Kranig · Sachs · Gierschmann

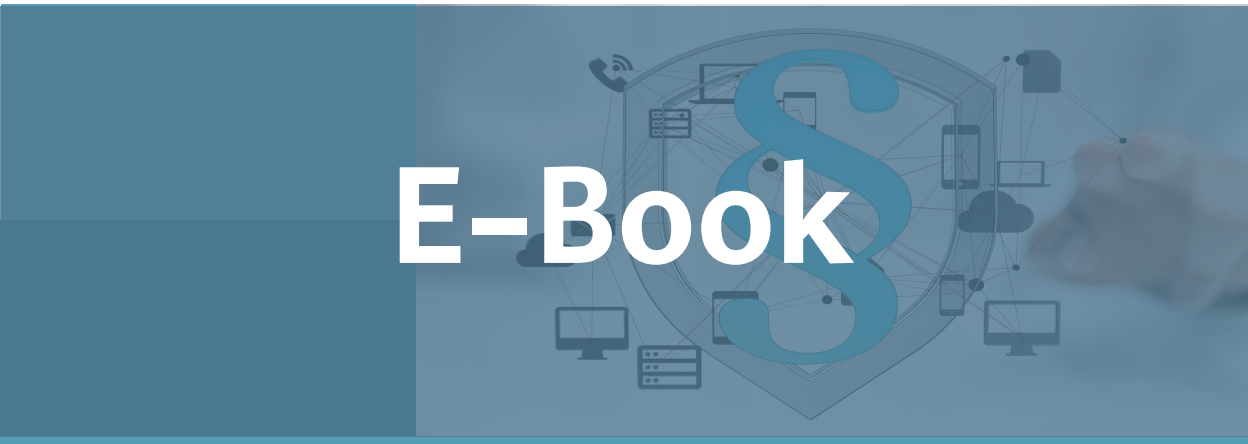
Datenschutz-Compliance nach der DS-GVO

Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden

Best Practice für
Compliance und Sicherheit

comply.

2. Auflage



Reguvis
Bundesanzeiger Verlag

Datenschutz Compliance nach der DS–GVO

Datenschutz-Compliance nach der DS-GVO

Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden

Thomas Kranig, Jurist, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA),

Andreas Sachs, Dipl.-Informatiker, Leiter des technischen Referats sowie Vertreter des Präsidenten beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) und

Markus Gierschmann, Dipl.-Wirtschaftsingenieur, Finanzökonom (ebs), CIPP/E, CIPM, Datenschutzbeauftragter (udis, TÜV), Datenschutzauditor (TÜV), Unternehmensberater

2. Auflage

Reguvis

Bundesanzeiger Verlag

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.

Reguvis | Bundesanzeiger Verlag

Eine Marke der Bundesanzeiger Verlag GmbH · Amsterdamer Straße 192 · 50735 Köln
www.reguvis.de

Beratung und Bestellung:

Tel.: +49 (0) 221 97668-315
Fax: +49 (0) 221 97668-271
E-Mail: wirtschaft@bundesanzeiger.de

Weitere Informationen finden Sie auch in unserem Themenportal unter
www.betrifft-unternehmen.de

ISBN (Print): 978-3-8462-1023-9

ISBN (E-Book): 978-3-8462-1024-6

Herstellung: Günter Fabritius
Produktmanagement: Marieke Stöcker-Pritz
Satz: Cicero Computer GmbH, Bonn
Druck und buchbinderische Verarbeitung: Appel & Klinger Druck und Medien GmbH, Schneckenlohe
Titelabbildung: © vege Fotolia

Printed in Germany

Vorwort von Ulrich Kelber

Ein Jahr nach dem endgültigen Inkrafttreten der europäischen Datenschutz-Grundverordnung (DS-GVO) zeichnen sich erste Erfahrungen und Entwicklungen ab, die im Rahmen der Evaluierung im Jahr 2020 noch genauer zu betrachten sein werden.

Deutlich ist aber schon heute, dass die Europäische Union mit der DS-GVO einen auch international viel beachteten und zur Orientierung genutzten Standard in Sachen Datenschutz gesetzt hat. Nicht nur Japan und Kalifornien orientieren sich bei ihrer Datenschutzgesetzgebung an der DS-GVO, weitere südamerikanische und afrikanische Länder informieren sich intensiv, um die eigene Gesetzgebung entsprechend zu regeln.

Dennoch ist der Rechtsrahmen der DS-GVO an vielen Stellen noch unscharf, weil nicht zu allen wichtigen Bereichen schon eindeutige und abschließende Gerichtsurteile vorliegen, dies wird erst in einigen Jahren der Fall sein. Der europäische Datenschutzausschuss und die deutsche Datenschutzkonferenz versuchen mit ihren Leitlinien, Anleitungen, Orientierungshilfen und Entschließungen Klarheit hinsichtlich der einheitlichen Auslegung und Bewertung zu geben.

Auch wenn vieles, das die DS-GVO regelt, in Deutschland schon vor deren Inkrafttreten im Bundesdatenschutzgesetz stand und galt, ist Orientierung gefragt. Was muss neu oder anders als bisher geregelt werden, wie sensibilisiere ich die gesamte Mitarbeiterschaft für datenschutzkonformes Verhalten, wie müssen Verfahrensabläufe geregelt werden, damit der Datenschutz nicht zum Hemmschuh wird? Mit diesen und vielen weiteren Fragen befasst sich das vorliegende Buch. Es ist aus der Praxis für die Praxis geschrieben. Die Tatsache, dass die Autoren den Datenschutz beruflich betreiben, aber auf unterschiedlichen Seiten – Aufsicht und Verarbeitungspraxis – trägt dazu bei, dass dieses Buch sehr praxisorientiert konzipiert ist und die unterschiedlichen Sicht- und Herangehensweisen verständlich macht.

Die jetzt vorliegende 2. Auflage des Buches nimmt dabei schon die ersten Erfahrungen mit der praktischen Umsetzung und Aufsicht der DS-GVO auf und bietet damit eine echte Orientierungshilfe für die Arbeit in Betrieben und Ämtern. Es ist ein „wertvolles Werkzeug" für die Datenschutzverantwortlichen, wie Dr. Eugen Ehmann in seinem Vorwort für die 1. Auflage richtig feststellte.

Bonn, September 2019

Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

Vorwort von Dr. Eugen Ehmann zur 1. Auflage

Zäsur und Meilenstein – beide Begriffe beschreiben die Datenschutz-Grundverordnung (DS-GVO) unter verschiedenen Aspekten, aber gleichermaßen treffend. Die DS-GVO bildet eine Zäsur, weil sie eine über 40 Jahre währende Datenschutzepoche in Deutschland zum Abschluss bringt. Diese Epoche begann nach ersten gesetzgeberischen Vorläufen auf Landesebene (Hessen 1970) spätestens mit dem BDSG 1977. Das Volkszählungsurteil von 1983 gestaltete sie verfassungsrechtlich aus. Sie war entscheidend geprägt durch nationales Datenschutzrecht. Die EU-Datenschutz-Richtlinie von 1995 modifizierte diese Situation allenfalls, bedurfte sie doch der Umsetzung in nationales Recht, um Wirkung entfalten zu können. Zudem konnte der nationale Gesetzgeber wesentliche Bereiche nach wie vor eigenständig regeln.

All das ändert die DS-GVO am 25. Mai 2018 umfassend, letztlich sogar radikal. Nationales Recht tritt in seiner Bedeutung völlig in den Hintergrund. Die DS-GVO regelt alles Wesentliche selbst. Einer Umsetzung in nationales Recht bedarf sie als EU-Verordnung gewissermaßen definitionsgemäß nicht. Die von ihrer Zahl her beeindruckenden „Öffnungsklauseln" sind genau genommen bloße „Spezifizierungsklauseln", welche die Vorgaben der DS-GVO lediglich im einen oder anderen Detail präzisieren, sie aber als solche nicht verändern können. So gesehen stellt die DS-GVO einen Meilenstein dar, der für die künftige Entwicklung des Datenschutzes in der gesamten Europäischen Union auf Jahrzehnte hinaus maßgebend sein wird.

Jeder Praktiker steht vor der Frage, wie er mit dieser Situation des Umbruchs und mit dem ungewohnten wie in mancherlei Hinsicht noch unklaren Rechtsrahmen umgehen soll. Abwarten, bis möglichst alles Wichtige geklärt ist, beispielsweise durch Papiere des Europäischen Datenschutzausschusses, stellt keine ernsthafte Option dar. Denn am 25. Mai 2018 müssen die Vorgaben der DS-GVO von einem Tag auf den anderen eingehalten werden. Eine Übergangsfrist im eigentlichen Sinn gibt es dabei nicht, lediglich eine Art Vorbereitungsfrist, die bereits seit dem Inkrafttreten der DS-GVO am 25. Mai 2016 läuft. Einfach ohne Plan punktuell los zu agieren, verbietet sich andererseits ebenso. Zu groß erscheint die Gefahr, dass dabei gerade das Wesentliche übersehen wird. Gefragt ist also Orientierung darüber, was in einer Situation der Unsicherheit jetzt schon sinnvoll angegangen werden kann.

An dieser Stelle setzt das vorliegende Werk an. Ausgerichtet an Ablaufprozessen legt es dar, welche Anforderungen die DS-GVO stellt und was daraus an Handlungsbedarf abzuleiten ist. Im Vordergrund steht also das, was auf jeden Fall angegangen werden muss und auch schon jetzt angegangen werden kann. Dabei liefert die Handlungshilfe ungeachtet zahlreicher Checklisten keine fertigen Patentrezepte „zum Abhaken" und das ist auch gut so. Denn zu unterschiedlich sind – worauf die Autoren zutreffend hinweisen – die Verhältnisse in den einzelnen Branchen und den einzelnen Unternehmen.

Lösungen, die Nutzer des Werks auf dieser Basis in der Praxis herausarbeiten, können nicht detailgenau für alle Zukunft in Stein gemeißelt sein. Betriebliche Abläufe verändern sich immer wieder aufgrund wirtschaftlicher und sonstiger Notwendigkeiten. Die Diskussion über die Umsetzung der DS-GVO und die für die Zukunft einerseits erhofften, manchmal

aber vielleicht auch gefürchteten „Papiere aus Brüssel" (namentlich des Europäischen Datenschutzausschusses) werden immer wieder neue Erkenntnisse liefern, gerade in der Anfangszeit der Geltung der DS-GVO. Doch all dies lässt sich bewältigen, wenn man erst einmal auf einem soliden Fundament aufbauen kann. Wer sich ein solches schaffen will, dem bietet diese Handlungshilfe kompetente Unterstützung.

Verantwortlichen für die Verarbeitung einerseits und Aufsichtsbehörden andererseits weist die DS-GVO naturgemäß unterschiedliche Aufgaben zu. Gleichwohl widmen sie sich – von verschiedenen Seiten herkommend – denselben Themen. Es erscheint deshalb nur konsequent, dass sich für die Erstellung dieser Handlungshilfe Autoren beider Provenienz zusammengefunden haben. Sie bringen unterschiedliche Sichtweisen ein – für den Nutzer ganz sicher ein erheblicher Vorteil.

Der gut strukturierten Handlungshilfe ist zu wünschen, dass sie viele Verantwortliche auf fruchtbare Weise nutzen. Das gestalten, was jetzt schon möglich ist, statt auf das zu warten, was irgendwann kommen mag – wer so denkt, bekommt mit ihr ein wertvolles Werkzeug in die Hand, das ihm effektiv weiterhelfen wird.

Ansbach, im Februar 2017

Dr. Eugen Ehmann

Vorwort der Autoren zur 2. Auflage

Etwa eineinhalb Jahre nach Anwendbarkeit der DS-GVO und des neuen BDSG sind wir der Auffassung, dass für diese von uns so bezeichnete Handlungshilfe noch ein nachhaltiger Bedarf besteht. Zahlreiche Prüfungen der Aufsichtsbehörde zeigen (leider), dass der Paradigmenwechsel, der mit der DS-GVO eingetreten ist, bei vielen Verantwortlichen und Auftragsverarbeitern noch nicht angekommen ist. Insbesondere die Rechenschaftspflicht, aber auch die sonstigen Nachweispflichten, verlangen ein systematisches Herangehen an die Datenverarbeitung, die Sicherstellung der Betroffenenrechte und auch die Handhabung von Datenschutzverletzungen. Die enorm gestiegene Anzahl von Beschwerden bei den (zumindest deutschen) Aufsichtsbehörden, die zu einem ganz erheblichen Teil auch begründet sind, zeigen zum einen, dass betroffene Personen sich ihrer Rechte mehr und mehr bewusst werden und sie auch wahrnehmen, zum anderen, dass Verantwortliche in vielen Bereichen noch überfordert sind. Insbesondere die hohe Anzahl von Beschwerden wegen nicht erfolgter oder ungenügender Auskunftserteilung gäbe es nicht, wenn Verantwortliche sich wirklich bewusst wären, dass es dieses Recht gibt und dass sie verpflichtet sind, vorbereitet zu sein, wenn ein entsprechender Auskunftsanspruch geltend gemacht wird.

Für diese, aber auch andere Fälle ist unsere Handlungshilfe gedacht. Mit einer sehr detaillierten Strukturierung auf der Basis des PDCA-Zyklus haben wir die Themen so aufbereitet, dass Sie, liebe Leserin, lieber Leser, die Möglichkeit haben, für viele Teilbereiche Gliederungen zu übernehmen und für die eigene Arbeit zu verwenden.

Etwas intensiver haben wir uns mit der Frage befasst, was Verantwortliche bei der Einbindung von Auftragsverarbeitern oder der Zusammenarbeit auf der Basis einer gemeinsamen Verantwortlichkeit berücksichtigen sollten. Dabei haben wir uns auch ausführlicher mit den Anforderungen des Art. 25 DS-GVO, des Datenschutzes durch Technikgestaltung, auseinandergesetzt. Wir haben die vom Europäischen Datenschutzausschuss (EDSA) veröffentlichten Leitlinien wie z.B. das WP 250 bei der Überarbeitung der Handhabung der Datenschutzverletzung durch Integration mit Informationssicherheit und der Darstellung einer Methodik zur Bewertung von Datenschutzverletzungen einbezogen.

Erfreut konnten wir feststellen, dass wir unsere Ausführungen zu einem zentralen Begriff der DS-GVO, dem Risiko, nicht wesentlich ändern mussten, sondern sich unser Verständnis auch in den deutschen und europäischen Papieren zu diesem Thema wiederfindet.

Dieses Buch kann, wie von Anfang an geplant, keine Antwort darauf geben, wie die Anforderungen der DS-GVO, des BDSG und/oder der Landesdatenschutzgesetze umgesetzt werden sollen. Ziel ist vielmehr nach wie vor, möglichst vollständig darzustellen, was auf dem Weg zur Datenschutz-Compliance gemacht werden muss. Insofern könnte der gerade erst veröffentlichte ISO-Standard 27701 für ein Datenschutz-Managementsystem (DSMS) als Erweiterung eines Informationssicherheitsmanagementsystems (ISMS) sich in der Praxis als hilfreich erweisen. Dieser Standard wird nach unserer Auffassung im internationalen Kontext Maßstäbe setzen.

Es besteht die begründete Hoffnung, dass das neue Instrument der Zertifizierung bald durch akkreditierte Unternehmen Einzug in den Unternehmensalltag findet, damit insbe-

sondere die Sorgfaltspflicht bezüglich der Auswahl von Dienstleistern anhand geeigneter technischer und organisatorischer Maßnahmen (TOM) für (kleine und mittlere) Unternehmen ohne größeren Aufwand machbar ist. Ob dann irgendwann einmal auch ein Datenschutz-Managementsystem nach Art. 42 DS-GVO zertifiziert werden kann, was sicherlich wünschenswert wäre, aber zumindest von Seiten der (deutschen) Aufsichtsbehörden zum jetzigen Zeitpunkt aufgrund formaler Restriktionen nicht als möglich angesehen wird, bleibt abzuwarten.

Die Anforderungen, die auf dem Weg zur Datenschutz-Compliance zu erfüllen sind, werden zunehmend klarer, stehen aber – bezogen auf das notwendige einheitliche europäische Verständnis – lange noch nicht fest. Mit großer Aufmerksamkeit werden wir darauf zu achten haben, welche Meilensteine der Europäische Gerichtshof dabei setzt, was er zuletzt mit mehreren Entscheidungen zur Konkretisierung der Anforderungen für die gemeinsame Verantwortlichkeit getan hat.

Die Befürchtung, dass die Aufsichtsbehörden das Land flächendeckend mit Bußgeldern überziehen, hat sich nicht bewahrheitet. Gründe dafür mögen neben der Überlastung der Aufsichtsbehörden durch die exorbitant angestiegene Zahl der Beschwerden und Beratungsanfragen auch eine teilweise Unschärfe bezüglich des zu sanktionierenden Verhaltens sein. Viele Aufsichtsbehörden, auch die, der zwei Autoren dieses Buches angehören, haben wiederholt darauf hingewiesen, dass die Verantwortlichen oder Auftragsverarbeiter, die sich um Themen der DS-GVO gar nicht kümmern (und erwischt werden), sofort mit Sanktionen zu rechnen haben, während bei denjenigen, die sich um Compliance bemühen, Sanktionen nur im Extremfall zur Diskussion stehen.

Möge diese Handlungshilfe auch als Prävention für „unnötige" Sanktionen dienen.

Ansbach, Hamburg im September 2019

Die Autoren

Vorwort der Autoren zur 1. Auflage

Datenschutz-Compliance nach der Datenschutz-Grundverordnung (DS-GVO), d.h. ein an den gesetzlichen Vorgaben orientiertes Verhalten, ist schwer zu definieren und deshalb auch schwer zu erreichen. Wissenschaft und Aufsichtsbehörden kommentieren und definieren in großem Umfang, was Recht ist, bis zu gegebener Zeit die Gerichte und hier insbesondere der Europäische Gerichtshof in Luxemburg entscheiden, was wirklich Recht ist. Unternehmen und Dienstleister, in der Datenschutzsprache: Verantwortliche und Auftragsverarbeiter, die heute mit personenbezogenen Daten umgehen, können aber nicht warten, bis sämtliche Unklarheiten des neuen Rechts beseitigt sind, sondern müssen handeln.

Verantwortlichen und Auftragsverarbeitern ist dabei dringend zu empfehlen, sich mit den neuen datenschutzrechtlichen Anforderungen vertraut zu machen und zu versuchen, zu verstehen, welche Anforderungen sich für sie daraus ergeben könnten. Dies gilt unabhängig davon, ob sie der Wunsch nach Compliance, der vorbeugende Grundrechtsschutz für die Betroffenen oder auch nur das Vermeiden relevanter Bußgeldzahlungen und Reputationsverlust dazu veranlasst. Wichtig ist deshalb für Verantwortliche und Auftragsverarbeiter, sich darüber klar zu werden, was sie tun müssen, selbst wenn es noch etwas dauern kann, bis sie wissen, wie sie ihre Compliance erreichen.

Wir Autoren dieses Buches, die wir aus der unmittelbaren Aufsichtspraxis und der prozessorientierten Beratungsbranche stammen, versuchen mit diesem Buch allen Anwendern der DS-GVO Orientierung auf dem steinigen Weg zur Datenschutz-Compliance zu geben. Aufgeteilt in die drei großen Bereiche der allgemeinen Fragen der Datenverarbeitung, der Sicherstellung der Betroffenenrechte und der Handhabung von Datenschutzverletzungen werden für die immer wiederkehrenden Schritte der Planung, Betrieb, Bewertung und Verbesserung (Plan-Do-Check-Act – PDCA) mit Gliederungsvorschlägen, Checklisten und Prüffragebogen Hilfen für die tägliche Praxis angeboten.

Für die in dem Buch vorgeschlagenen Prozesse wird wiederholt auf ISO-Normen Bezug genommen. Die Ausrichtung der Abläufe in den Unternehmen an diesen ISO-Normen garantiert nicht die Einhaltung der Vorgaben der DS-GVO, aber für den Weg der Einhaltung der DS-GVO kann die Orientierung an ISO-Normen, die zur Einhaltung sonstiger Unternehmensziele (z.B. Qualitätsmanagement, Informationssicherheit, Compliance) schon im Einsatz sind, eine hilfreiche Unterstützung bieten.

Uns ist bewusst, dass die Veröffentlichung eines Buches zum Thema Compliance nach der DS-GVO zu einem Zeitpunkt, der etwa in der Mitte zwischen Inkrafttreten und Wirksamkeit der Norm liegt, d.h. zu einem Zeitpunkt, zu dem es noch keine praktischen Erfahrungen, keine Leitlinien des europäischen Datenschutzausschusses und auch keine einschlägige Rechtsprechung gibt, insofern etwas schwierig ist, weil sich viele derzeit von allen Seiten an den Text der DS-GVO herantasten und sich um das richtige Verständnis bemühen. Dieser Situation trägt das Buch dadurch Rechnung, dass es sich bezüglich der Anforderungen für Verantwortliche und Auftragsverarbeiter eng an den gesetzlichen Normen orientiert. Schwerpunkt der Darstellung ist jedoch die Beschreibung von Verfahren, die bei Verarbeitern, die mit personenbezogenen Daten umgehen, implementiert werden sollten. Die

Einhaltung der vielfältigen Datenschutzvorschriften, die Verzahnung des Datenschutzes in die Unternehmenskultur und ein datenschutzkonformer Umgang mit einer stark an Bedeutung zunehmender Digitalisierung wird zukünftig noch stärker davon abhängig sein, dass die Verantwortlichen in der Lage sind, die unterschiedlichen dafür notwendigen Disziplinen und Ressourcen (vor allem Juristen, Informatiker und Betriebswirte) „*an einen Tisch zu bekommen*", um sich gemeinsam der Herausforderung Datenschutz zu stellen. Dabei handelt es sich aber nicht um eine einmalige „Übung", sondern um einen dauerhaften und den sich ständig verändernden Umständen anpassenden Prozess. Hierfür hat der Verantwortliche die geeigneten Bedingungen zu schaffen. Dieses Vorgehen (PDCA) ermöglicht es, bei einer Veränderung des Verständnisses der materiell-rechtlichen Datenschutzvorschriften unverzüglich zu reagieren und damit auf dem oben beschriebenen Weg zur Datenschutz-Compliance zu bleiben oder wieder auf diesen zurückzukehren.

Die Autoren sind dankbar für Anmerkungen, Anregungen und konstruktive Kritik an folgende E-Mail-Adresse: feedback@datenschutz-compliance-buch.de. Gerne greifen wir diese in der nächsten Auflage auf.

Ansbach, München im März 2017

Die Autoren

Inhaltsübersicht

Teil I: Einführung in die DS-GVO

Teil II: Sicherstellung der Datenschutz-Compliance

Teil III: Überwachung der Datenschutz-Compliance

Inhaltsverzeichnis

Teil III:
Überwachung der Datenschutz-Compliance

Abkürzungsverzeichnis

Abl.	Amtsblatt
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AFNOR	Association Française de Normalisation (französische Stelle für Normung)
AICPA	American Institute of Certified Public Accountants (US-amerikanisches Institut der Wirtschaftsprüfer)
AktG	Aktiengesetz
Art.	Artikel
AV	Auftragsverarbeiter
AZ	Aktenzeichen
BayLDA	Bayerisches Landesamt für Datenschutzaufsicht
BayMG	Bayerisches Mediengesetz
BayRG	Bayerisches Rundfunkgesetz
BB	Der Betriebs-Berater (Zeitschrift)
BCR	Binding Corporate Rules (Verbindliche Unternehmensregeln)
BDSG	Bundesdatenschutzgesetz
Beschl.	Beschluss
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BSI	British Standard Institut oder Bundesamt für Sicherheit in der Informationstechnik
BvD	Berufsverband der Datenschutzbeauftragten
BVerG	Bundesvergabegesetz
BvL	Bundesamt für Verbraucherschutz und Lebensmittelsicherheit
bspw.	beispielsweise
bzw.	beziehungsweise
CAPA	Corrective And Preventive Action (Korrektive und präventive Maßnahme)
CB	Circumstances of Breach (Umstände der Datenschutzverletzung)
CEN	Europäisches Kommitee für Normung
CENELEC	Europäisches Komitee für elektronische Normung
CICA	Canadian Institute of Chartered Accountants (kanadisches Institut der Wirtschaftsprüfer)
CMS	Compliance-Management-System
CNIL	Commission Nationale de l'Informatique et des Libertés (deutsch: Nationale Kommission für Informatik und Freiheit; französische Datenschutzbehörde)
COBIT	Control Objectives for Information and Related Technology
CoC	Code of Conduct (Verhaltensregeln)
CoP	Code of Practices (Verhaltensregeln)
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRM	Client-Relationship-Management
d.h.	das heißt

Abkürzungsverzeichnis

DAkkS	Deutsche Akkreditierungsstelle
DIN	Deutsches Institut für Normung e.V.
DIS	Draft International Standard, ein ISO-Normentwurf
DMS	Dokumentenmanagementsystem
DPC	Data Processing Context (Kontext der Verarbeitung)
DS	Datenschutz
DS-GVO	Datenschutz-Grundverordnung
DSAnpUG	Datenschutz-Anpassungs- und -Umsetzungsgesetz
DSB	Datenschutzbeauftragter
DSFA	Datenschutz-Folgenabschätzung
DSK	Datenschutzkonferenz
DSMS	Datenschutz-Managementsystem
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DGQ	Deutsche Gesellschaft für Qualität e.V.
EDSA	Europäischer Datenschutzausschuss
EI	Ease of Identification (Leichtigkeit der Identifizierbarkeit)
Einf.	Einführung
ErwGr.	Erwägungsgrund
etc.	et cetera
EN	Europäische Norm
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
FDIS	Final Draft International Standard, Schlussentwurf für einen ISO-Standard
ff.	folgende
GDD	Gesellschaft für Datenschutz und Datensicherheit e.V.
ggf.	gegebenenfalls
GmbHG	Gesetz über Gesellschaften mit beschränkter Haftung
GRC	Governance, Risk und Compliance
Hrsg.	Herausgeber
i.d.R.	in der Regel
i.V.m.	in Verbindung mit
IACA	International Association of Consulting Actuaries
IAPP	International Association of Privacy Professionals
ICO	Information Commissioner's Office (britische Datenschutzbehörde)
IDW	Institut der Wirtschaftsprüfer
IEC	International Electrotechnical Commission (Internationale elektronische Kommission)
IKS	Internes Kontrollsystem
IMI	Internal Market Information System (Binnenmarkt-Informationssystem)
IMS	Integriertes Managementsystem
insb.	insbesondere
IoT	Internet of Things

ISMS	Informationssicherheitsmanagementsystem
ISO	Internationale Organisation für Normung
IT	Informationstechnologie
ITIL	IT Infrastructure Library
KMU	Kleinere und Mittlere Unternehmen
LDI	Landesbeauftrage für Datenschutz und Informationsfreiheit
lfd.	laufend
lit.	Littera = Buchstabe
Mio.	Million
MS	Managementsystem
NIST	National Institute of Standards and Technology
Nr.	Nummer
NWIP	New Work Item Proposal, ISO-Normenantrag
OECD	Organisation for Economic Co-operation and Development
OPC	Office of the Privacy Commissioner of Canada (kanadische Datenschutzbehörde)
OWiG	Gesetz über Ordnungswidrigkeiten
pbD	personenbezogene Daten
PCI DSS	Payment Card Industry Data Security Standard
PDCA	Plan-Do-Check-Act
PET	Privacy Enhancing Technologies
PH	Prüfungshinweis
PIA	Privacy impact assessment
PIAF	Privacy Impact Assessment Framework (von der Europäischen Kommission teilfinanziertes Projekt)
PII	Personal identifiable information
PS	Prüfungsstandard
QM	Qualitätsmanagement
QMS	Qualitätsmanagementsystem
RDV	Recht der Datenverarbeitung (Zeitschrift)
rev.	revised (überarbeitet)
RL	Richtlinie
RMS	Risikomanagementsystem
Rn.	Randnummer
S.	Seite
s.	siehe
s.a.	siehe auch
SDM	Standard-Datenschutzmodell
SE	Severity Level (Ausmaß der Schwere)
sog.	sogenannte
TKG	Telekommunikationsgesetz

Abkürzungsverzeichnis

TMG	Telemediengesetz
TOM	Technische und organisatorische Maßnahmen
u.a.	unter anderem
u.U.	unter Umständen
ULD	Unabhängiges Landeszentrum für Datenschutz
UMS	Umweltmanagementsystem
Urt.	Urteil
US	United States, Vereinigte Staaten
USA	United States of America
v.	von
vgl.	vergleiche
vs.	versus
VwGO	Verwaltungsgerichtsordnung
WG	Working Group
WP	Working Paper
z.B.	zum Beispiel
ZASt	Zentrale Anlaufstelle
ZD	Zeitschrift für Datenschutz (Zeitschrift)
Ziff.	Ziffer
z.T.	zum Teil

Teil I:

Einführung in die DS-GVO