

Christoph Werner

Die Resilienz als neue Anforderung des Rechts der Daten- und IT-Sicherheit

Eine Untersuchung anhand der exemplarischen Betrachtung
kritischer, personalisierter Dienste



Nomos

Schriften zum IT-Sicherheitsrecht

Herausgegeben von

Prof. Dr. Gerrit Hornung

Prof. Dr. Ralf Poscher

MinDir a.D. Martin Schallbruch

Prof. Dr. Tobias Singelnstein

Prof. Dr. Gerald Spindler

Prof. Dr. Louisa Specht-Riemenschneider

Prof. Dr. Indra Spiecker gen. Döhmann

Band 4

Christoph Werner

Die Resilienz als neue Anforderung des Rechts der Daten- und IT-Sicherheit

Eine Untersuchung anhand der exemplarischen Betrachtung
kritischer, personalisierter Dienste



Nomos

Dissertation an der rechtswissenschaftlichen Fakultät
der Albert-Ludwigs-Universität Freiburg

Dekan: Prof. Dr. Jan Lieder, LL.M. (Harvard)
Erstgutachter: Prof. Dr. Thomas Dreier, M.C.J.
Zweitgutachter: Prof. Dr. Jens-Peter Schneider
Mündliche Prüfung: 08.-09.07.2024
Dissertationsort: Freiburg im Breisgau
Erscheinungsjahr: 2025

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

Zugl.: Freiburg im Breisgau, Univ., Diss., 2024

1. Auflage 2025

© Christoph Werner

Publiziert von

Nomos Verlagsgesellschaft mbH & Co. KG
Walzseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:

Nomos Verlagsgesellschaft mbH & Co. KG
Walzseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-7560-0144-6

ISBN (ePDF): 978-3-7489-4752-3

DOI: <https://doi.org/10.5771/9783748947523>



Onlineversion
Nomos eLibrary



Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung
4.0 International Lizenz.

Für Leonie und Henri

Vorwort

Diese Untersuchung zur Resilienz im Recht der Daten- und IT-Sicherheit entstand in einer Zeit großen Wandels nicht zuletzt auch in der digitalen Entwicklung. Eine tendenziell zunehmend kritische Lage in der Daten- und IT-Sicherheit, neue digitale Produkte wie KI-basierte Chatbots und Bildgenerierungswerzeuge sowie eine gesellschaftlich als auch rechtlich zunehmend bedenkliche öffentliche Diskursentfaltung in sozialen Medien sind nur einige Beispiele, die insbesondere den europäischen Gesetzgeber motivierten, eine Vielzahl von Gesetzen auf den Weg zu bringen, von denen auch einige in dieser Untersuchung Beachtung finden werden.

Am bedeutendsten für die hiesige Untersuchung ist dabei die NIS2-RL, deren nationale Umsetzung insbesondere in das BSIG zum Abschluss dieser Untersuchung leider noch im Stadium eines Regierungsentwurfs vom 22.07.2024 in Form eines Artikelgesetzes mit dem Titel NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) verharrt. Da die NIS2-RL und damit auch das künftige BSIG aber bis auf Weiteres die zentralen Rahmenwerke des IT-Sicherheitsrecht darstellen (werden), wird in dieser Untersuchung bereits die NIS2-RL und der Regierungsentwurf zum BSIG (RegE BSIG) zugrunde gelegt. Die zum Zeitpunkt der Veröffentlichung noch bestehende nationale Rechtslage wird aber gleichwohl einbezogen.

Bedanken möchte ich mich bei Prof. Dr. Oliver Raabe, der mit seinen stets hilfreichen und analytisch äußerst scharfsinnigen Gedanken die Entstehung dieser Dissertation bereichert hat, mir zugleich im Rahmen dieser großartigen Betreuung aber auch einen angenehmen Freiraum ließ. Hinsichtlich der zügigen und inhaltlich anregenden Begutachtung dieser Untersuchung gilt mein Dank Prof. Dr. Thomas Dreier und Prof. Dr. Jens-Peter Schneider.

Außerdem möchte ich mich bei den Kolleg:innen von ITSR.sys, KASTEL sowie der Forschungsgruppe ITR bedanken. Aus letzterer ist insbesondere unsere Sekretärin Sandra Schommer hervorzuheben, die mir stets nach besten Möglichkeiten alle „nicht-wissenschaftlichen“ Anliegen ferngehalten oder andernfalls zumindest mit allen Kräften bei der Bewältigung derselben unterstützt hat.

Vorwort

Schließlich möchte ich mich bei meiner lieben Lebensgefährtin und Kollegin Leonie Sterz bedanken, die mit ihrer liebe- und humorvollen sowie stets unterstützenden Art den erfolgreichen Abschluss dieser Dissertation in dieser Form erst ermöglicht hat. Und in diesem Zusammenhang ist natürlich unser gemeinsamer Sohn Henri nicht zu vergessen, der insbesondere noch bis zur Abgabe dieser Dissertation gewartet hat, bis er zu uns gekommen ist.

Rechtslage, Literatur und Rechtsprechung wurden bis zum 15.04.2024 berücksichtigt, lediglich die laufende Gesetzesentwicklung wurde insbesondere mit dem benannten Regierungsentwurf zum NIS2UmsuCG vom 22.07.2024 nachträglich eingearbeitet. Die Open-Access-Veröffentlichung wurde dankenswerterweise von den KASTEL Security Research Labs finanziell unterstützt.

Karlsruhe, November 2024

Christoph Werner

Inhaltsübersicht

Inhaltsverzeichnis	13
Abbildungsverzeichnis	21
Tabellenverzeichnis	23
Abkürzungsverzeichnis	25
1. Kapitel: Einleitung	29
A. Motivation	29
I. Digitale Entwicklung der Gesellschaft	30
II. Rechtliche Ausgangslage	36
III. Adressaten und Störungsszenario	41
IV. Übergreifende Bedeutung des Szenarios	44
V. Fazit	49
B. Untersuchungsgegenstand	50
C. Gang der Untersuchung	53
I. Funktionsweise und Manipulation von Personalisierungsalgorithmen	53
II. Resilienz in Art. 32 DSGVO	54
III. Übertragbarkeit in § 30 RegE BSIG	55
IV. Zusammenfassung und Gestaltungsempfehlung	56
2. Kapitel: Funktion und Manipulation der algorithmenbasierten Personalisierung	59
A. Ermittlung von Personenwissen nach dem DIW-Modell	59
I. Daten	60
II. (Persönliche) Information	61
III. Wissen	64
IV. Entscheidung und Verhaltenssteuerung	65
V. Zusammenfassung	67

Inhaltsübersicht

B. Technische Grundlagen	67
I. Automatisierte Verarbeitung	67
II. Autonome Verarbeitung durch maschinelles Lernen	68
III. Verarbeitung in personalisierten Dienstangeboten	69
C. Manipulation der Informationen	73
I. Allgemeine Darstellung	73
II. Singuläre Informationsmanipulation	74
III. Plurale Informationsmanipulation	77
IV. Fazit und Ansatz für das Erfordernis der Resilienz	78
3. Kapitel: Die Resilienz in der DSGVO	81
A. Anwendungsbereich von Art. 32 DSGVO	81
I. Normenübersicht	82
II. Verhältnis der Art. 25 Abs. 1, 32 DSGVO	87
B. Schutzgüter	101
I. Terminologie und normative Bedeutung	102
II. Die Schutzgüter der DSGVO	105
III. Bestimmung in Art. 32 DSGVO	109
C. Auslegung der Resilienz	110
I. Vorbegriffe	110
II. Auslegung nach dem Wortlaut	121
III. Systematische Auslegung	159
IV. Historische Auslegung	205
V. Teleologische Auslegung	208
VI. Ergebnis	212
D. Demonstration anhand personalisierter Dienste	215
I. Ungewissheit	215
II. Resilienzmaßnahmen	216
III. Abstrakte Angemessenheit	219
IV. Fazit	220

4. Kapitel: Übertragung in das IT-Sicherheitsrecht	221
A. Bestimmung der Schutzgüter	222
I. Historische Entwicklung des BSIG	222
II. Schutzgüter kritischer Anlagen	230
III. Schutzgüter digitaler Dienste	254
B. Systematische Beschreibung der gesetzlichen IT-Sicherheitsvorgaben	262
I. IT-Sicherheit und Schutzziele	263
II. Systeme, Dienste, Daten und Informationen	272
III. Risiko und Angemessenheit	289
IV. Zusammenfassung	296
C. Unterschiede zur DSGVO und Folgen für die Resilienz	297
I. IT-Sicherheit vs. Datensicherheit	298
II. Bedeutung der Schutzziele und des Dienstes	299
III. Verständnis des Systembegriffs	303
IV. Risiko	307
V. Zusammenfassung	311
D. Übertragung der Resilienz in den RegE BSIG	313
I. Bestehende, funktionale Resilienz-Elemente	313
II. Teleologische Gründe	316
III. Gesamtergebnis	317
E. Demonstration anhand des Szenarios	318
I. Ungewissheit	318
II. Resilienzmaßnahmen	319
III. Abstrakte Angemessenheit	321
5. Kapitel: Zusammenfassung und Implementierungsvorschlag	323
A. Zusammenfassung der Ergebnisse	323
I. Resilienz in der DSGVO	324
II. Übertragbarkeit in den RegE BSIG	328
B. Implementierungsvorschlag	333
C. Ausblick	335
Literaturverzeichnis	339

Inhaltsverzeichnis

Abbildungsverzeichnis	21
Tabellenverzeichnis	23
Abkürzungsverzeichnis	25
1. Kapitel: Einleitung	29
A. Motivation	29
I. Digitale Entwicklung der Gesellschaft	30
1. Die Welt der personenbezogenen Daten	30
2. Die kritischen Dienste der Gesellschaft	32
3. Zweifache Bedeutung digitaler Dienste	33
4. Technische Innovation in Ungewissheit	34
5. Fazit	35
II. Rechtliche Ausgangslage	36
1. Datensicherheitsrecht und IT-Sicherheitsrecht	37
2. Unterschiede beider Rechtsgebiete	38
3. Überschneidungsbereich	39
III. Adressaten und Störungsszenario	41
IV. Übergreifende Bedeutung des Szenarios	44
1. Energierecht	45
2. Gesundheitsversorgung	46
3. Dienste in digitalen Ökosystemen	46
4. Telekommunikationsrecht	48
V. Fazit	49
B. Untersuchungsgegenstand	50
C. Gang der Untersuchung	53
I. Funktionsweise und Manipulation von Personalisierungsalgorithmen	53
II. Resilienz in Art. 32 DSGVO	54
III. Übertragbarkeit in § 30 RegE BSIG	55
IV. Zusammenfassung und Gestaltungsempfehlung	56

Inhaltsverzeichnis

2. Kapitel: Funktion und Manipulation der algorithmenbasierten Personalisierung	59
A. Ermittlung von Personenwissen nach dem DIW-Modell	59
I. Daten	60
II. (Persönliche) Information	61
III. Wissen	64
IV. Entscheidung und Verhaltenssteuerung	65
V. Zusammenfassung	67
B. Technische Grundlagen	67
I. Automatisierte Verarbeitung	67
II. Autonome Verarbeitung durch maschinelles Lernen	68
III. Verarbeitung in personalisierten Dienstangeboten	69
C. Manipulation der Informationen	73
I. Allgemeine Darstellung	73
II. Singuläre Informationsmanipulation	74
1. Wirkung nach dem DIW-Modell	74
2. Technische Ausgestaltung	75
III. Plurale Informationsmanipulation	77
1. Wirkung nach dem Informationsmodell	77
2. Technische Gestaltung	77
IV. Fazit und Ansatz für das Erfordernis der Resilienz	78
3. Kapitel: Die Resilienz in der DSGVO	81
A. Anwendungsbereich von Art. 32 DSGVO	81
I. Normenübersicht	82
1. Dekomposition der einzelnen Normen	83
a. Art. 24 DSGVO	83
b. Art. 25 DSGVO	84
c. Art 32 Abs. 1 DSGVO	85
2. Tabellarische Übersicht	86
II. Verhältnis der Art. 25 Abs. 1, 32 DSGVO	87
1. Inhaltliche Unterschiede der Normen	88
a. Perspektiven	88
b. Umsetzung der Verarbeitung durch Systeme und Dienste	89
c. Rollenansprache	89

d. Voluntative Schutzrichtungen	90
i. Vertraulichkeit	90
ii. Verfügbarkeit/Integrität	92
2. Übergreifende Zuordnung in Erwägungsgrund 83	94
3. Normaufträge und Fazit	95
a. Keine eindeutige Differenzierung nach voluntativem Element und Quelle	95
b. Art. 25 Abs. 1 DSGVO	97
c. Art. 32 DSGVO	98
B. Schutzgüter	101
I. Terminologie und normative Bedeutung	102
II. Die Schutzgüter der DSGVO	105
1. Sachliche Bestimmung der „Grundrechte und Grundfreiheiten“	106
2. Kreis der geschützten „natürlichen Personen“	108
III. Bestimmung in Art. 32 DSGVO	109
C. Auslegung der Resilienz	110
I. Vorbegriffe	110
1. Datensicherheit / Sicherheit der Verarbeitung	111
2. Maßnahmen	112
3. Systeme	114
a. Erfassung personenbezogener Daten	115
b. Soziotechnisches Systemverständnis	117
4. Dienste	119
a. Ökonomische Betrachtung	119
b. Rechtliche Betrachtung	119
c. Technische Betrachtung	120
II. Auslegung nach dem Wortlaut	121
1. „Belastbarkeit“ oder Resilienz	121
2. Allgemeine Wortbedeutung und domänenspezifische Verwendung	124
a. Psychologie	126
b. Ökologie, Umwelt- und Klimaforschung	129
c. Technische Resilienz	132
i. Material- und Ingenieurwissenschaft	132
ii. Informationstechnik	133
(1) Verlässlichkeit	133

Inhaltsverzeichnis

(2) IT-Sicherheit	137
(3) Weitere Teilbereiche und Fazit	139
iii. Kritische Infrastrukturen	141
d. Gesellschaftliche Resilienz / Katastrophenschutz	142
e. IT-Sicherheitsrecht	145
i. Einführung	145
ii. RegE BSIG und NIS2-RL	147
iii. RefE KRITIS-DachG	148
iv. Digital Operational Resilience Act (DORA)	149
v. Cybersecurity-Act (CSA)	149
vi. Strategie zum Schutz kritischer Infrastrukturen (Schweiz)	150
vii. Strategic Plan 2023-2025 (USA)	151
viii. Fazit	152
3. Synthese	153
4. Fazit	158
III. Systematische Auslegung	159
1. Risiko	159
a. Einleitung	159
b. Begriffsdefinition	160
c. Methodik	163
i. Einleitung	163
ii. Identifizieren von Datenschutzrisiken	165
iii. Analysieren der Datenschutzrisiken	166
iv. Bewerten von Datenschutzrisiken	166
v. (Angemessene) Behandlung von Datenschutzrisiken	167
vi. Iteration	168
d. Gegenüberstellung der Resilienz	169
i. Resilienz als Umgang mit Ungewissheit	169
(1) Ungewissheit als (Un)bekanntheit und (Nicht)-Wissen	170
(2) Was ist unbekannt und worüber besteht kein Wissen?	176
(3) Resilienz als spezifische Antwort	178
(4) Folgen für die Risikodefinition	179

ii.	Methodische Einordnung	180
(1)	Adressierung unterschiedlicher Formen der Ungewissheit	181
(2)	Angemessenheit von Resilienzmaßnahmen	182
(3)	Resilienzlernen und Risikomanagement-Iteration	183
(4)	Zusammenfassung der Methodik	185
iii.	Ergebnis und Folgen für den Resilienzbegriff	185
2.	Schutzziele nach Art. 32 Abs. 1 lit b) DSGVO	187
a.	Historische Entwicklung	187
b.	Einführung im deutschen und europäischen Datenschutzrecht	189
c.	Vorkommen und Auslegung in der DSGVO	190
i.	Verfügbarkeit	192
ii.	Integrität	193
iii.	Vertraulichkeit	195
d.	Zusammenfassung	196
e.	Einordnung der Resilienz	198
3.	Systeme und Dienste	201
4.	Fazit	203
IV.	Historische Auslegung	205
1.	Vorgängervorschrift Art. 17 DS-RL	206
2.	Entwicklung der DSGVO	206
3.	Fazit	207
V.	Teleologische Auslegung	208
1.	Ungewissheit in komplexen, offenen Systemen	209
2.	KI als ungewisse Komponente	210
3.	Ermöglichung von Resilienz durch Komplexität und Autonomie	211
4.	Fazit	212
VI.	Ergebnis	212
D.	Demonstration anhand personalisierter Dienste	215
I.	Ungewissheit	215
II.	Resilienzmaßnahmen	216
1.	Ereigniserkennung	216
2.	Anpassungsfähigkeit	217
3.	Erholung	218
III.	Abstrakte Angemessenheit	219

Inhaltsverzeichnis

IV. Fazit	220
4. Kapitel: Übertragung in das IT-Sicherheitsrecht	221
A. Bestimmung der Schutzgüter	222
I. Historische Entwicklung des BSIG	222
1. Novelle 2015 – Schutz kritischer Infrastrukturen	224
2. Novelle 2017 – Schutz digitaler Dienste	225
3. Novelle 2021 – Unternehmen im besonderen öffentlichen Interesse	227
4. Novelle 2024 – NIS2-RL	228
5. Fazit	230
II. Schutzgüter kritischer Anlagen	230
1. Begriff der Daseinsvorsorge	230
a. Verfassungsrechtliche Pflichten zur Leistungsbereitstellung	235
i. Leistungsansprüche aus Grundrechten	235
ii. Grundrechtliche Schutzpflichten	237
iii. Gemeinwohlziele	238
iv. Sozialstaatsprinzip	242
v. Zwischenfazit	243
b. Originäre Wahrnehmung durch den Staat	244
c. Heutige Gewährleistungsverantwortung	247
d. Fazit	249
2. Öffentliche Sicherheit	250
3. Erhalt der Umwelt	251
4. Zusammenfassung	252
III. Schutzgüter digitaler Dienste	254
1. Individualrechtsgüter	256
a. Ausfälle des Dienstes	256
b. Manipulationen des Dienstes	256
c. Eingeschränkter Schutz von Individualrechtsgütern im IT-Sicherheitsrecht	257
2. Gemeinwohlziele und Sozialstaatsprinzip	259
3. Öffentliche Sicherheit	261
4. Fazit	261

B. Systematische Beschreibung der gesetzlichen IT-Sicherheitsvorgaben	262
I. IT-Sicherheit und Schutzziele	263
1. IT-Sicherheit	263
2. Verfügbarkeit, Vertraulichkeit und Integrität	269
3. Authentizität	271
II. Systeme, Dienste, Daten und Informationen	272
1. Systeme	272
a. Systeme, Komponenten und Prozesse	273
b. Netz- und Informationssysteme	274
i. Netzsystem	275
ii. Informationssystem	276
iii. Digitale Daten	276
c. Zusammenführung und soziotechnisches Verständnis	277
2. Dienste	279
a. Dienstbegriffe nach der NIS2-RL	279
i. Der ökonomische Dienst: Art. 21 Abs. 1 NIS2-RL	280
ii. Der IT-Dienst: Art. 6 Nr. 2 NIS2-RL	281
iii. Der IKT-Dienst und der digitale Dienst	282
b. Dienstverständnisse im RegE BSIG	283
i. Verständnis des nationalen Gesetzgebers	283
ii. Folgen der unionsrechtswidrigen IT-Sicherheitsdefinition	285
c. Fazit	286
3. (Digitale) Daten und Informationen	288
III. Risiko und Angemessenheit	289
1. Risiko	289
a. Beschränkung auf den „vernünftigen Aufwand“	289
b. Bezugspunkt des Risikos	290
2. Methodik, einschließlich Angemessenheit	293
3. Fazit	295
IV. Zusammenfassung	296
C. Unterschiede zur DSGVO und Folgen für die Resilienz	297
I. IT-Sicherheit vs. Datensicherheit	298
II. Bedeutung der Schutzziele und des Dienstes	299
1. Schutzziele	299
2. Dienst	300
a. Im Datensicherheitsrecht	301

Inhaltsverzeichnis

b.	Im IT-Sicherheitsrecht	301
c.	Fazit und Folgen für die Resilienz	302
III.	Verständnis des Systembegriffs	303
1.	Maßnahmenträger oder Schutzobjekt	303
2.	Systembestandteile	304
3.	Fazit und Folgen für die Resilienz	305
IV.	Risiko	307
1.	Definitionen des Risikos	307
a.	Vergleich	307
b.	Folgen für die Resilienz	310
2.	Methodik, einschließlich Angemessenheit	311
V.	Zusammenfassung	311
D.	Übertragung der Resilienz in den RegE BSIG	313
I.	Bestehende, funktionale Resilienz-Elemente	313
II.	Teleologische Gründe	316
III.	Gesamtergebnis	317
E.	Demonstration anhand des Szenarios	318
I.	Ungewissheit	318
II.	Resilienzmaßnahmen	319
1.	Ereigniserkennung	319
2.	Anpassungsfähigkeit	320
3.	Erholung	321
III.	Abstrakte Angemessenheit	321
5.	Kapitel: Zusammenfassung und Implementierungsvorschlag	323
A.	Zusammenfassung der Ergebnisse	323
I.	Resilienz in der DSGVO	324
II.	Übertragbarkeit in den RegE BSIG	328
B.	Implementierungsvorschlag	333
C.	Ausblick	335
Literaturverzeichnis		339

Abbildungsverzeichnis

Abbildung 1: Datenschutzrecht und IT-Sicherheitsrecht	37
Abbildung 2: Manipulation von personalisierten Diensten	43
Abbildung 3: Abgrenzung Art. 25/32 DSGVO	101
Abbildung 4: Abwägung zwischen Schutzgütern und Grundrechten der Adressaten	104
Abbildung 5: IT-System	115
Abbildung 6: Fehlerkette in der Verlässlichkeit	134
Abbildung 7: Fault Tolerance/Resilience	135
Abbildung 8: Risiko aus Wahrscheinlichkeit und Schadensschwere	162
Abbildung 9: Risiko- und Resilienzmethode	185
Abbildung 10: Schutzgüter kritischer Anlagen	253
Abbildung 11: IT-Sicherheitsdefinitionen nach RegE BSIG und NIS2-RL	265
Abbildung 12: Bezugspunkt des Risikos nach NIS-RL	291
Abbildung 13: Bezugspunkt des Risikos nach NIS2-RL	292
Abbildung 14: Risikobezugspunkte und -definitionen von NIS-RL, DSGVO und NIS2-RL	308

Tabellenverzeichnis

Tabelle 1: Art. 24/25/32 DSGVO	86
Tabelle 2: Schutzziele in Art. 25 Abs. 1 i.V.m. 5 Abs. 1 lit f) und 32 Abs. 2 DSGVO	96
Tabelle 3: Übersetzungen von Resilienz im Daten- und IT- Sicherheitsrecht	123
Tabelle 4: Kategorien von Ungewissheit	176
Tabelle 5: Verständnisse des Dienstes in NIS2-RL und RegE BSIG	287

Abkürzungsverzeichnis

a.A.	anderer Ansicht/Auffassung
ABl.	Amtsblatt der Europäischen Union
a.E.	am Ende
a.F.	alte Fassung
Art.	Artikel
AS-Nr.	Aufsatznummer
Az.	Aktenzeichen
BDSG	Bundesdatenschutzgesetz
BKartA	Bundeskartellamt
BMI	Bundesministerium des Innern und für Heimat
BR-Drs.	Bundesratsdrucksache
BReg	Bundesregierung
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik in seiner Fassung ab dem 23.06.2021
BT-Drs.	Bundestagsdrucksache
BW	Baden-Württemberg
bzgl.	Bezüglich
bzw.	Beziehungsweise
CISA	Cybersecurity and Infrastructure Security Agency (USA)
CR	Computer und Recht
CRA-E	Entwurf für eine EU-VO über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM(2022) 454 final.
CSA	Cybersecurity Act (EU-VO 2019/881)
DDoS	Distributed Denial-of-Service
DIW-Modell	Daten-, Informations-, Wissensmodell
DoD	United States Department of Defense (Verteidigungsministerium der USA)

Abkürzungsverzeichnis

DORA	EU-VO 2022/2554 des europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (Digital Operational Resilience Act), ABl. 2022 L 333, 1
DSA	EU-VO 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Digital Services Act), ABl. 2022 L 277, 1
DS-RL	RL 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281/31 (alte Rechtslage, aufgehoben durch die DSGVO am 25.05.2018)
DSGVO	EU-VO 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119/1
DSK	Datenschutzkonferenz (Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder)
DVO	Durchführungsverordnung
ebd.	ebenda
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäische Datenschutzbeauftragte
EL	Ergänzungslieferung
en	Englisch
EU	Europäische Union
(EU-)VO	Europäische Verordnung
EuG	Gericht der Europäischen Union
EuGH	Europäische Gerichtshof
EG	Erwägungsgrund
GG	Grundgesetz für die Bundesrepublik Deutschland
ggf.	gegebenenfalls
Hs.	Halbsatz
i.d.R.	in der Regel/im Regelfall

Abkürzungsverzeichnis

IEEE	Institute of Electrical and Electronics Engineers (Globaler Berufsverband mit Sitz in New York, USA)
ISMS	Informationssicherheitsmanagementsystem
ISO	Internationale Organisation für Normung
i.e.S.	im engeren Sinn
IT	Informationstechnik/Informationstechnologie
IT-Sicherheit	Sicherheit in der Informationstechnik
i.V.m.	in Verbindung mit
i.w.S.	im weiteren Sinn
KI	Künstliche Intelligenz
KI-VO-E	Entwurf einer Verordnung zu harmonisierten Vorschriften über Künstliche Intelligenz, Stand: 16.01.2024, 5662/24.
LfDI BW	Landesbeauftragte für den Datenschutz und die Informationsfreiheit BW
lit	littera (lateinisch für Buchstabe)
IT-Sicherheitsrecht	Recht der Sicherheit in der Informationstechnik
MedizinProdVO	EU-VO 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, ABl. 2017 L 117/1
ML	Maschinelles Lernen
m.w.N.	mit weiteren Nachweisen
NIS-RL	RL über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (RL 2016/1148), Abl. 2016 L 194/1
NIS2-RL	RL über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (RL 2022/2555), ABl. 2022 L 333/80
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
o.g.	oben genannt
RED	RL 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften

Abkürzungsverzeichnis

	der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG Text von Bedeutung für den EWR (en: Radio Equipment Directive), ABl. 2014 L 153/62
RefE	Referentenentwurf
RefE BSIG	Gesetz über das Bundesamt für Sicherheit in der Informations-technik <i>Referentenentwurf des BMI aus dem NIS2UmsuCG vom 22.12.2023</i>
RefE KRITIS-DachG	Dachgesetz zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen, <i>Referentenentwurf des BMI vom 21.12.2023</i>
RefE NIS2Umsu-CG	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz <i>Referentenentwurf des BMI vom 22.12.2023</i>
RegE	Regierungsentwurf
RegE BSIG	Gesetz über das Bundesamt für Sicherheit in der Informations-technik, <i>Regierungsentwurf des NIS2UmsuCG vom 22.07.2024, 380/24</i>
RKE-RL	Richtlinie für die Resilienz kritischer Einrichtungen,
RL	Europäische Richtlinie
S.	Satz / Seite
sog.	sogenannt
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutzgesetz (ehemals TTDSG)
toM	technische und organisatorische Maßnahmen
UEBA	User and Entity Behavior Analysis
UN-R 155	UN-Regelung Nr. 155 — Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems [2021/387], ABl. 2021 L 82/30
USA	Vereinigte Staaten von Amerika
Vol.	Volume (en), bezeichnet v.a. bei ausländischen Fachzeitschriften eine Menge von Heften (en.: Issue) in einem bestimmten Zeitraum.
z.B.	Zum Beispiel
Ziff.	Ziffer