Rechtsrahmen der Cybersicherheit und Privatheit

Reihe herausgegeben von

Annika Selzer, ATHENE, Fraunhofer-Institut für Sichere Informationstechnologie, Darmstadt, Deutschland

In dieser Reihe erscheinen Konferenzbände, Herausgeberwerke und Dissertationen des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE im Themenschwerpunkt „Rechtsrahmen der Cybersicherheit und Privatheit“.

Annika Selzer

Die technisch-organisatorische Implementierung von Datenschutz in Organisationen unter besonderer Berücksichtigung der wirtschaftlichen Angemessenheit

Springer Vieweg

Annika Selzer
Fraunhofer SIT | ATHENE
Darmstadt, Deutschland

Vom Fachbereich IV der Universität Trier zur Verleihung des akademischen Grades Doktorin der Naturwissenschaften (Dr. rer. nat.) genehmigte Dissertation. Datum der Disputation: 29.10.2025

ISSN 3059-4243 ISSN 3059-4251 (electronic)
Rechtsrahmen der Cybersicherheit und Privatheit
ISBN 978-3-658-50743-5 ISBN 978-3-658-50744-2 (eBook)
https://doi.org/10.1007/978-3-658-50744-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://portal.dnb.de abrufbar.

Die vorliegende Arbeit wurde vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Planung/Lektorat: Karina Kowatsch
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Zusammenfassung

Kaum eine Organisation kommt heutzutage ohne die Verarbeitung großer Mengen personenbezogener Daten in Informationssystemen aus, so dass sie sich konsequenterweise mit der Umsetzung datenschutzrechtlicher Anforderungen befassen müssen. Einerseits sollen die Regelungen der DSGVO dafür Sorge tragen, natürliche Personen vor Eingriffen in ihre Persönlichkeitsrechte zu schützen, die im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten stehen. Andererseits ist die Umsetzung der einschlägigen Datenschutzvorschriften häufig mit sehr hohen Kosten verbunden, während das Datenschutzrecht zusätzlich häufig als Hemmschuh für innovative Datennutzungsmöglichkeiten wahrgenommen wird. Vor diesem Hintergrund wünschen sich Organisationen einen pragmatischen Umgang mit der Umsetzung datenschutzrechtlicher Anforderungen, sind aber unsicher, wie viel Pragmatik die Umsetzung der DSGVO-Anforderungen erlaubt, ohne dem Risiko des hohen Bußgeldrahmens der DSGVO ausgesetzt zu sein.

Vor diesem Hintergrund beantwortet die vorliegende Arbeit aus der Perspektive der Wirtschaftsinformatik und Rechtswissenschaften offene Fragen zur angemessenen Umsetzung der DSGVO-Anforderungen, insbesondere im Bereich des technisch-organisatorischen Datenschutzes. Sie unterstützt insbesondere den in Organisationen umzusetzenden schwierigen Abwägungsprozess von Risiken für die Rechte und Freiheiten der von einer Datenverarbeitung betroffenen Personen (einerseits) und Implementierungskosten von dem Stand der Technik entsprechenden technischen und organisatorischen Maßnahmen (andererseits). Aus den daraus gewonnenen Erkenntnissen leitet die Arbeit wiederum u. a.

organisatorische, technische und rechtliche Schritte zur systematischen Umsetzung des Datenschutzes in Organisationen ab. Die einzelnen organisatorischen, technischen und rechtlichen Schritte werden in dieser Arbeit so aufbereitet, dass sie Wirtschaftsinformatiker in Organisationen zukünftig dabei unterstützen, bereits in der Planungs- und Implementierungsphase neuer IT-Systeme die angemessene Umsetzung datenschutzrechtlicher Anforderungen und die angemessene Datennutzung einplanen und beachten zu können.

Der im Rahmen dieser Arbeit entwickelte Vorschlag für die datenschutzkonforme Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen wurde abschließend im Rahmen von Evaluationsworkshops vorgestellt und erfolgreich evaluiert. An den Evaluationsworkshops nahmen u. a. potenzielle Anwender des Gestaltungsvorschlags, betriebliche Datenschutz- und IT-Sicherheitsbeauftragte sowie Mitarbeiter einer deutschen Datenschutzaufsichtsbehörde teil.

Wissenschaftlicher Werdegang der Doktorandin

2020	Promotion zum Dr. iur. an der Universität Bremen
Seit 2011	Rechtswissenschaftlerin am Fraunhofer-Institut für Sichere Informationstechnologie
2010	Auslandsaufenthalt
2006–2009	Studium des Informationsrechts an der Hochschule Darmstadt, Abschluss: Diplom Informationsjuristin (FH)

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abb.	Abbildung
Abs.	Absatz
AES	Advanced Encryption Standard (englisch für „fortgeschrittener Verschlüsselungsstandard“, Verschlüsselungsverfahren)
AK	Arbeitskreis
Alt.	Alternative
App	Applikation (englisch für „Anwendung“ bzw. „Anwendungssoftware“)
ArbG	Arbeitsgericht
Art.	Artikel
Az.	Aktenzeichen
BAföG	(Förderung nach) Bundesausbildungsförderungsgesetz
BDSG	Bundesdatenschutzgesetz
BDSG a. F.	Bundesdatenschutzgesetz, bis 24. Mai 2018
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGH	Bundesgerichtshof
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BSI	Bundesamt für Sicherheit in der Informationstechnik
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
CA	Certification authority (englisch für „Zertifizierungsstelle“)

CD	Compact Disk (englisch für „kompakte Scheibe“, Speichermedium)
DAkkS	Deutsche Akkreditierungsstelle
DoS	Denial of Service (englisch für „Verweigerung des Dienstes“)
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (auch kurz „Datenschutzkonferenz“ genannt)
DSRITB	Tagungsband der Deutschen Stiftung für Recht und Informatik
DSRL	Datenschutz-Richtlinie
DStR	Das deutsche Steuerrecht (Zeitschrift)
DuD	Zeitschrift für Datenschutz und Datensicherheit
e. V.	Eingetragener Verein
Ebd.	Ebenda
EDPL	European Data Protection Law Review (Zeitschrift)
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EG	Europäische Gemeinschaft
EK	Einmalige Kosten
E-Mail	Electronic Mail (englisch für „elektronische Post“)
ENISA	Agentur der Europäischen Union für Cybersicherheit
Erwgr.	Erwägungsgrund
et al.	Et Alia
etc.	Et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuR	Europarecht (Zeitschrift)
EuV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (Zeitschrift)
Fax	Telefax/Fernkopie
Fn.	Fußnote
gem.	Gemäß
Ggf.	Gegebenenfalls
GRCh	Charta der Grundrechte der EU
HICSS	Hawaii International Conference on System Sciences
Hinweisbes.	Hinweisbeschluss
Hrsg.	Herausgeber
HS	Halbsatz
I. d. R.	In der Regel

I. S. d.	Im Sinne des
I. V. m.	In Verbindung mit
ICECC	International Conference on Electronics, Communications and Control
IDS	Intrusion Detection System
IGel	Individuelle Gesundheitsleistungen
IT	Informationstechnologie
JuS	Juristische Schulung (Zeitschrift)
Kap.	Kapitel
LAG	Landesarbeitsgericht
LG	Landgericht
Lit	Littera, Buchstabe
MMR	Multimedia und Recht (Zeitschrift)
NIST	National Institute of Standards and Technology (englisch für „nationales Institut für Standards und Technologie“ in den USA)
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NR.	Nummer
O. g.	Oben genannt(e/n)
OLG	Oberlandesgericht
ÖOGH	Der Oberste Gerichtshof Österreich
P. a.	Per annum (lateinisch für „jährlich“)
PIN	Personal Identification Number (englisch für „persönliche Identifikationsnummer“)
PKI	Public Key Infrastructure (englisch für „Public-Key Infrastruktur“)
Rdnr.	Randnummer
RL	Richtlinie
S.	Seite / Siehe
SDM	Standard-Datenschutzmodell
TeleTrusT	Bundesverband IT-Sicherheit e. V.
TISSEC	Transactions on Information and System Security (Journal)
TLS	Transport Layer Security (englisch für „Transportschichtsicherheit“)
U. A.	Unter anderen/unter anderem
Urt.	Urteil
USA	United States of America (englisch für „Vereinigte Staaten von Amerika“)
USB	Universal Serial Bus
usw.	Und so weiter

V.	Von (dem)
Vgl.	Vergleiche
VO	Verordnung
VPN	Virtual Private Network (englisch für „virtuelles privates Netzwerk“)
WEIS	Workshop on the Economics of Information Security
WK	Wiederkehrende Kosten
WWW	World Wide Web (englisch für „weltweites Netz“)
z. B.	Zum Beispiel
ZD	Zeitschrift für Datenschutz
ZfDR	Zeitschrift für Digitalisierung und Recht
zw.	zwischen

Abbildungsverzeichnis

Gliederungsillustration

Tabellenverzeichnis