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

DRACOON

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**

5 TESTED TYP 2 CLOUD COMPUTING COMPLIANCE CONTROLS CATALOGUE

TÜVRheinland ZERTIFIZIERT Management System ISO/IEC 27001:2013 www.tuv.com ID 9105042422

Software Bundesverband IT-Mittelstand Made in Germany 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

Edition Wissenschaft & Praxis

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

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

III. Managementsysteme

IV. Zukunft des Datenschutzes

Leitsätze und Übersichten

Leitsätze und Übersichten

Leitsätze und Übersichten

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
AI	Artificial Intelligence
AO	Abgabenordnung
APPI	Act on the Protection of Personal Information
Art.	Artikel
Aufb.Pflicht	Aufbewahrungspflicht
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&A	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 Nutzungsmöglichmöglichkeiten. 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