
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

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.

© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert an Springer Fachmedien
Wiesbaden GmbH, ein Teil von Springer Nature 2026

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen. Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jede Person benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des/der jeweiligen Zeicheninhaber*in sind zu beachten. Der Verlag, die Autor*innen und die Herausgeber*innen gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autor*innen oder die Herausgeber*innen übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

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

Wenn Sie dieses Produkt entsorgen, geben Sie das Papier bitte zum Recycling.

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

Teil I Hintergrund der Arbeit

1	Einleitung	3
1.1	Gegenstand der Untersuchung	7
1.2	Beitrag der Arbeit	8
1.3	Hintergrund und Forschungsmethodik der Arbeit	10

Teil II Angemessene Schutzmaßnahmen

2	Technische und organisatorische Maßnahmen gemäß Datenschutz-Grundverordnung	19
2.1	Grundsätze für die Verarbeitung personenbezogener Daten	22
2.1.1	Adressat der Verpflichtungen	23
2.1.2	Relevante Regelungen im Überblick	24
2.1.3	Bußgelder bei Verstößen	29
2.2	Verantwortung des für die Verarbeitung Verantwortlichen	30
2.2.1	Adressat der Verpflichtungen	32
2.2.2	Relevante Regelungen im Überblick	32
2.2.3	Bußgelder bei Verstößen	40
2.3	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen	41
2.3.1	Adressat der Verpflichtungen	42
2.3.2	Relevante Regelungen im Überblick	44
2.3.3	Bußgelder bei Verstößen	49

2.4	Sicherheit der Verarbeitung	50
2.4.1	Adressat der Verpflichtungen	51
2.4.2	Relevante Regelungen im Überblick	52
2.4.3	Bußgelder bei Verstößen	71
2.5	Ergebnis	72
3	Auswahlkriterien zur Umsetzung technischer und organisatorischer Maßnahmen	75
3.1	Angemessenheit gem. Art. 24 Abs. 1, 25 Abs. 1 und 32 Abs. 1 DSGVO	77
3.1.1	Kriterium: Stand der Technik	78
3.1.2	Kriterium: Implementierungskosten	82
3.1.3	Kriterium: Art, Umfang, Umstände und Zwecke der Verarbeitung	88
3.1.4	Kriterium: Schwere und Eintrittswahrscheinlichkeit von Risiken	93
3.2	Weitere Konkretisierungen zur Angemessenheit	98
3.2.1	Angemessenheit gem. Art. 32 Abs. 2 DSGVO	98
3.2.2	Angemessenheit gem. Art. 24 Abs. 2 DSGVO	102
3.3	Ergebnis	102
4	Implementierungskosten als wirtschaftlicher Faktor der Angemessenheitsbewertung	105
4.1	Regelungshintergrund	106
4.1.1	Historische Entwicklung	106
4.1.2	Verhältnismäßigkeitsprinzip	109
4.2	Angemessenheit aus datenschutzrechtlicher, technischer und wirtschaftlicher Sicht	111
4.2.1	Angemessenheit aus datenschutzrechtlicher Sicht	112
4.2.2	Angemessenheit aus technischer Sicht	113
4.2.3	Angemessenheit aus betriebswirtschaftlicher Sicht	120
4.2.4	Empfehlungen des EDSB	122
4.2.5	Datenschutz-Folgenabschätzung	128
4.2.6	Standard-Datenschutzmodell der Datenschutzkonferenz	133
4.2.7	Chancen und Grenzen bestehender Instrumente	137
4.3	Ergebnis	139

5	Quantifizierung der Implementierungskosten	143
5.1	Methodisches Vorgehen	144
5.1.1	Vorbereitung der Interviews	144
5.1.2	Strukturierte Interviews	148
5.2	Quantifizierung der Implementierungskosten von dem Stand der Technik entsprechender technischer und organisatorischer Maßnahmen	152
5.2.1	Validierungsgrad der Implementierungskosten	156
5.2.2	Implementierungskosten unter Berücksichtigung des Verarbeitungsrisikos	158
5.2.3	Implementierungskosten je Mitarbeiter unterschiedlicher Kostengruppengrößen	159
5.2.4	Zusammenhang zwischen der Organisationsgröße und der Umsetzung von Maßnahmen	161
5.2.5	Konfidenz und Verallgemeinerbarkeit	162
5.2.6	Einschränkungen der Datenerhebung und -auswertung	163
5.3	Ergebnis	163
6	Zwischenergebnis	167
 Teil III Angemessene Datennutzung unter Umsetzung angemessener Schutzmaßnahmen		
7	Chancen und Grenzen personenbezogener Datenverarbeitung in Smart Cities aus Sicht des Verantwortlichen	175
7.1	Methodisches Vorgehen	176
7.2	Relevante Vorarbeiten	178
7.3	Personenbezogene und anonyme Datenverarbeitung in Smart Cities	179
7.4	Konfidenz und Verallgemeinerbarkeit	183
7.5	Ergebnis	183
7.5.1	Ergebnisse der Umfragen	184
7.5.2	Ableitung des exemplarischen Datenverarbeitungsszenarios und -systems	184

8	(Weitere) Rechtliche Grundlagen zur Gestaltung von Datenverarbeitungssystemen	197
8.1	Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	198
8.2	Zweckbindung	200
8.3	Datenminimierung	201
8.4	Richtigkeit	202
8.5	Speicherbegrenzung	203
8.6	Ergebnis	204
9	Exemplarische Umsetzung angemessener Schutzmaßnahmen	205
9.1	Gestaltung der Umsetzung des technisch-organisatorischen Datenschutzes im Datenverarbeitungssystem	209
9.1.1	Gestaltung des Rollenkonzepts	209
9.1.2	Gestaltung der Umsetzung des Datenschutz-Grundsatzes der Vertraulichkeit und Integrität	219
9.1.3	Gestaltung der Umsetzung der weiteren Datenschutz-Grundsätze im Datenverarbeitungssystem	232
9.2	Evaluation der Gestaltung des Datenschutzes im System	237
9.2.1	Methodisches Vorgehen	237
9.2.2	Evaluation der Geeignetheit des vorgeschlagenen Systems zur Problemlösung der Smart-City-Akteure	239
9.2.3	Evaluation der Einstufung in die drei Schutzbedarfsbereiche	240
9.2.4	Evaluation der Gestaltung der Vertraulichkeit und Integrität	240
9.2.5	Evaluation der Angemessenheit der Maßnahmen zur Vertraulichkeit und Integrität	241
9.2.6	Evaluation der Gestaltung der weiteren Datenschutz-Grundsätze	241
9.2.7	Konfidenz	242
9.3	Ergebnis	242
10	Zwischenergebnis	245

Teil IV Zusammenfassende Strukturierung

11 Vorschlag für die datenschutzkonforme Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen	249
11.1 Rahmenbedingungen	250
11.2 Rollen möglicher Beteiligter	251
11.3 Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen	252
11.3.1 Schritt 1: Entscheidung über die personenbezogene oder anonyme Datenverarbeitung	253
11.3.2 Schritt 2: Vorabentscheidung über die grundsätzliche Machbarkeit	256
11.3.3 Schritt 3: Planung der Umsetzung der allgemeinen Grundsätze des Datenschutzrechts	256
11.3.4 Schritt 4: Planung geeigneter und angemessener technischer und organisatorischer Schutzmaßnahmen	256
11.4 Evaluation des Vorschlags	266
11.4.1 Methodisches Vorgehen	266
11.4.2 Evaluation der Vollständigkeit der Anforderungen und Teilaufgaben	268
11.4.3 Evaluation der vorgeschlagenen personellen Verantwortlichkeiten und sonstigen Beteiligungen	269
11.4.4 Evaluation des Zeitplans	270
11.4.5 Sonstige Rückmeldungen	270
11.4.6 Konfidenz	271
11.5 Ergebnis	272
12 Zwischenergebnis	273

Teil V Gesamtergebnis

13 Angemessenheit im technisch-organisatorischen Datenschutz: Gesamtergebnis	277
13.1 Grenzen der Arbeit	278
13.1.1 Rechtsdogmatische Erkenntnisse	278
13.1.2 Empirische Erkenntnisse	279

13.2	Umsetzungspflicht angemessener technischer und organisatorischer Maßnahmen	280
13.3	Angemessene Umsetzung am Beispiel eines exemplarischen Datenverarbeitungssystems	282
13.4	Vorschlag für die datenschutzkonforme Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen	283
13.5	Ausblick	284
Literaturverzeichnis		285

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

Abbildung 2.1	TOMs als Überschneidung des Datenschutzes und der Datensicherheit	20
Abbildung 2.2	Umsetzungsbeispiel einer Pseudonymisierung	55
Abbildung 2.3	Varianten der Datensicherung	65
Abbildung 3.1	Abgrenzung von Technologieständen	81
Abbildung 3.2	Risikomatrix der Datenschutzkonferenz	97
Abbildung 4.1	Abwägung von Sicherheit und Benutzbarkeit	115
Abbildung 4.2	Abwägung von Sicherheit und Komplexität	116
Abbildung 4.3	Abwägung von Sicherheit und Kosten	117
Abbildung 4.4	Abwägung von Sicherheit und Aufwand	118
Abbildung 7.1	Regelfall der exemplarischen Datenverarbeitung	191
Abbildung 7.2	Ausnahmefall der exemplarischen Datenverarbeitung	192
Abbildung 7.3	Trennung der personenbezogenen und anonymen Datenverarbeitung im exemplarischen Datenverarbeitungssystem	193
Abbildung 9.1	Modell des Informationsmanagements	207
Abbildung 9.2	Abgestufter Schutzbedarf im exemplarischen Datenverarbeitungssystem	220
Abbildung 11.1	Schritte zur Umsetzung des Datenschutzrechts bei der Planung neuer IT-Systeme	253

Gliederungsillustration

Gliederungsillustration 2.1	Frage Kapitel 2	19
Gliederungsillustration 2.2	Antwort Kapitel 2	73
Gliederungsillustration 3.1	Frage Kapitel 3	75
Gliederungsillustration 3.2	Antwort Kapitel 3	104
Gliederungsillustration 4.1	Frage Kapitel 4	105
Gliederungsillustration 4.2	Antwort Kapitel 4	142
Gliederungsillustration 5.1	Frage Kapitel 5	143
Gliederungsillustration 5.2	Antwort Kapitel 5	165
Gliederungsillustration 7.1	Frage Kapitel 7	175
Gliederungsillustration 7.2	Antwort Kapitel 7	196
Gliederungsillustration 8.1	Frage Kapitel 8	197
Gliederungsillustration 8.2	Antwort Kapitel 8	204
Gliederungsillustration 9.1	Frage Kapitel 9	205
Gliederungsillustration 9.2	Antwort Kapitel 9	243
Gliederungsillustration 11.1	Frage Kapitel 11	249
Gliederungsillustration 11.2	Antwort Kapitel 11	272

Tabellenverzeichnis

Tabelle 1.1	Dokumentation der Literaturrecherche	13
Tabelle 4.1	Datenschutzfolgenabschätzung: Positiv- und Negativliste	129
Tabelle 5.1	Rahmenbedingungen der Interviews zur initialen Kostenerhebung	148
Tabelle 5.2	Rahmenbedingungen der Interviews zur Kostenvalidierung	151
Tabelle 5.3	Kosten für exemplarische technische Maßnahmen	153
Tabelle 5.4	Kosten für exemplarische organisatorische Maßnahmen	154
Tabelle 5.5	Kosten für exemplarische technisch-organisatorische Maßnahmen	155
Tabelle 5.6	Zusammenfassende Darstellung der Quantifizierung von Implementierungskosten	164
Tabelle 7.1	Rahmenbedingungen der Interviews zu Chancen und Risiken der Datenverarbeitung	178
Tabelle 9.1	Berechtigungen der Rollen des exemplarischen Datenverarbeitungssystems	218
Tabelle 9.2	Rahmenbedingungen der Evaluationsworkshops (1)	239
Tabelle 11.1	Entscheidung über die personenbezogene oder anonyme Datenverarbeitung	254
Tabelle 11.2	Vorprüfung der Machbarkeit	257
Tabelle 11.3	Planung der Umsetzung der allgemeinen Grundsätze des Datenschutzrechts	258

Tabelle 11.4	Planung geeigneter & angemessener technischer und organisatorischer Schutzmaßnahmen	264
Tabelle 11.5	Rahmenbedingungen der Evaluationsworkshops (2)	268