

---

Dipl.-Ing. (FH) Oliver Gauer

1. Ausgabe, Juli 2025

ISBN 978-3-98569-262-0

# Datenschutz Grundlagen

(Stand 2025)

DSU-G\_2025



**HERDT**

# Impressum

Matchcode: DSU-G\_2025

Autor: Dipl.-Ing. (FH) Oliver Gauer

1. Ausgabe, Juli 2025

HERDT-Verlag für Bildungsmedien GmbH

Uwe-Zeidler-Ring-12

55294 Bodenheim

Internet: [www.herdt.com](http://www.herdt.com)

E-Mail: [info@herdt.com](mailto:info@herdt.com)

© HERDT-Verlag für Bildungsmedien GmbH, Bodenheim

Druck und Bindearbeiten: Esser printSolutions GmbH, D-75015 Bretten  
Edubook AG, CH-5634 Merenschwand

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder einem anderen Verfahren) ohne schriftliche Genehmigung des Verlags reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Dieses Buch wurde mit großer Sorgfalt erstellt und geprüft. Trotzdem können Fehler nicht vollkommen ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Unser Ziel ist es, unsere Bildungsmedien so zugänglich und verständlich wie möglich zu gestalten. Dieses Buch (Print und E-Book in PDF-Form) wurde gemäß dem Barrierefreiheitsstärkungsgesetzes (BFSG) nach bestem Wissen und Gewissen erstellt. Die Empfehlungen der WCAG (WCAG 2.1, Konformitätsstufe AA) wurden dabei umgesetzt. Gerne nehmen wir Ihre Kritik und Verbesserungsvorschläge per E-Mail an [barrierefreiheit@herdt.com](mailto:barrierefreiheit@herdt.com) entgegen.

Wenn nicht explizit an anderer Stelle des Werkes aufgeführt, liegen die Copyrights an allen Screenshots beim HERDT-Verlag. Sollte es trotz intensiver Recherche nicht gelungen sein, alle weiteren Rechteinhaber der verwendeten Quellen und Abbildungen zu finden, bitten wir um kurze Nachricht an die Redaktion.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Die in diesem Buch und in den abgebildeten bzw. zum Download angebotenen Dateien genannten Personen und Organisationen, Adress- und Telekommunikationsangaben, Bankverbindungen etc. sind frei erfunden. Eventuelle Übereinstimmungen oder Ähnlichkeiten sind unbeabsichtigt und rein zufällig.

Die Bildungsmedien des HERDT-Verlags enthalten Verweise auf Webseiten Dritter. Diese Webseiten unterliegen der Haftung der jeweiligen Betreiber, wir haben keinerlei Einfluss auf die Gestaltung und die Inhalte dieser Webseiten.

Bei der Bucherstellung haben wir die fremden Inhalte daraufhin überprüft, ob etwaige Rechtsverstöße bestehen.

Zu diesem Zeitpunkt waren keine Rechtsverstöße ersichtlich. Wir werden bei Kenntnis von Rechtsverstößen jedoch umgehend die entsprechenden Internetadressen aus dem Buch entfernen.

Die in den Bildungsmedien des HERDT-Verlags vorhandenen Internetadressen, Screenshots, Bezeichnungen bzw. Beschreibungen und Funktionen waren zum Zeitpunkt der Erstellung der jeweiligen Produkte aktuell und gültig. Sollten Sie die Webseiten nicht mehr unter den angegebenen Adressen finden, sind diese eventuell inzwischen komplett aus dem Internet genommen worden oder unter einer neuen Adresse zu finden. Sollten im vorliegenden Produkt vorhandene Screenshots, Bezeichnungen bzw. Beschreibungen und Funktionen nicht mehr der beschriebenen Software entsprechen, hat der Hersteller der jeweiligen Software nach Drucklegung Änderungen vorgenommen oder vorhandene Funktionen geändert oder entfernt.

<b>Bevor Sie beginnen ...</b>	<b>4</b>	6.3 Ausnahmen	36
<b>1 Was bedeutet Datenschutz?</b>	<b>5</b>	6.4 Auftragsverarbeiter außerhalb der EU	37
1.1 Die neue Zeitrechnung	5	<b>7 Der betriebliche Datenschutzbeauftragte</b>	<b>38</b>
1.2 Der Verantwortliche: Datenschutz = Chefsache	6	7.1 Zweck des betrieblichen Datenschutzbeauftragten	38
1.3 Informationelle Selbstbestimmung	6	7.2 Betrieblicher Datenschutzbeauftragter vs. Landesbeauftragter für den Datenschutz	38
1.4 Definition „Datenschutz“	7	7.3 Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten	39
1.5 Definition „Daten“	7	7.4 Freiwillige Benennung eines betrieblichen Datenschutzbeauftragten	42
1.6 Personenbezogene Daten – Ja oder Nein?	8	7.5 Kriterien für die Benennung	42
<b>2 Anwendungsbereich und Aufsichtsbehörden</b>	<b>10</b>	7.6 Aufgaben des betrieblichen Datenschutzbeauftragten	43
2.1 Anwendungsbereich des Datenschutzes	10	7.7 Muster: Bestellung eines internen Mitarbeiters zum betrieblichen Datenschutzbeauftragten	44
2.2 Für welche Unternehmen findet die DSGVO Anwendung?	11	7.8 Meldung an Aufsichtsbehörde und allgemeine Bekanntmachung	45
2.3 Abgrenzung zur Datensicherheit	12	<b>8 Sicherheit in der Verarbeitung – TOM</b>	<b>46</b>
2.4 Überschneidung Datenschutz – Datensicherheit	12	8.1 Datenschutz und Datensicherheit	46
2.5 Aufsichtsbehörden	12	8.2 Technische und organisatorische Maßnahmen	47
2.6 Betrieblicher Datenschutzbeauftragter	13	<b>9 Betroffenenrechte</b>	<b>51</b>
<b>3 Datenverarbeitung: Definition, Vorgehensweise zur Einhaltung und Maßnahmenkatalog</b>	<b>14</b>	9.1 Recht auf transparente Information	51
3.1 Definition „Datenverarbeitung“	14	<b>10 Neuerungen und Änderungen in der DSGVO</b>	<b>55</b>
3.2 Vorgehensweise zur Einhaltung	15	10.1 Neuerungen 2022	55
3.3 Maßnahmenkatalog zur Überprüfung der unternehmenseigenen DSGVO-konformen Datenverarbeitung	16	10.2 Neuerungen 2024	56
<b>4 Grundsätze zur Verarbeitung personenbezogener Daten</b>	<b>17</b>	<b>11 Verletzung des Schutzes personenbezogener Daten</b>	<b>61</b>
4.1 Grundprinzip der Datenverarbeitung: Verbot mit Erlaubnisvorbehalt	17	11.1 Begriffsklärung	61
4.2 Rechtmäßigkeit	18	11.2 Strenge Meldepflicht	62
4.3 Zweckbindung	19	11.3 „Fünf Gebote“ bei Verletzung des Schutzes personenbezogener Daten	63
4.4 Datenminimierung	19	11.4 Meldung an die Aufsichtsbehörde	64
4.5 Richtigkeit	20	11.5 Benachrichtigung der betroffenen Person	64
4.6 Speicherbegrenzung	20	<b>12 Folgen von Verstößen</b>	<b>66</b>
4.7 Integrität und Vertraulichkeit	20	12.1 Verschärfte Sanktionen	66
4.8 Rechenschaftspflicht	21	12.2 Geldbußen nach der DSGVO	66
<b>5 Verzeichnis von Verarbeitungstätigkeiten</b>	<b>22</b>	12.3 Zivilrechtliche Konsequenzen	67
5.1 Pflicht zur Erstellung	22	12.4 Verstöße und verhängte Sanktionen aus der Praxis	67
5.2 Form	22	<b>13 Datenschutz außerhalb der EU</b>	<b>70</b>
5.3 Mindestinhalt	23	13.1 Grundlagen	70
5.4 Optionales, erweitertes Verzeichnis	24	13.2 Konkret: Sonderfall USA	71
5.5 Ausnahmen von der Verpflichtung zur Erstellung eines Verzeichnisses	24	13.3 Der aktuelle Stand: EU-U.S. Data Privacy Framework	72
5.6 Musterformulare	24	<b>Stichwortverzeichnis</b>	<b>76</b>
<b>6 Auftragsverarbeitung</b>	<b>35</b>		
6.1 Definition	35		
6.2 Gestaltung der Auftragsverarbeitung	35		

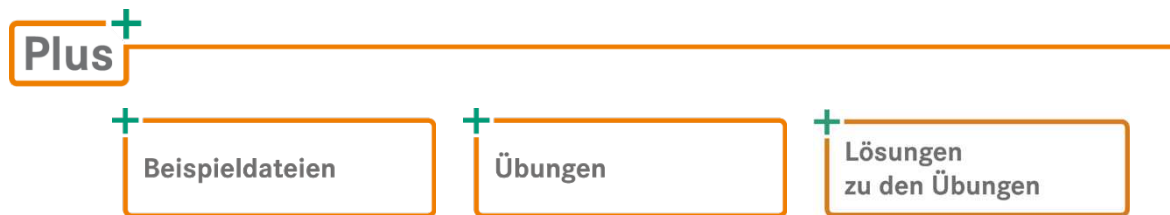
## Bevor Sie beginnen ...

### **HERDT BuchPlus** – unser Konzept:

**Problemlos einsteigen – Effizient lernen – Zielgerichtet nachschlagen**

(weitere Infos unter [www.herdt.com/BuchPlus](http://www.herdt.com/BuchPlus))

Nutzen Sie dabei unsere maßgeschneiderten, im Internet frei verfügbaren Medien:



Wie Sie schnell auf diese BuchPlus-Medien zugreifen können, erfahren Sie unter [www.herdt.com/BuchPlus](http://www.herdt.com/BuchPlus)

# 1

## Was bedeutet Datenschutz?

### Pressemitteilung 6/2025: BfDI verhängt Geldbußen gegen Vodafone

Zitat der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit,  
Prof. L. Specht-Riemenschneider

„Datenschutz wird häufig fälschlicherweise als Hindernis für IT-Investitionen angesehen. Dabei ist das Gegenteil der Fall: Ohne IT-Investitionen drohen Sicherheitsvorfälle und auch Sanktionen der Datenschutzaufsicht. Daher mein Aufruf: Investieren statt Riskieren!“

(Quelle: [https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2025/06\\_Geldbu%C3%9Fe-Vodafone.html](https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2025/06_Geldbu%C3%9Fe-Vodafone.html)).

### 1.1 Die neue Zeitrechnung

Seit dem 25. Mai 2018 gilt in der Europäischen Union (EU) ein einheitliches Datenschutzrecht. Es wurde in Form einer EU-Verordnung erlassen und muss somit nicht in den einzelnen Mitgliedsstaaten durch nationale Gesetze umgesetzt werden, sondern gilt unmittelbar ab diesem Datum.

Die Datenschutz-Grundverordnung (DSGVO) kann von den nationalen Gesetzgebern mit zusätzlichen Regelungen versehen werden, sofern diese nicht der DSGVO entgegenwirken.

In Deutschland trat bereits am 01. Januar 1978 die erste Fassung des Bundesdatenschutzgesetzes (BDSG) in Kraft, die jüngste Fassung ergänzt die DSGVO und ist am 14. Mai 2024 in Kraft getreten („BDSG-neu“). Es beinhaltet unter anderem spezielle Regelungen zu Bonitätsauskünften, zu Scoring-Anfragen, zum Beschäftigtendatenschutz, zur Videoüberwachung und dem betrieblichen Datenschutzbeauftragten.

- ! Die nationalen Datenschutzaufsichtsbehörden werden durch die DSGVO ermächtigt, Geldbußen von **bis zu 20 Millionen Euro** zu verhängen bzw. bei Unternehmen bis zu 4 % ihres Weltjahresumsatzes.

Die DSGVO bezieht sich nicht nur auf Unternehmen, unabhängig von ihrer Größe und Mitarbeiterzahl, ihre Einhaltung und Beachtung der Vorschriften betrifft ebenso Klein(st)betriebe sowie Vereine und sonstige Institutionen.

Hieraus resultiert die nicht unerhebliche Frage: Wer ist für die Einhaltung des Datenschutzes gemäß der DSGVO verantwortlich, wer kann bei Verstößen haftbar gemacht werden?

## 1.2 Der Verantwortliche: Datenschutz = Chefsache

Sind bestimmte Voraussetzungen erfüllt, muss ein Unternehmen einen Datenschutzbeauftragten benennen. Unabhängig davon, ob ein Datenschutzbeauftragter bestellt wurde oder nicht, regelt die DSGVO, dass die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorgaben immer beim Verantwortlichen verbleibt und nicht auf den Datenschutzbeauftragten übertragen wird.

Gemäß Artikel 4 definiert die DSGVO den Verantwortlichen als „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“.

In Unternehmen ist/sind dies in aller Regel der/die Geschäftsführer. Gegen den Verantwortlichen richten sich sowohl Sanktionen der Aufsichtsbehörden als auch Haftungsansprüche der betroffenen Personen. Bei Vereinen ist der Vorstand die verantwortliche Person.

## 1.3 Informationelle Selbstbestimmung

Jede Person hat das Recht auf informationelle Selbstbestimmung. Dies bedeutet, dass jede Person selbst bestimmen kann, welche Daten sie von sich preisgeben will.

Ohne den Einsatz von EDV (elektronischer Datenverarbeitung) war dies sehr einfach zu bewerkstelligen. Eine Frage wie „Wie ist deine Adresse?“ konnte ablehnend beantwortet werden – getreu dem Motto „Was ich nicht sage, erfährt auch niemand“.

Heutzutage kommen annähernd überall Computer zum Einsatz und jeder Anwender gibt riesige Mengen „seiner“ Daten preis. Und das oft, ohne sich darüber im Klaren zu sein.

An dieser Stelle tritt der Datenschutz in Kraft – um zu verhindern, dass ein Anwender ohne seine ausdrückliche Zustimmung Daten von sich preisgibt bzw. die gegenüberliegende Seite den Anwender explizit auf die Verarbeitung seiner Daten aufmerksam macht und in diesem Zuge das Einverständnis zur Verarbeitung einholt.

## 1.4 Definition „Datenschutz“

Durch den Datenschutz werden nicht die Daten selbst geschützt, sondern das Recht auf informationelle Selbstbestimmung. Der Datenschutz bezieht sich also ausschließlich auf natürliche Personen zum Schutz deren Persönlichkeitsrechte.

## 1.5 Definition „Daten“

### Daten im Allgemeinen

Jegliche Art von Information stellt Daten dar, jedoch sind nicht alle datenschutzrelevant.

#### Beispiele:

- ✓ Zeitpunkte (Lieferdaten verschiedener Bestellungen)
- ✓ Geburtsdaten der Kinder
- ✓ Einkaufs-/Verkaufspreise
- ✓ Zahlungsinformationen bei Kreditkartennutzung (Wo wurde was gekauft?)
- ✓ Die Einwahlposition des Mobiltelefons (Bewegungsdaten)
- ✓ Messdaten der Wetterstation
- ✓ Technische Daten eines Pkws
- ✓ Besuchte Seiten im Internet (Browserverlauf als „digitale Bewegungsdaten“)

### Daten im Sinne des Datenschutzes

Für den Datenschutz sind nur personenbezogene Daten von Belang, jedoch gehen diese weit über den Name und das Geburtsdatum einer Person hinaus.

#### Beispiele:

- ✓ Telefonnummer
- ✓ Wohnort
- ✓ IP-Adresse
- ✓ Religionszugehörigkeit
- ✓ Parteizugehörigkeit
- ✓ Gesundheitsdaten
- ✓ E-Mail-Adresse
- ✓ ...