



1. Auflage
Dein Plus:
39 Übersichten
und 31 Leitsätze

Datenschutz *leicht gemacht* ✓

Management personenbezogener Daten
im Unternehmen: EU-DSGVO, BDSG & DSMS

*Alexander Deicke
Leonie Schönhagen*

Edition Wissenschaft & Praxis

EWP



Politiker versprechen. DRACOON liefert.
Ihre Daten waren nie sicherer.

- DSGVO-konformer Cloud-Speicher
- Höchste Sicherheitszertifizierungen für volle Compliance
- Ende-zu-Ende-Verschlüsselung inkl.
clientseitiger Verschlüsselung



CLOUD
COMPUTING
COMPLIANCE
CONTROLS
CATALOGUE



Management
System
ISO/IEC 27001:2013
www.dracoon.com
E 910560422



100%
Service
Qualität
Zukunft

dracoon.com

Datenschutz – *leicht gemacht*

GELBE SERIE – *leicht gemacht*
Herausgegeben von Helwig Hassenpflug

Die *leicht gemacht*-Lehrbücher führen Studierende erfolgreich in die Fächer Recht (GELBE SERIE) und Steuern / Rechnungswesen (BLAUE SERIE) ein, indem sie besonderes Augenmerk auf didaktische Erfordernisse legen und die wichtigsten Grundlagen vermitteln. Die Bände richten sich insbesondere an Anfängerinnen und Anfänger ohne Vorkenntnisse und sind daher ideal für den Einstieg und zur Prüfungsvorbereitung.

Weitere spannende Bände unter:
www.leicht-gemacht.de

Datenschutz *leicht gemacht* ✓

Management personenbezogener Daten
im Unternehmen: EU-DSGVO, BDSG & DSMS

von Alexander Deicke und Leonie Schönhagen

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Umschlagbild: © Sean Pavone – iStock

Alle Rechte vorbehalten

©2024 Edition Wissenschaft & Praxis
bei Duncker & Humblot GmbH, Berlin

Satz: Michael Haas

Druck: Prime Rate Kft., Budapest, Ungarn
Gedruckt auf FSC-zertifiziertem Papier

leicht gemacht® ist ein eingetragenes Warenzeichen

ISBN 978-3-87440-389-4 (Print)

ISBN 978-3-87440-789-2 (E-Book)

www.duncker-humblot.de

Inhalt

I. Management Summary

II. Datenschutzrecht

Lektion 1: Was ist Datenschutz?	14
Lektion 2: Was ist der gesetzliche Rahmen?	18
Lektion 3: Definitionen	27
Lektion 4: Grundsätze des Datenschutzes	33
Lektion 5: Rechtsgrundlagen der Verarbeitung	40
Lektion 6: Drittparteien und Datentransfer	65
Lektion 7: Das Verarbeitungsverzeichnis, VVT	77
Lektion 8: Sanktionen und Bußgelder	80
Lektion 9: Weitere Aspekte, die im Datenschutz eine Rolle spielen	82

III. Managementsysteme

Lektion 10: Was ist ein Managementsystem?	92
Lektion 11: Die Implementierung eines Managementsystems	94
Lektion 12: Das Compliance Management System (CMS)	96
Lektion 13: Das Datenschutzmanagementsystem.	97
Lektion 14: Interdisziplinarität	112
Lektion 15: Sensibilisierung ist das Herz aller Systeme.	124

IV. Zukunft des Datenschutzes

Lektion 16: Was passiert, wenn ich mich nicht an den Datenschutz halte?	131
Lektion 17: Frühzeitig Risiken erkennen und managen.	132
Lektion 18: Mehrwert generieren und Vertrauen aufbauen	133
Lektion 19: Noch ein kleiner Ausblick	135
Sachregister.	142
Abkürzungen.	9

Leitsätze und Übersichten

Leitsatz	1	Datenschutz – Wer hat's erfunden?	17
Übersicht	1	Entwicklung des BDSG	18
Übersicht	2	Übersicht über die Datenschutzgesetze in Deutschland	19
Übersicht	3	Struktur der Gesetzgebung zum Datenschutz in Deutschland	21
Übersicht	4	Struktur der Datenschutzaufsicht in Deutschland ..	22
Leitsatz	2	Datenschutzrecht als Querschnittsmaterie	23
Leitsatz	3	Der räumliche Anwendungsbereich der DSGVO	26
Übersicht	5	Was sind personenbezogene Daten?	28
Übersicht	6	Übersicht über den Begriff der Verarbeitung	29
Übersicht	7	Vergleich zwischen anonymisierten, pseudonymisierten und personenbezogenen Daten ..	31
Leitsatz	4	Verarbeitung von Daten	32
Übersicht	8	Grundsätze der DSGVO	33
Leitsatz	5	Grundsätze der Datenverarbeitung	39
Übersicht	9	Grundlagen rechtmäßiger Verarbeitung	41
Übersicht	10	Auszug Ermächtigungsgrundlagen aus Artikel 6 der DSGVO	45
Übersicht	11	Was zählt zu personenbezogenen Daten?	47
Leitsatz	6	Verbot mit Erlaubnisvorbehalt	47
Leitsatz	7	Rechte der Betroffenen	49
Übersicht	12	Betroffenenrechte aus der DSGVO	50
Leitsatz	8	Betroffene müssen informiert werden	52
Übersicht	13	Checkliste für die Datenschutzerklärung	53
Übersicht	14	Ablauf eines Auskunftsprozesses	56
Leitsatz	9	Anspruch auf Auskunft	57

Leitsätze und Übersichten

Übersicht 15	Bearbeitung eines Antrags auf Löschung	59
Übersicht 16	Erstellung eines Löschkonzepts nach DSGVO	60
Übersicht 17	Exemplarisches Löschkonzept	62
Leitsatz 10	Recht auf Löschung.	62
Übersicht 18	Muster eines Widerspruchs gegen die Datenverarbeitung	64
Leitsatz 11	Recht auf Widerspruch	64
Übersicht 19	Muster einer Auftragsverarbeitungsvereinbarung ..	66
Übersicht 20	Verhältnis zwischen den Personen bei der Auftragsverarbeitung	67
Übersicht 21	Bestandteile einer Auftragsverarbeitungsvereinbarung	71
Leitsatz 12	Mittel der parteiübergreifenden Datenverarbeitung..	72
Übersicht 22	Modelle und Rollen im Datenverarbeitungsprozess ..	75
Leitsatz 13	Internationale Datenübermittlung.	76
Übersicht 23	Das Verarbeitungsverzeichnis gemäß Artikel 30 der DSGVO	78
Leitsatz 14	Folgen von Verstößen	81
Übersicht 24	Beispiele für technische und organisatorische Maßnahmen („TOMs“)	83
Übersicht 25	Aufgaben eines Datenschutzbeauftragten	86
Übersicht 26	Bestellungsurkunde eines Datenschutzbeauftragten .	87
Leitsatz 15	Datenschutzvorfälle	89
Übersicht 27	Meldung eines Datenschutzvorfalls.	90
Übersicht 28	Implementieren eines Datenschutzmanagementsystemsgaben.	93
Leitsatz 16	Managementsysteme.	95
Übersicht 29	Compliance Management System (IDW PS 980)	96

Leitsätze und Übersichten

Übersicht 30	Ebenen eines Datenschutzmanagementsystems	101
Leitsatz 17	Die Pyramide eines Managementsystems	101
Leitsatz 18	Der Datenschutzbeauftragte als Bindeglied	104
Leitsatz 19	Der Datenschutzbeauftragte als Risikomanager	105
Übersicht 31	Datenschutzbeauftragter nach Artikel 37 der DSGVO	107
Leitsatz 20	Segregation of Duties	111
Übersicht 32	Aufbau eines ISMS	113
Leitsatz 21	Datenschutzmanagementsysteme	115
Übersicht 33	Verhältnis von Compliance, DSMS und ISMS	116
Leitsatz 22	Prozessorientierung	117
Übersicht 34	Beantwortung eines Auskunftsverlangens Artikel 15 der DSGVO	118
Leitsatz 23	Informationssicherheit	120
Übersicht 35	Der BCM-Kreislauf	121
Leitsatz 24	Handlungsanweisungen	122
Übersicht 36	Implementierung der DSGVO	123
Übersicht 37	Internationale Koordination des Datenschutzes in einem Unternehmen	127
Leitsatz 25	Koordinatoren für den Datenschutz	127
Leitsatz 26	Digitales Dokumentenmanagement	129
Leitsatz 27	Haftungsszenarien	134
Übersicht 38	Vermeidung von Haftungsfällen	136
Leitsatz 28	Musterstruktur für regulatorische Funktionen	136
Leitsatz 29	Prozessorientierung in Unternehmen	138
Übersicht 39	Was ist Legal Tech?	139
Leitsatz 30	Nachhaltigkeit	141
Leitsatz 31	Komplexität des Datenschutzes	141

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
AI	Artificial Intelligence
AO	Abgabenordnung
APPI	Act on the Protection of Personal Information
Art.	Artikel
Aufb.Pflicht	Aufbewahrungs pflicht
AVV	Auftragsverarbeitungsvereinbarung
Bay DB	Bayerischer Datenschutzbeauftragter
BCM	Business Continuity Management
BCP	Business Continuity Plans
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für Datenschutz und Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BIA	Business Impact Analyse
BW	Baden-Württemberg
BY	Bayern
bzw.	beziehungsweise
C-C	Controller zu Controller
CCPA	California Consumer Privacy Act
CMS	Compliance Management System
DE	Deutschland
DPIA	Data Protection Impact Assessment
DS	Datenschutz
DSB	Datenschutzbeauftragter

DSGVO	Datenschutzgrundverordnung
DSK	Datenschutzkonferenz
DSMS	Datenschutzmanagementsystem
DV	Datenverarbeitung
ESG	Environmental Social Governance
EU	Europäische Union
EuGH	Europäischer Gerichtshof
ev.	evangelisch
EWR	Europäischer Wirtschaftsraum
f.	folgende
ff.	fortfolgende
GF	Geschäftsführer
ggf.	gegebenenfalls
GRC	Governance, Risk und Compliance
HDSG	Hessisches Datenschutzgesetz
HGB	Handelsgesetzbuch
HH	Hansestadt Hamburg
HR	Human Resources
i.d.R.	in der Regel
ID	Identifier
IDW	Institut der Wirtschaftsprüfer
IP-Adresse	Internet-Protokoll-Adresse
IPO	Initial Public Offering
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization

IT	Information Technology
JC	Joint Controller
kath.	katholisch
KI	Künstliche Intelligenz
KVP	Kontinuierlicher Verbesserungsprozess
LDSG	Landesdatenschutzgesetz
LfD	Landesbeauftragter für Datenschutz
LfDI	Landesbeauftragter für Datenschutz und Informationsfreiheit
LGPD	brasilianisches Datenschutzgesetz (Lei Geral de Proteção de Dados Pessoais)
Lit.	Literatur
LkSG	Lieferkettensorgfaltspflichtengesetz
M&tA	Mergers and Acquisitions
MA	Mitarbeiter
max.	maximal
Meck-Pomm.	Mecklenburg-Vorpommern
NDS	Niedersachsen
Nr.	Nummer
NRW	Nordrhein-Westfalen
o.	oder
ö.-r.	öffentlich-rechtlich
PDCA-Modell	Plan-Do-Check-Act Modell
PDPA	Personal Data Protection Act 2012
PDPB	Personal Data Protection Bill
pers.bez.	personenbezogene

PIPEDA	Personal Information Protection and Electronic Documents Act
PIPL	Personal Information Protection Law
POPIA	Protection of Personal Information Act
priv.	privat
Rh.-Pf.	Rheinland-Pfalz
Sa.-Anh.	Sachsen-Anhalt
SCCs	Standard Contractual Clauses
SH	Schleswig-Holstein
s.u.	siehe unten
THÜ	Thüringen
TIA	Transfer Impact Assessment
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOMs	Technische und organisatorische Maßnahmen
TQM	Total Quality Management
TTDSG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien
u.	und
u.U.	unter Umständen
USA	United States of America
usw.	und so weiter
VO	Verordnung
VV	Verarbeitungsverzeichnis
VVT	Verzeichnis über Verarbeitungstätigkeiten
z.B.	zum Beispiel

I. Management Summary

Karla Krake ist **Unternehmerin** und möchte mit Ihrem Hyperscaler Start-Up möglichst alle für ihr Unternehmen zugänglichen **Daten maximal effizient nutzen**. Sie verspricht sich damit großes Wachstumspotential für ihr jetzt schon erfolgreiches Start-Up. Weil sie weiß, dass es den Datenschutz gibt und auch schon von allgemeinen Persönlichkeitsrechten gelesen hat, bittet sie ihren alten Studienfreund **Peter Pingel**, ihr einige Fragen zum Thema Datenschutz zu beantworten. Peter nimmt es mit allen **regulatorischen Vorgaben nämlich sehr genau**, und gerade, weil sie etwas Sorge vor der persönlichen Haftung hat, will sie sich auch mal seine Ansichten anhören.

Nachfolgend fließen zusätzlich auch noch die praktischen Erfahrungen der Autorin und des Autors, als **Juristen und Datenschutzbeauftragte** mit ein, damit das hier vorliegende Buch den ersten Einstieg in das Thema Datenschutz erleichtert und an der einen oder anderen Stelle Impulse für mehr gibt.

II. Datenschutzrecht

Lektion 1: Was ist Datenschutz?

■ Fall 1

Was ist Datenschutz, woher kommt er und warum ist er wichtig?

Karla Krake und Peter Pingel treffen sich zu einem ersten Gespräch über das Thema Datenschutz: „Kannst du mir, Peter, bitte einmal erklären, was **Datenschutz** eigentlich wirklich ist? Ständig höre ich diesen Begriff überall und habe den Eindruck, dass das Wort recht inflationär verwendet wird.“ - „Ja, den Eindruck habe ich manchmal auch, Karla. Also lass mich von vorne beginnen: Es kommt ...“, Karla springt gleich auf und ruft: „Und bitte verständlich erklären und lass dabei dieses **„Es kommt darauf an“** weg“. Peter Pingel muss schmunzeln. „Das ist wohl eine Berufskrankheit von Jurist:innen“, meint er und fängt langsam an.

„Also erstmal ganz allgemein: Datenschutz umfasst alle **Verarbeitungen von personenbezogenen Daten**.“

„Wie bitte?“, fragt Karla. „Nun ja, das war ja nur die Einleitung“, grinst Peter und fährt fort.

„Zum Hintergrund: Der Sinn und Zweck vom Datenschutz liegt darin, die **Privatsphäre natürlicher Personen** zu schützen und sicherzustellen, dass sie die **Hoheit und Kontrolle über ihre Daten** haben und weiterhin behalten. Diesen Grundsatz sollten wir immer im Hinterkopf behalten.“

Die Verarbeitung von personenbezogenen Daten findet in allen Lebensbereichen statt. **Ich behaupte, es gibt kein Unternehmen, keine juristische Person, Behörde oder sonstige öffentliche Stelle, die nicht in irgendeiner Form personenbezogene Daten verarbeitet**: wenn sich jemand nach einem Umzug beim Einwohnermeldeamt mit dem Wohnort anmeldet; wenn jemand an der Kasse im Supermarkt mit einer EC-Karte bezahlt oder Bonuspunkte sammelt; beim Besuch fast jeder Webseite usw. In all diesen Situationen werden personenbezogene Daten verarbeitet.

Um den **Missbrauch von personenbezogenen Daten zu verhindern**, wird die Datenverarbeitung reguliert. Die regulatorischen Gesetze umfassen

zum Beispiel die Datenschutzgrundverordnung (die „**DSGVO**“) und das Bundesdatenschutzgesetz (das „**BDSG**“), aber dazu später mehr.“

Wie ist die historische Entwicklung?

„Aber wo kommt denn dieser Datenschutz jetzt her? Gibt es hierzu Gründe oder Ursachen in der Vergangenheit? Ich bin ja nicht zwingend ein Fan von Geschichte, aber vielleicht verstehe ich dann alles etwas besser?“

„Gute Frage, Karla. Wusstest du, dass 1970 in Hessen mit dem **Hessischen Datenschutzgesetz („HDSG“)** das weltweit **erste Datenschutzgesetz** in Kraft trat? 1977 wurde mit dem **Bundesdatenschutzgesetz** dann das erste deutsche Datenschutzgesetz auf Bundesebene verabschiedet. Hintergrund der Gesetzgebungsbestrebungen war die zunehmende Automatisierung der Datenverarbeitung, sowohl in der **Verwaltung als auch in nicht-öffentlichen Stellen**, und die damit verbundenen neuen Nutzungsmöglichkeiten. Damit einher gingen schon damals Missbrauchsrisiken, sowohl durch den Staat als auch durch Private: Daten können zunehmend aus dem Kontext genommen und missbraucht werden. Die Konsequenzen für den Einzelnen können schwerwiegend sein.“

Mit seinem Volkszählungsurteil etablierte das Bundesverfassungsgericht 1983 das **Grundrecht auf informationelle Selbstbestimmung** als Ausfluss des allgemeinen **Persönlichkeitsrechts und der Menschenwürde**. Das gilt bis heute gilt als Meilenstein des Datenschutzes. Es bestimmte mit der Entscheidung zahlreiche Bedingungen für die Zulässigkeit der Datenverarbeitung durch den Staat, unter anderem die heute gut bekannte **Zweckbindung**. Das Urteil war eine Aufforderung an die Gesetzgeber auf Landes- und Bundesebene, das Datenschutzrecht zu reformieren. Die Folge war eine Novellierung sowohl des **BDSG** als auch zahlreicher Landesdatenschutzgesetze. Wieder war Hessen Vorreiter in dieser Entwicklung. Das **dritte Hessische Datenschutzgesetz** forderte sowohl für die Erhebung als auch für die folgende Verarbeitung personenbezogener Daten eine gesetzliche Grundlage, legte die Zweckbindung fest, festigte den Landesdatenschutzbeauftragten als Kontrollinstanz und formulierte damit erstmals zahlreiche heute bekannte Datenschutzprinzipien. Weitere Bundesländer folgten und erneuerten ihre Datenschutzgesetze, bis schließlich 1990 auch der Bund die Forderungen des Bundesverfassungsgerichts