgeber insbesondere an dem erforderlichen Rechtsbindungswillen, gegenüber Beschäftigten Telekommunikationsdienste zu erbringen. Dies bedeutet jedoch nicht, dass jedwede Auswertung (z. B. von Protokolldaten oder E-Mails) nun ohne die Beachtung datenschutzrechtlicher Vorgaben zulässig ist. Die LDI NRW führt hierzu ausdrücklich aus:

*„Die DS-GVO sichert ein ähnlich hohes Schutzniveau für die personenbezogenen Daten der Beschäftigten. Auch nach der DS-GVO bedarf es einer Rechtsgrundlage für den Zugriff der Arbeitgeber\*innen auf die personenbezogenen Daten der Beschäftigten. Die LDI NRW empfiehlt den Arbeitgeber\*innen daher wie bislang, über die betriebliche und/oder private Nutzung des Internets und des betrieblichen E-Mail-Accounts eine schriftliche Regelung zu treffen. Darin sollen die Fragen des Zugriffs, der Protokollierung, der Auswertung und der Durchführung von Kontrollen eindeutig geklärt werden. Zudem sind die Beschäftigten auch künftig über mögliche Überwachungsmaßnahmen und Sanktionen zu informieren.“*

Etwas strenger positioniert sich der LfDI Baden-Württemberg, wenn er in seinem aktuellen Tätigkeitsbericht<sup>3</sup> die folgende Aussage trifft:

*„Ob sie nach § 3 Abs. 2 Nr. 2 und 4 TDDDG an das Fernmeldegeheimnis gebunden sind, wenn sie die private Nutzung des dienstlichen E-Mail-Accounts und Internetzugangs gestatten, ist umstritten. Wenn Arbeitgebende an das Fernmeldegeheimnis gebunden sind, dürfen sie sich oder anderen grundsätzlich nur in dem Maß Kenntnis vom Inhalt oder von den näheren Umständen der Telekommunikation der Beschäftigten verschaffen, wie es für den Betrieb und die Gewährleistung der Sicherheit des Telekommunikationsnetzes und der Telekommunikationsanlagen erforderlich ist. Ausnahmen gelten bei einer Einwilligung der betroffenen Beschäftigten und einer gesetzlichen Erlaubnis. Wir vertreten die Auffassung, dass Arbeitgebende mangels Klärung der Frage bei erlaubter Privatnutzung im Zweifel von der Anwendbarkeit des Fernmeldegeheimnisses ausgehen sollen.“*

Für die Praxis bedeutet dies, dass die Rechtslage nicht abschließend geklärt ist und jedenfalls die Anforderungen der DS-GVO zu beachten sind. Unternehmen sollten daher folgende Maßnahmen umsetzen:

- Klare Regelungen im Unternehmen schaffen, ob die private Nutzung von Internet und E-Mail erlaubt ist oder nicht. Sofern eine entsprechende Nutzung untersagt wird, muss dies unmissverständlich gegenüber allen Beschäftigten kommuniziert werden.

---

<sup>3</sup> Abrufbar unter: [https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2025/03/TB\\_40\\_Datenschutz-2024\\_barrierefrei.pdf](https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2025/03/TB_40_Datenschutz-2024_barrierefrei.pdf)

- Bei Erlaubnis zur Privatnutzung: Aus Gründen der Rechtssicherheit sollte weiterhin eine Einwilligung der Beschäftigten eingeholt werden, welche dem Arbeitgeber Auswertungsmaßnahmen gestattet und die Beschäftigten über Art und Umfang der Datenverarbeitung informiert.
- In allen Fällen: Einbindung des Betriebsrats und Abschluss einer Betriebsvereinbarung

Bei einer Untersagung der Privatnutzung können einige Probleme von vornherein umgangen werden. Auch wenn ein entsprechendes Verbot häufig nicht mehr als „State of the Art“ wahrgenommen wird, lassen sich Auswertungsmaßnahmen jedenfalls deutlich einfacher begründen. Bei einem Verbot der Privatnutzung dürfen Arbeitgeber davon ausgehen, dass sich nur geschäftliche E-Mails in dem Postfach befinden, weshalb eine Kontrolle lediglich die Einhaltung dienstlicher Vorgaben betrifft.

**Praxishinweis:**

Der Umfang der Erlaubnis zur Nutzung von Internet und E-Mail im Unternehmen kann mit einigen Fragestellungen einhergehen. Unternehmen sollten hier ein klares Konzept erarbeiten und zwingend den Datenschutzbeauftragten bzw. den Datenschutzkoordinator einbeziehen. Die vorstehenden Ausführungen können lediglich eine kurze Zusammenfassung der Problematik darstellen und keineswegs eine Prüfung im Einzelfall ersetzen.