

Recht der Informationssicherheit

Kipker / Reusch / Ritter

2023

ISBN 978-3-406-78339-5

C.H.BECK

schnell und portofrei erhältlich bei
beck-shop.de

Die Online-Fachbuchhandlung beck-shop.de steht für Kompetenz aus Tradition. Sie gründet auf über 250 Jahre juristische Fachbuch-Erfahrung durch die Verlage C.H.BECK und Franz Vahlen.

beck-shop.de hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird beck-shop.de für sein umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

Kipker/Reusch/Ritter (Hrsg.)
Recht der Informationssicherheit


beck-shop.de
DIE FACHBUCHHANDLUNG

beck-shop.de
DIE FACHBUCHHANDLUNG

Recht der Informationssicherheit

Kommentar

Herausgegeben von

Prof. Dr. Dennis-Kenji Kipker

Professor für IT-Sicherheitsrecht an der HSB
Legal Advisor für den VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V. in Offenbach am Main

Philipp Reusch

Rechtsanwalt in Berlin
Lehrbeauftragter für Produkthaftung und Produktsicherheit
an der RWTH Aachen
Lehrbeauftragter an der TH Köln

Steve Ritter

Referatsleiter IT-Sicherheit und Recht beim Bundesamt für Sicherheit
in der Informationstechnik (BSI)

Bearbeitet von den Herausgebern und

Klaus Beucher, LL.M. (Wisconsin); Dr. Markus Böhme, LL.M.;
Dr. Vyacheslav Bortnikov; Dr. Anne Brandenburg;
Mareike Christine Gehrman; Moritz Glade; Dr. Martin Hecheltjen;
Prof. Dr. Tobias Herbst; Stefan Hessel, LL.M.; Detlef Klett;
Dr. Hannfried Leisterer; Dr. Carlo Piltz; Karin Potel;
Dr. Philipp Roos; Dr. Paul Voigt, Lic. en Derecho, CIPP/E;
Rebekka Weiß, LL.M.; Rigo Wenning; Johannes Zwerschke, LL.M.

2023



C.H. BECK

Zitiervorschlag: Kipker/Reusch/Ritter/Brandenburg BSIG § 3a Rn. 1


beck-shop.de
DIE FACHBUCHHANDLUNG
www.beck.de

ISBN 978 3 406 78339 5

© 2023 Verlag C. H. Beck oHG
Wilhelmstraße 9, 80801 München

Umschlaggestaltung: Druckerei C. H. Beck Nördlingen

Druck und Bindung: Beltz Grafische Betriebe GmbH,
Am Fliegerhorst 8, 99947 Bad Langensalza

Satz: Jung Crossmedia Publishing GmbH
Gewerbestraße 17, 35633 Lahnau



chbeck.de/nachhaltig

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

Vorwort

Informationssicherheit, Cybersecurity, IT-Sicherheit, Datensicherheit: Diese Begriffe stehen allesamt für ein Thema, das wichtiger denn je ist, um Staat, Wirtschaft und Gesellschaft vor schädlichen Auswirkungen aus dem Cyberraum zu schützen. Jüngst belegen die Corona-Pandemie und der Krieg in der Ukraine, dass die Schutzbedarfe ganz erheblich gestiegen und die Bedrohungslagen international vielfältig sind. Dementsprechend müssen auch die erhöhten gemeinsamen Anstrengungen von Regierung, Behörden und Unternehmen vor diesem Hintergrund gesehen werden. Zuvorderst geht es darum, informationstechnische Systeme in den unterschiedlichsten Sektoren und Branchen sowie von verschiedener Größe vom KMU bis hin zum transnational agierenden Konzern technisch-organisatorisch abzusichern. Ein solches Vorgehen kann jedoch nicht im „luftleeren Raum“ stattfinden, sondern muss stets an Leitsätze und verbindliche, konkretisierende Vorgaben geknüpft sein. Dies ist die Aufgabe der Gesetzgebung zur Informationssicherheit, der sich dieser Kommentar widmet. Bewusst wird der Blick dabei nicht nur auf das deutsche, sondern auch auf das europäische Recht gerichtet, denn längst geht es nicht mehr allein darum, den Schutz ausschließlich von Kritischen Infrastrukturen auf nationaler Ebene sicherzustellen, sondern es müssen der europäische digitale Binnenmarkt und dessen digitale Souveränität in die Betrachtung einbezogen werden. Auch findet der Informationsaustausch zu den Gefahren für die Cybersicherheit und deren Abwehr mitgliedstaatenübergreifend statt, da die Cyberbedrohungen nicht an nationalstaatlichen Grenzen enden. Die Cybersecurity ist zu einer horizontalen, multidisziplinären und hybriden Herausforderung geworden, die alle Sektoren und Branchen gleichermaßen adressiert und über die Bezüge zur Datensicherheit auch im Datenschutzrecht eine bedeutende Rolle spielt. Sie beginnt im Kleinen bei Themen des Verbraucherschutzes und der Absicherung von IoT, bewegt sich im Kontext industrieller Umgebungen sowie industrieller Steuerungssysteme und reicht bis zur Absicherung der Kritischen Infrastrukturen und zentraler staatlicher Einrichtungen. Betroffen sein können dabei Hardware, Software und eingebettete Systeme gleichermaßen. Die Vielfalt dieser Möglichkeiten zur rechtlichen Regulierung einerseits, andererseits aber auch ihre Bezüge zur praxisgerechten Umsetzung will der Kommentar zum Recht der Informationssicherheit aktuell und systematisch aufbereitet, verständlich sowie detailreich formuliert wiedergeben, indem er als tägliches Arbeitsmittel dabei unterstützt, den richtigen Maßstab für die Cybersecurity im konkreten Einzelfall zu bestimmen.

Bremen/Berlin/Königswinter
im Dezember 2022

Prof. Dr. Dennis-Kenji Kipker
Philipp Reusch
Steve Ritter

beck-shop.de
DIE FACHBUCHHANDLUNG

Bearbeiterverzeichnis

- Klaus Beucher, LL.M. (Wisconsin)*
Rechtsanwalt in Köln §§ 7, 7c, 7d, 44b AtG;
Art. 58–69 CSA
- Dr. Markus Böhme, LL.M.*
Rechtsanwalt in Düsseldorf § 11 EnWG
- Dr. Vyacheslav Bortnikov*
Regierungsdirektor beim Bundes-
beauftragten für den Datenschutz
und die Informationsfreiheit §§ 29, 30 TTDSG
- Dr. Anne Brandenburg*
Oberregierungsrätin beim Bundesamt für
Sicherheit in der Informationstechnik §§ 3a, 6–6f, 7a, 8 BSIG
- Mareike Christine Gehrman*
Rechtsanwältin in Düsseldorf § 178 TKG; § 12 TTDSG
- Moritz Glade*
Regierungsrat beim Bundesamt für
Sicherheit in der Informationstechnik §§ 7d, 9, 9b, 9c, 14 BSIG;
§§ 1, Anhang 1–7 BSI-Kri-
tisiV
- Dr. Martin Hecheltjen*
Oberregierungsrat beim Bundesamt für
Sicherheit in der Informationstechnik §§ 5, 5b BSIG
- Prof. Dr. Tobias Herbst*
Professor an der Hochschule für Polizei und
öffentliche Verwaltung NRW
Privatdozent an der Humboldt-Universität
zu Berlin Art. 5 DS-GVO
- Stefan Hessel, LL.M.*
Rechtsanwalt in Saarbrücken §§ 8b, 8c BSIG;
§§ 165–169 TKG
- Prof. Dr. Dennis-Kenji Kipker*
Professor für IT-Sicherheitsrecht an der HSB
Legal Advisor für den VDE Verband der
Elektrotechnik Elektronik Informations-
technik e.V. in Offenbach am Main Art. 24 DS-GVO
- Detlef Klett*
Rechtsanwalt in Düsseldorf § 178 TKG, § 12 TTDSG

Bearbeiterverzeichnis

<i>Dr. Hannfried Leisterer</i> Regierungsrat beim Bundesministerium des Innern und für Heimat	§§ 4, 4b, 5a, 7, 8f, 9b, 10, 13 BSIG
<i>Dr. Carlo Piltz</i> Rechtsanwalt in Berlin	Art. 32 DS-GVO
<i>Karin Potel</i> Rechtsanwältin in Saarbrücken	§§ 8b, 8c BSIG
<i>Philipp Reusch</i> Rechtsanwalt in Berlin Lehrbeauftragter für Produkthaftung und Produktsicherheit an der RWTH Aachen	Art. 51–57 CSA
<i>Steve Ritter</i> Referatsleiter IT-Sicherheit und Recht beim Bundesamt für Sicherheit in der Informationstechnik (BSI) Lehrbeauftragter an der TH Köln	§§ 1–3, 4a, 5c, 7b, 7c, 8a, 8d, 8e, 9a, 11, 12, 14a, 15 BSIG; §§ 2–9, Anhang 1–7 BSI-KritisV
<i>Dr. Philipp Roos</i> Rechtsanwalt in Düsseldorf	§§ 7, 7c, 7d, 44b AtG; Art. 58–69 CSA
<i>Dr. Paul Voigt, Lic. en Derecho, CIPP/E</i> Rechtsanwalt in Berlin	§ 11 EnWG
<i>Rebekka Weiß, LL.M.</i> Leiterin Vertrauen & Sicherheit	Art. 46–50 CSA
<i>Rigo Wénning</i> Unternehmensjurist und Rechtsanwalt in Frankfurt am Main	Art. 1–45 CSA
<i>Johannes Zwerschke, LL.M.</i> Rechtsanwalt in Berlin	§ 19 Abs. 4 TTDSG; Art. 32 DS-GVO

Inhaltsverzeichnis

Vorwort	V
Bearbeiterverzeichnis	VII
Abkürzungsverzeichnis	XV

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)

§ 1	Bundesamt für Sicherheit in der Informationstechnik	1
§ 2	Begriffsbestimmungen	5
§ 3	Aufgaben des Bundesamtes	25
§ 3a	Verarbeitung personenbezogener Daten	37
§ 4	Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes	43
§ 4a	Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte	50
§ 4b	Allgemeine Meldestelle für die Sicherheit in der Informationstechnik	57
§ 5	Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes	62
§ 5a	Verarbeitung behördeninterner Protokollierungsdaten	102
§ 5b	Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen	106
§ 5c	Bestandsdatenauskunft	120
§ 6	Beschränkungen der Rechte der betroffenen Person	127
§ 6a	Informationspflicht bei Erhebung von personenbezogenen Daten	130
§ 6b	Auskunftsrecht der betroffenen Person	133
§ 6c	Recht auf Berichtigung	136
§ 6d	Recht auf Löschung	138
§ 6e	Recht auf Einschränkung der Verarbeitung	140
§ 6f	Widerspruchsrecht	142
§ 7	Warnungen	144
§ 7a	Untersuchung der Sicherheit in der Informationstechnik	159
§ 7b	Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden	167
§ 7c	Anordnungen des Bundesamtes gegenüber Diensteanbietern	173
§ 7d	Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten	185
§ 8	Vorgaben des Bundesamtes	190
§ 8a	Sicherheit in der Informationstechnik Kritischer Infrastrukturen	201

Inhaltsverzeichnis

§ 8b	Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen	218
§ 8c	Besondere Anforderungen an Anbieter digitaler Dienste	231
§ 8d	Anwendungsbereich	239
§ 8e	Auskunftsverlangen	248
§ 8f	Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse	252
§ 9	Zertifizierung	264
§ 9a	Nationale Behörde für die Cybersicherheitszertifizierung	283
§ 9b	Untersagung des Einsatzes kritischer Komponenten	291
§ 9c	Freiwilliges IT-Sicherheitskennzeichen	310
§ 10	Ermächtigung zum Erlass von Rechtsverordnungen	329
§ 11	Einschränkung von Grundrechten	338
§ 12	Rat der IT-Beauftragten der Bundesregierung	339
§ 13	Berichtspflichten	340
§ 14	Bußgeldvorschriften	346
§ 14a	Institutionen der Sozialen Sicherung	369
§ 15	Anwendbarkeit der Vorschriften für Anbieter digitaler Dienste	372

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)

§ 1	Begriffsbestimmungen	373
§ 2	Sektor Energie	396
§ 3	Sektor Wasser	400
§ 4	Sektor Ernährung	403
§ 5	Sektor Informationstechnik und Telekommunikation	406
§ 6	Sektor Gesundheit	409
§ 7	Sektor Finanz- und Versicherungswesen	413
§ 8	Sektor Transport und Verkehr	419
§ 9	Evaluierung	422
§ 7	Inkrafttreten	423
Anhang 1		424
Anhang 2		443
Anhang 3		450
Anhang 4		458
Anhang 5		468
Anhang 6		477
Anhang 7		498

Inhaltsverzeichnis

Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz)

§ 7	Genehmigung von Anlagen	519
§ 7c	Pflichten des Genehmigungsinhabers	532
§ 7d	Weitere Vorsorge gegen Risiken	538
§ 44b	Meldewesen für die Sicherheit in der Informationstechnik	543

Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG)

§ 11	Betrieb von Energieversorgungsnetzen	555
------	--	-----

Telekommunikationsgesetz (TKG)

§ 165	Technische und organisatorische Schutzmaßnahmen	601
§ 166	Sicherheitsbeauftragter und Sicherheitskonzept	614
§ 167	Katalog von Sicherheitsanforderungen	619
§ 168	Mitteilung eines Sicherheitsvorfalls	621
§ 169	Daten- und Informationssicherheit	626
§ 178	Gewährleistung der Sicherheit der Daten	634

Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz – TTDSG)

§ 12	Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten	647
§ 19 Abs. 4	Technische und organisatorische Vorkehrungen	667
§ 29	Zuständigkeit, Aufgaben und Befugnisse der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit	678
§ 30	Zuständigkeit, Aufgaben und Befugnisse der Bundesnetz- agentur	686

Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)

Titel I Allgemeine Bestimmungen

Art. 1	Gegenstand und Geltungsbereich	714
Art. 2	Begriffsbestimmungen	719

Inhaltsverzeichnis

Titel II ENISA (Agentur der Europäischen Union für Cybersicherheit)

Kapitel I Mandat und Ziele

Art. 3 Mandat	736
Art. 4 Ziele	739

Kapitel II Aufgaben

Art. 5 Entwicklung und Umsetzung der Unionspolitik und des Unionsrechts	743
Art. 6 Kapazitätsaufbau	748
Art. 7 Operative Zusammenarbeit auf Unionsebene	754
Art. 8 Markt, Cybersicherheitszertifizierung und Normung	757
Art. 9 Wissen und Informationen	760
Art. 10 Sensibilisierung und Ausbildung	762
Art. 11 Forschung und Innovation	764
Art. 12 Internationale Zusammenarbeit	766

Kapitel III Organisation der ENISA

Art. 13 Struktur der ENISA	768
--------------------------------------	-----

Abschnitt 1 Verwaltungsrat

Art. 14 Zusammensetzung des Verwaltungsrats	770
Art. 15 Aufgaben des Verwaltungsrats	773
Art. 16 Vorsitz des Verwaltungsrats	784
Art. 17 Sitzungen des Verwaltungsrats	785
Art. 18 Vorschriften für die Abstimmung im Verwaltungsrat	787

Abschnitt 2 Exekutivrat

Art. 19 Exekutivrat	789
-------------------------------	-----

Abschnitt 3 Exekutivdirektor

Art. 20 Pflichten des Exekutivdirektors	792
---	-----

Abschnitt 4 ENISA-Beratungsgruppe, Gruppe der Interessenträger für die Cybersicherheitszertifizierung und Netz der nationalen Verbindungsbeamten

Art. 21 ENISA-Beratungsgruppe	796
Art. 22 Gruppe der Interessenträger für die Cybersicherheitszertifizierung	799
Art. 23 Netz der nationalen Verbindungsbeamten	802

Abschnitt 5 Arbeitsweise

Art. 24 Einheitliches Programmplanungsdokument	805
--	-----

Inhaltsverzeichnis

Art. 25	Interessenerklärung	809
Art. 26	Transparenz	810
Art. 27	Vertraulichkeit	812
Art. 28	Zugang zu Dokumenten	815

Kapitel IV Aufstellung und Gliederung des Haushaltsplans der ENISA

Art. 29	Aufstellung des Haushaltsplans der ENISA	817
Art. 30	Gliederung des Haushaltsplans der ENISA	819
Art. 31	Ausführung des Haushaltsplans der ENISA	820
Art. 32	Finanzregelung	824
Art. 33	Betrugsbekämpfung	825

Kapitel V Personal

Art. 34	Allgemeine Bestimmungen	827
Art. 35	Vorrechte und Befreiungen	828
Art. 36	Exekutivdirektor	829
Art. 37	Abgeordnete nationale Sachverständige und sonstiges Personal	831

Kapitel VI Allgemeine Bestimmungen für die ENISA

Art. 38	Rechtsform der ENISA	833
Art. 39	Haftung der ENISA	834
Art. 40	Sprachenregelung	835
Art. 41	Schutz personenbezogener Daten	836
Art. 42	Zusammenarbeit mit Drittländern und internationalen Organisationen	837
Art. 43	Sicherheitsvorschriften für den Schutz von vertraulichen Informationen, die nicht zu den Verschlusssachen zählen und von Verschlusssachen	840
Art. 44	Sitzabkommen und Arbeitsbedingungen	841
Art. 45	Verwaltungskontrolle	843

Titel III Zertifizierungsrahmen für die Cybersicherheit

Art. 46	Europäischer Zertifizierungsrahmen für die Cybersicherheit	844
Art. 47	Das fortlaufende Arbeitsprogramm der Union für die europäische Cybersicherheitszertifizierung	847
Art. 48	Auftrag für ein europäisches Schema für die Cybersicherheitszertifizierung	848
Art. 49	Ausarbeitung, Annahme und Überarbeitung der europäischen Schemata für die Cybersicherheitszertifizierung	850
Art. 50	Website zu europäischen Schemata für die Cybersicherheitszertifizierung	852
Art. 51	Sicherheitsziele der europäischen Schemata für die Cybersicherheitszertifizierung	853

Inhaltsverzeichnis

Art. 52	Vertrauenswürdigkeitsstufen der europäischen Schemata für die Cybersicherheitszertifizierung	867
Art. 53	Selbstbewertung der Konformität	872
Art. 54	Elemente der europäischen Schemata für die Cybersicherheitszertifizierung	875
Art. 55	Ergänzende Informationen über die Cybersicherheit von zertifizierten IKT-Produkten, -Diensten und -Prozessen	884
Art. 56	Cybersicherheitszertifizierung	888
Art. 57	Nationale Cybersicherheitszertifizierungsschemata und Cybersicherheitszertifikate	894
Art. 58	Nationale Behörden für die Cybersicherheitszertifizierung	897
Art. 59	Gegenseitige Begutachtung	908
Art. 60	Konformitätsbewertungsstellen	912
Art. 61	Notifikation	916
Art. 62	Europäische Gruppe für die Cybersicherheitszertifizierung	919
Art. 63	Beschwerderecht	924
Art. 64	Recht auf einen wirksamen gerichtlichen Rechtsbehelf	927
Art. 65	Sanktionen	930

Titel IV Schlussbestimmungen

Art. 66	Ausschussverfahren	934
Art. 67	Bewertung und Überarbeitung	936
Art. 68	Aufhebung und Rechtsnachfolge	940
Art. 69	Inkrafttreten	942

Verordnung (EU) 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)

Kapitel II Grundsätze

Art. 5	Grundsätze für die Verarbeitung personenbezogener Daten	948
--------	---	-----

Kapitel IV Verantwortlicher und Auftragsverarbeiter

Abschnitt 1 Allgemeine Pflichten

Art. 24	Verantwortung des für die Verarbeitung Verantwortlichen	968
---------	---	-----

Abschnitt 2 Sicherheit personenbezogener Daten

Art. 32	Sicherheit der Verarbeitung	978
---------	-----------------------------	-----

Stichwortverzeichnis		1013
-----------------------------	--	------