
DuD-Fachbeiträge

Reihe herausgegeben von

Gerrit Hornung, Kassel, Deutschland

Helmut Reimer, Erfurt, Deutschland

Karl Rihaczek, Bad Homburg vor der Höhe, Deutschland

Alexander Roßnagel, Kassel, Deutschland

Die Buchreihe ergänzt die Zeitschrift DuD – Datenschutz und Datensicherheit in einem aktuellen und zukunftsreichen Gebiet, das für Wirtschaft, öffentliche Verwaltung und Hochschulen gleichermaßen wichtig ist. Die Thematik verbindet Informatik, Rechts-, Kommunikations- und Wirtschaftswissenschaften. Den Lesern werden nicht nur fachlich ausgewiesene Beiträge der eigenen Disziplin geboten, sondern sie erhalten auch immer wieder Gelegenheit, Blicke über den fachlichen Zaun zu werfen. So steht die Buchreihe im Dienst eines interdisziplinären Dialogs, der die Kompetenz hinsichtlich eines sicheren und verantwortungsvollen Umgangs mit der Informationstechnik fördern möge.

Reihe herausgegeben von

Prof. Dr. Gerrit Hornung

Universität Kassel

Prof. Dr. Helmut Reimer

Erfurt

Dr. Karl Rihaczek

Bad Homburg v.d. Höhe

Prof. Dr. Alexander Roßnagel

Universität Kassel

Johannes Karl Martin Müller

Datenschutz und IT-Sicherheitsmaßnahmen in der Industrie 4.0

Rechtsverträgliche
Technikgestaltung

 Springer Vieweg

Johannes Karl Martin Müller
Mühlhausen, Deutschland

Zugl.: Dissertation zur Erlangung des akademischen Grades Doktor der Rechtswissenschaften (Dr. jur.) an der Universität Kassel, Fachbereich 07 – Wirtschaftswissenschaften
Erstgutachter: Prof. Dr. Alexander Roßnagel
Zweitgutachter: Prof. Dr. Gerrit Hornung, LL.M.
Disputation am 31.01.2024

Die Kernarbeiten der Dissertation entstanden im Rahmen des vom Bundesministerium für Bildung und Forschung geförderten Forschungsprojekts „IUNO – Nationales Referenzprojekt für IT-Sicherheit in der Industrie 4.0“.

ISSN 2512-6997

ISSN 2512-7004 (electronic)

DuD-Fachbeiträge

ISBN 978-3-658-45746-4

ISBN 978-3-658-45747-1 (eBook)

<https://doi.org/10.1007/978-3-658-45747-1>

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

© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert an Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2024

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 jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geographische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: Carina Reibold

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.

Meinen Eltern

Vorwort der Herausgeber

Die Arbeit von Herrn Müller befasst sich mit einem für die digitale Gesellschaft sowie das Verhältnis von Wirtschaft und Datenschutzrecht sehr aktuellen und bedeutsamen Thema, nämlich die gleichzeitige Gewährleistung von IT-Sicherheit und Datenschutz in der Industrie 4.0.

Industrie 4.0 verspricht durch die Nutzung allgegenwärtiger Datenverarbeitung und die Vernetzung der Sensoren und Aktoren der Produktionsmittel und Werkstücke, der Produkte und Menschen eine erheblich höhere Produktivität, Automatisierung der Arbeit und Individualisierung der Produkte. Die Stärke der Industrie 4.0, die Digitalisierung und Vernetzung der Produktion, ist zugleich auch ihre Schwäche. Sie ist von dieser Digitalisierung und Vernetzung vollständig abhängig. Dies erhöht das Schadenspotential von Fehlern und Angriffen und ermöglicht neue Fehler- und Angriffsformen. Industrie 4.0 setzt daher vielfältige und umfassende Sicherheitsmaßnahmen voraus. Diese müssen die enormen in der Industrie 4.0 entstehenden Daten und Kommunikationsflüsse für das rechtzeitige Erkennen von Angriffen und Fehlern sowie deren unverzügliche Abwehr und Korrektur nutzen.

Dabei werden zwangsläufig auch Daten von Beschäftigten und Kooperationspartnern erfasst und ausgewertet. Dies ermöglicht und erfordert bisweilen sogar, ihr Verhalten zu kontrollieren und die erfassten Daten zu personenbezogenen Verhaltensprofilen zusammenzuführen. Die Sicherheitsmaßnahmen und die durch sie erfolgenden Datenverarbeitungen greifen daher in den Schutzbereich des Grundrechts auf Datenschutz und informationelle Selbstbestimmung der betroffenen Personen ein. Dadurch entsteht die für Industrie 4.0 entscheidende Frage, wie Sicherheit und Freiheit, Überwachung der Produktion und Datenschutz der Beschäftigten und Kooperationspartner zugleich gewährleistet werden können.

Hier setzt die Arbeit von Herrn Müller an. Sie untersucht, wie die grundrechtlich gesicherten Positionen der Unternehmer und diejenigen der Beschäftigten und anderen betroffenen Personen (und damit im Weiteren der Gesellschaft) für die Umsetzung von Sicherheitsmaßnahmen zu einem schonenden Ausgleich gebracht werden können, um die Chancen der Sicherheitstechnik für Industrie 4.0 zu verwirklichen und die Risiken zu minimieren. Hierfür überführt er rechtliche Vorgaben mit Hilfe von Methoden rechtsverträglicher Technikgestaltung in technisch-organisatorische Vorschläge zur Gestaltung einer grundrechtsschonenden Implementierung von Sicherheitsmaßnahmen, die insbesondere die Anforderungen des Datenschutzes berücksichtigen.

Für diese Untersuchung bestimmt er zum einen den Schutzbedarf der Industrie 4.0 und die von ihm geforderten Sicherheitsmaßnahmen, um die Datenschutzrisiken der Beschäftigten und Kooperationspartner zu erkennen und die Aufgaben des Rechts in dem Konflikt zwischen Sicherheitskonzepten der Industrie 4.0 und dem notwendigen Schutz der betroffenen Personen zu konkretisieren. Zum anderen sucht er nach Lösungen des Konflikts in den vielfältigen Möglichkeiten der Gestaltung der Sicherheitssysteme. Praktische Konkordanz zwischen den berechtigten Sicherheitsinteressen und dem notwendigen Schutz der Grundrechte der betroffenen Personen verfolgt er sodann durch eine an Rechtsvorgaben orientierte Systemgestaltung.

Mit seiner hier vorgelegten Arbeit füllt Herr Müller wesentliche Lücken im Recht modernster Informations- und Kommunikationstechniken. Indem er den Schutzbedarf der Industrie 4.0, notwendige Sicherheitsmaßnahmen, die Risiken für den Datenschutz der betroffenen Personen und die Aufgaben des Rechtsstaats und des Gesetzgebers in der Bewältigung dieses Konflikts untersucht, bietet er sowohl wertvolle Hinweise für das Verständnis eines aktuellen und bedeutsamen Rechtsproblems und erarbeitet wichtige Grundlagen für seine Lösung. Indem er zeigt, wie Lösungen durch rechtsverträgliche Technikgestaltung gefunden werden können, gibt er wertvolle Vorschläge für die Praxis der

Sicherheitsgewährleistung und den Grundrechtsschutz in der Industrie 4.0 und bietet wichtige Hinweise für die Rechtspolitik, die solche Lösungen unterstützen muss.

Die Arbeit entstand zu großen Teilen im Rahmen der Mitarbeit im nationalen Referenzprojekt für IT-Sicherheit in Industrie 4.0 „IUNO“. Das interdisziplinäre Forschungsprojekt wurde von 20 Partnern von 2015 bis 2018 mit Unterstützung des Bundesministeriums für Bildung und Forschung durchgeführt. In ihm bearbeitete Herr Müller selbstständig die hier untersuchten Rechtsthemen und konnte in enger interdisziplinärer Zusammenarbeit mit Forschern aus Hochschulen, Fraunhofer-Instituten und Unternehmen Fragen nachgehen, die für seine Untersuchung relevant sind. Die Erkenntnisse hat er in den folgenden Jahren konkretisiert, erweitert und aktualisiert.

Für die künftige Gewährleistung von Sicherheit und Datenschutz in der Industrie 4.0 sowie die rechtswissenschaftliche Diskussion über diese Aufgabe ist zu hoffen, dass die Entscheidungsträger in Politik, Wirtschaft und Wissenschaft die Erkenntnisse dieser Arbeit zur Kenntnis nehmen und bei ihren Entscheidungen berücksichtigen.

Kassel, im Juni 2024

Alexander Roßnagel

Vorwort des Autors

Diese Arbeit entstand während meiner Zeit als wissenschaftlicher Mitarbeiter am Fachgebiet Öffentliches Recht, insb. Umwelt- und Technikrecht, an der Universität Kassel. Dort insbesondere am Wissenschaftlichen Zentrum für Informationstechnik-Gestalt (ITeG) in der Projektgruppe für verfassungsrechtliche Technikgestaltung, kurz: provet, unter der Leitung von Herrn Prof. Alexander Roßnagel und später auch durch Herrn Prof. Dr. Gerrit Hornung, LL.M.

Ausgangspunkt meiner Forschung und gleichzeitig deren Grundlage bildete meine Mitarbeit im interdisziplinären Projekt IUNO, Nationales Referenzprojekt für IT-Sicherheit in der Industrie 4.0, welches vom Bundesministerium für Bildung und Forschung gefördert wurde. IUNO begann im Juli 2015 und endete im September 2018. Die vorliegende Arbeit wurde im Mai 2023 unter dem Titel „Rechtsverträgliche Technikgestaltung: Datenschutz bei IT-Sicherheitsmaßnahmen in der Industrie 4.0“ als Dissertation bei der Universität Kassel eingereicht und im Dezember 2023 angenommen. Der ihr zugrundeliegende Rechtsstand ist Mai 2023.

Bedanken möchte ich mich bei allen Menschen, die im Beruflichen und/oder auch im Privaten dazu beigetragen haben, dass diese Arbeit ihren Abschluss fand.

In erster Linie möchte ich meinem Doktorvater, Herrn Prof. Dr. Alexander Roßnagel, danken. Bedanken möchte ich mich für das in mich gesetzte Vertrauen, seine Geduld und seine unersetzlichen Anregungen. Ihm gebührt nicht nur die erfolgreiche Unterstützung zur Findung des Themas meiner Dissertation und die fachliche Begleitung auf dem Weg bis zu deren Fertigstellung, sondern vielmehr hat er es über die vielen Jahre bei provet immer wieder aufs Neue verstanden, durch seine konstruktive Kritik und seine behutsame, aber stets weitsichtige Art, meine Freude an der juristischen Auseinandersetzung aufrechtzuerhalten.

Weiter danke ich Herrn Prof. Dr. Gerrit Hornung, LL.M. für die Übernahme und Erstellung des Zweitgutachtens.

Meinen Kollegen bei provet danke ich für 7 ½ interessante und schöne Jahre sowie das angenehme und mitunter freundschaftliche Arbeitsklima, zu dem Herr Privatdozent Dr. Christian Geminn und Frau Edith Weise in besonderer Weise beigetragen haben.

Danken möchte ich auch allen Freunden abseits des beruflichen Umfeldes, die trotz des Umstands, dass ich immer seltener zur Verfügung gestanden habe, ihre Freundschaft unerschütterlich aufrechterhalten haben.

Mein ganz besonderer Dank gilt jedoch meiner Familie. Sie erdet mich, ist mir stets Anker und zugleich Inspiration. Ohne ihren Rückhalt und ihre Ablenkung wäre ich über die Jahre wohl nicht zu einem Ende gelangt. Vielen Dank insofern meinen Eltern, Geschwistern, ihren Partnern, und nicht zuletzt, ihren Kindern.

Meinen Eltern ist diese Arbeit in großer Dankbarkeit gewidmet. Sie haben mich zu dem werden lassen, was und wer ich heute bin. Ihr Vertrauen, ihre Unterstützung, ihr unbedingter und liebevoller Rückhalt begleiten mich ein Leben lang. Vielen Dank, Euch.

Mühlhausen, im Juni 2024

Dr. Johannes Karl Martin Müller MLE.

Inhaltsverzeichnis

Abkürzungsverzeichnis	XVII
1. Einleitung	2
1.1. Einbettung der Arbeit	2
1.2. Herleitung der Fragestellung	4
1.3. Bisherige Bearbeitung	6
1.4. Methode	6
1.5. Übersicht	7
2. Industrielle Revolutionen	9
3. Digitalisierung	14
3.1. Informationstechnologie und Informationstechnik	15
3.2. Computer und Netzwerke	15
3.3. Das Internet: Ein Fundament mit Schwächen	19
3.4. Ubiquitäres Computern	20
3.5. Internet of Things	21
3.6. Industrial Internet of Things	23
4. Industrie 4.0: Sicherungsgegenstand und Schadenspotential	25
4.1. Vierte industrielle Revolution: Industrie 4.0?	26
4.2. Automatisierung und Digitalisierung der Produktion als Dogma einer Industrie 4.0	28
4.3. Das Aufbrechen hierarchisch gesteuerter Automatisierung	29
4.3.1. Die Automatisierungspyramide	30
4.3.1.1. Das Enterprise Resource Planning System (ERP), Produktionsplanung und -steuerung (PPS) und Advanced Planning and Scheduling (APS)	32
4.3.1.2. Das Manufacturing Execution System (MES)	33
4.3.1.3. Cyber Physical Systems (CPS)	34
4.3.1.3.1. CPS und Kognition	36
4.3.1.3.2. CPS und künstliche Intelligenz	36
4.3.1.3.3. Künstliche Intelligenz im Kontext von Varianz, Virtualisierung und Simulation für die Produktion der Industrie 4.0	37
4.3.1.4. Bedeutung der zentralen Systeme	39
4.3.2. Die Durchbrechung der Automatisierungspyramide: Die Ablösung tradierter Informationsflüsse	41
4.4. Neue Dienste, neue Anwendungsfelder	42
4.5. Big Data (Massendatenverarbeitung)	44
4.6. Macht, Industrie, Daten und die besondere Rolle Chinas im IoT	46

4.6.1. Einhegung durch Märkte	47
4.6.2. Konfliktpotenzial	48
4.6.3. Konzernmacht (Abhängigkeit von Infrastruktur, Know-How)	50
4.7. Verletzlichkeit der Datenverarbeitung	53
4.8. Bedeutung der Sicherheitsmechanismen in der Industrie 4.0	57
5. Potentielle Angreifer	61
5.1. (Fremd-)Staatliche Akteure	62
5.1.1. Geostrategische Lage	62
5.1.2. Militär	67
5.1.3. Nachrichtendienste	69
5.1.4. Anbieter von Spionagesoftware	71
5.2. Nichtstaatliche Akteure	72
5.2.1. Konkurrenten	72
5.2.2. „Skript Kiddies“	73
5.2.3. Professionelle Angreifer und Angriffsdienste	74
5.2.4. Überwachungs- und Auswertungsdienste	79
5.2.5. Arbeitgeber	81
5.3. Fazit	82
6. Schutzaufgaben	83
6.1. Allgemein	83
6.2. Technische Sicherheit	84
6.3. Sicherheit durch den Staat	86
6.3.1. Theoretische und ideengeschichtliche Vorlagen staatlicher Sicherheit (Staatszweck)	86
6.3.1.1. Hobbes: Staatszweck Gewaltmonopol und Sicherheit	87
6.3.1.2. Locke: Staatszweck Freiheit vor dem Staat und Schutz des Eigentums	88
6.3.1.3. Rousseau: Staatszweck Freiheit und Widerstandspflicht	89
6.3.1.4. Kant: Freiheit als Staatszweck und Sicherheit als Mittel dazu	90
6.3.1.5. Fazit: Staatszweck Sicherheit für Freiheit und Freiheit durch Sicherheit	90
6.3.2. Verortung von Sicherheit im modernen Verfassungsstaat	91
6.3.2.1. Staatsaufgaben	92
6.3.2.2. Staatsziele	93
6.3.2.3. Strukturprinzipien	97
6.3.2.4. Grundrechte	97
6.3.2.4.1. Beschränktes Gewaltmonopol des Staates durch Grundrechtsvorrang	99
6.3.2.4.2. Sicherheit und Sicherheitsfacetten	100

6.3.2.4.3. Schutzpflichten.....	103
6.3.3. Sicherheit und Freiheit in der Informationsgesellschaft	108
6.4. Industrie 4.0-Perspektive der IT-Sicherheit	111
6.5. IT-Sicherheit durch den Staat?.....	112
6.5.1. Das „Computergrundrecht“ oder das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“	113
6.5.2. IT-Sicherheitslücken	115
6.5.3. Einfachgesetzliche Ausprägungen der IT-Sicherheit.....	116
6.6. Freiheitsschutz.....	120
6.6.1. Menschenwürde	121
6.6.2. Die freie Entfaltung der Persönlichkeit.....	121
6.6.3. Die informationelle Selbstbestimmung.....	122
6.6.4. Datenschutz und einfachgesetzliche Ausprägungen des Schutzes personenbezogener Daten	125
7. IT-Sicherheit für ein Industrie 4.0-Szenario.....	128
7.1. Kundenindividuelle Produktion: Sichere Prozesse	129
7.1.1. Produktentstehung.....	129
7.1.2. Produktionsplanung.....	130
7.1.3. Produktion	133
7.1.4. Service.....	135
7.2. Fernwartung von Produktionsanlagen: Sichere Dienste	136
7.3. Technologiedatenmarktplatz: Sichere Daten	137
7.4. Visueller Security-Leitstand: Sichere Vernetzung	139
8. IT-Sicherheitsmaßnahmen und Datenschutz in Industrie 4.0	141
8.1. Konkordanz durch Technikgestaltung	141
8.2. Methode KORA: Konkretisierung rechtlicher Anforderungen.....	142
8.3. Relevanz der nationalen und unionalen Grundrechte.....	143
9. Verfassungsrechtliche Vorgaben	148
9.1. Fundament und vitale Voraussetzung zur Grundrechtswahrnehmung	148
9.1.1. Die Würde des Menschen	148
9.1.2. Recht auf Leben (geistige) und körperliche Unversehrtheit	149
9.2. Beruf, Unternehmen und Eigentum	150
9.2.1. Beruf und Unternehmen.....	150
9.2.2. Eigentum	154
9.3. Rechtsgrundsätze und Rechtsdurchsetzung.....	158
9.3.1. Gleichheit vor dem Gesetz	158

9.3.2. Zugang zu den Gerichten und effektiver Rechtsschutz.....	159
9.3.3. Rechtliches Gehör	161
9.3.4. Verhältnismäßige Beschränkungen von Grundrechten.....	162
9.4. Selbstbestimmter (und fernvermittelter) Informationsumgang.....	163
9.4.1. Informationelle Selbstbestimmung und (Fern-)Kommunikation	164
9.4.2. Schutz der Integrität und Vertraulichkeit informationstechnischer Systeme.....	170
9.5 Chancen und Risiken für die verfassungsrechtlichen Vorgaben.....	172
9.5.1. Chancen einer it-sicheren Industrie 4.0.....	173
9.5.1.1. Fundament und vitale Voraussetzungen zur Grundrechtswahrnehmung.....	173
9.5.1.2. Beruf, Unternehmen und Eigentum	175
9.5.1.3. Rechtsgrundsätze und Rechtsdurchsetzung	179
9.5.1.4. Selbstbestimmter (und fernvermittelter) Informationsumgang.....	181
9.5.2. Risiken einer it-sicheren Industrie 4.0.....	182
9.5.2.1. Fundament und vitale Voraussetzungen zur Grundrechtswahrnehmung.....	183
9.5.2.2. Beruf, Unternehmen und Eigentum	186
9.5.2.3. Rechtsgrundsätze und Rechtsdurchsetzung	190
9.5.2.4. Selbstbestimmter (und fernvermittelter) Informationsumgang.....	191
10. Anforderungen	203
10.1. A1 Fernmeldegeheimnis.....	203
10.2. A2 Geheimnisschutz	204
10.3. A3 Datenschutz	206
10.4. A4 Schutz der Produktions- und Arbeitsmittel	206
10.5. A5 Rechtssicherheit.....	207
10.6. A6 Mitbestimmung	208
11. Kriterien	209
11.1. K1 Technik- und Organisationssicherheit.....	210
11.2. K2 Vertraulichkeit.....	214
11.3. K3 Integrität	220
11.4. K4 Verfügbarkeit.....	223
11.5. K5 Zurechnung.....	224
11.6. K6 Zweckbindung.....	228
11.7. K7 Beweisbarkeit.....	231
11.8. K8 Erforderlichkeit	236
11.9. K9 Transparenz	238
11.10. K10 Souveränität.....	241

11.11. K11 (Nicht-)Verkettbarkeit	244
12. Technische Gestaltungsziele	247
12.1. Z1 Stand der Technik	247
12.2. Z2 Konfiguration und Updatefähigkeit (Systeme).....	248
12.3. Z3 Sichere Identitäten	249
12.4. Z4 Sichere Identifizierung und Authentisierung.....	250
12.5. Z5 Sicheres Identitätsmanagement.....	252
12.6. Z6 Kryptographieeinsatz	253
12.7. Z7 Vertraulichkeitsschutz.....	253
12.8. Z8 Integritätsschutz.....	254
12.9. Z9 Aufbau einer Sicherheitsinfrastruktur.....	255
12.10. Z10 Rollen- und Rechtevergabe (Daten/Systeme).....	256
12.11. Z11 Sicherer Zutritt und Zugang (Daten/Systeme).....	256
12.12. Z12 sicherer Zugriff (Daten/Systeme)	257
12.13. Z13 Sicherheits- und Vertrauensanker (Daten/Systeme).....	258
12.14. Z14 sicheres Dokumentieren (Daten/Systeme).....	259
12.15. Z15 Systeme mit Minimalfunktionalität (Systeme)	259
12.16. Z16 Modularer, strukturierter und nachvollziehbarer Aufbau (Daten/System).....	260
12.17. Z17 Exportmöglichkeiten / Schnittstellen (Systeme).....	261
12.18. Z18 Anonyme Datenverarbeitung (Daten).....	261
12.19. Z19 Pseudonyme Datenverarbeitung (Daten)	262
12.20. Z20 Beherrschbarkeit	264
12.21. Z21 Quelloffene Soft- und Hardware (Daten/Systeme).....	265
12.22. Z22 Offene Standards (Daten)	266
12.23. Z23 Datenvermeidende und datensparsame Designs (Daten).....	266
12.24. Z24 Löschen von Daten (Daten)	266
12.25. Z25 Datenschutzmanagement	267
12.26. Z26 IT-Sicherheitsmanagement	268
12.27. Z27 Auditier- und Revisionsfähigkeit (Systeme/Daten).....	269
12.28. Z28 Resilienz.....	269
12.29. Z29 Anomalieerkennung.....	272
12.30. Z30 Trennung (Systeme/Daten)	273
13. Technische Gestaltungsvorschläge	275
13.1. Basale Vorschläge	276
13.1.1. V1 Einhaltung des Stands der Technik durch Umsetzung aktueller und einschlägiger Normen und Standards.....	276

13.1.2. V2 Bedrohungs- und Risikomodellierung.....	278
13.1.3. V3 Up-to-Date-Halten.....	280
13.1.4. V4 Nutzbarmachen von Open Source-Lösungen.....	280
13.1.5. V5 Nutzbarmachen von offenen Standards.....	281
13.1.6. V6 Separieren.....	282
13.1.7. V7 Regelmäßige Datensicherung.....	284
13.1.8. V8 Löschroutine.....	285
13.1.9. V9 Protokollierung.....	288
13.1.10. V10 Schulung.....	291
13.1.11. V11 Modularisierung.....	292
13.2. Vorschläge zur Implementierung von Elementen einer datenschutzgerechten IT-Sicherheitsinfrastruktur.....	293
13.2.1. V12 Implementierung identitätsbasierter Sicherheitsmechanismen und Identitätsmanagement.....	294
13.2.2. Vorüberlegungen zur weiteren Anknüpfung an die Identität.....	298
13.2.2.1. Umsetzung der Zugangs- und Zutritts- und Zugriffskontrolle.....	300
13.2.2.2. Umsetzung des Identity- und Accessmanagements.....	302
13.2.2.3. Pseudonymisierung und Anonymisierung.....	305
13.2.3. V13 Kryptographische Anwendungen.....	309
13.2.3.1. Vertrauliche Speicherung und Kommunikation durch Verschlüsselung....	309
13.2.3.2. Verbindliche Zuordnung, Integrität sowie Authentizität durch Signaturen	311
13.2.3.3. Asymmetrische Kryptosysteme.....	314
13.2.3.3.1. Elemente.....	314
13.2.3.3.2. Schlüsselmanagement.....	315
13.2.3.3.3. Kryptographische Prämisse.....	316
13.2.4. V14 Aufbau initialer Systemsicherheit.....	317
13.2.5. V15 Ausgestaltung von Anomalieerkennungen und Abwehrmechanismen.....	321
13.3. Vorschläge zur dauerhaften Einhaltung und zum Nachweis von Datenschutz und IT-Sicherheit.....	324
13.3.1. V16 Implementierung eines Datenschutzmanagementsystems (DSM).....	324
13.3.2. V17 Implementierung eines Informationssicherheitsmanagements (ISM).....	329
13.3.3. V18 Nachweisen der datenschutz- und it-sicherheitsrechtlichen Maßnahmen..	334
14. Schlussbetrachtung.....	338
15. Literaturverzeichnis.....	342

Abkürzungsverzeichnis

Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AK Technik	Arbeitskreis der Datenschutzkonferenz für Technik
AöR	Archiv des öffentlichen Rechts (Zeitschrift)
App	kurz für: Application, Anwendung, kleines Softwareprogramm
APP	Anwendungen, Bausteine des BSI-IT-Grundschutzes
APR	Allgemeines Persönlichkeitsrecht
APS	Advanced Planning and Scheduling, häufig integraler Teil des ERP
APuZ	Aus Politik und Zeitgeschichte (Zeitschrift)
ARPANET	Advanced Research Projects Agency Network
ArbR	Arbeitsrecht
Art.	Artikel
ASEAN	Association of Southeast Asian Nations, Verband der südostasiatischen Nationen
AtG	Atomgesetz, Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren
ATZ	Automobiltechnische Zeitschrift
A[+Zahl]	Anforderung (und dessen Nummer)
BDSG	Bundesdatenschutzgesetz, (erstes) Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung v. 1977 (später nur noch: Bundesdatenschutzgesetz)
BGB	Bürgerliches Gesetzbuch
BImSchG	Bundesimmissionsschutzgesetz
BMBF	Bundesministerium für Bildung und Forschung
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur (heute: BMDV [Bundesministerium für Digitales und Verkehr])
BMWi BSI	Bundesministerium für Wirtschaft (heute: BMWK [...und Klimaschutz]) Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSI-TR	Technische Richtlinien des BSI
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
CA	Computer Aided, computergestützte
CA	Certification Authority, Zertifizierungsstelle im Rahmen einer PKI
CAD	Computer Aided Design, computergestützte Gestaltung
CAM	Computer Aided Manufacturing, computergestützte Fertigung
CCZ	Corporate Compliance Zeitschrift

CEN	Comité Européen de Normalisation, Europäisches Komitee für Normung
CENELEC	Comité Européen de Normalisation Électrotechnique, Europäisches Komitee für elektrotechnische Normung
CIM	Computer Integrated Manufacturing, computerintegrierte Fertigung
cms-journal	Computer- und Medienservice Journal
CNC	Computerized Numerical Control, computerisierte numerische Steuerung
CON	Konzeption und Vorgehensweise, Bausteine des BSI-IT-Grundschatzes
CP	Certification Policy, Zertifikatsrichtlinie im Rahmen einer PKI
CPS	Cyber Physical Systems, Cyberphysische Systeme
CR	Computer und Recht (Zeitschrift)
CRL	Certificate Revocation List, Spreeliste für zurückgezogene Zertifikate im Rahmen einer PKI
DAR	Deutsches Autorecht (Zeitschrift)
DER	Detektion und Reaktion, Bausteine des BSI-IT-Grundschatzes
DDR	Deutsche Demokratische Republik
DDoS	Distributed Denial of Service, verteilter Dienstverweigerungsangriff
DGAP	Deutsche Gesellschaft für Auswärtige Politik
DGRI	Deutsche Gesellschaft für Recht und Informatik
d.h.	das heißt
DIN	Deutsches Institut für Normung
DSK	Datenschutzkonferenz
DSM	Datenschutzmanagementsystem
DMZ	Demilitarized Zone, demilitarisierte Zone, d.h. eine informationstechnisch gesicherte Zone im Netzwerk
DNC	Direct Numerical Control
DNS	Domain Name System, weltweites Verzeichnis zur Verwaltung des Internetraums
DoS	Denial of Service, „Verweigerung des Dienstes“ häufig als Nichterreichbarkeit aufgrund Überlastung, z.B. aufgrund von Anfrageflut als Angriff
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DSK	Datenschutzkonferenz
DSGVO	Datenschutz-Grundverordnung, 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
DSRITB	Deutsche Stiftung für Recht und Information Tagungsband
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBl.	Deutsches Verwaltungsblatt (Zeitschrift)
EDV	Elektronische Datenverarbeitung

EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
eIDAS-VO	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
EMRK	Europäische Menschenrechtskonvention
EN	Europäische Normung (betrieben durch CEN und CENELEC)
EnWG	Energiewirtschaftsgesetz, Gesetz über die Elektrizitäts- und Gasversorgung
ERP	Enterprise Resource Planning, Ressourcenplanung und Geschäftsprozesssteuerung im Unternehmen durch übergeordnetes System
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuR	Europarecht (Zeitschrift)
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
FIfF	Forum InformatikerInnen für Frieden (und gesellschaftliche Verantwortung e.V)
FS	Festschrift
FSB	Federalnaja Slushba Besopasnosti, Inlandsnachrichtendienst der Russischen Föderation
gem.	gemäß
GeschGehG	Geschäftsgeheimnisgesetz, Gesetz zum Schutz von Geschäftsgeheimnissen
GG	Grundgesetz für die Bundesrepublik Deutschland
GRCh	Grundrechtecharta, Charta der Grundrechte der Europäischen Union
GRU	Glawnoje Raswedywatelnoje Uprawlenije, Militärischer Auslandsnachrichtendienst der Russischen Föderation
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
HdB	Handbuch
HTTP	Hypertext Transfer Protocol, Übertragungsprotokoll auf der Anwendungsschicht
HTTPS	Hypertext Transfer Protocol Secure, Übertragungsprotokoll auf der Anwendungs- und Transportschicht zur sicheren Internetübertragung
IAM	Identity and Access Management, Identitäts- und Zugangsmanagement
ICANN	Internet Corporation for Assigned Names and Numbers, die für die Koordinierung und Vergabe von einmaligen Namen und Adressen im Internet ins Leben gerufene Organisation
IIoT	Industrial Internet of Things, US-Äquivalent zur Industrie 4.0
ILO	International Labour Organization, Internationale Arbeitsorganisation
IND	Industrielle IT, Bausteine des BSI-IT-Grdschutzes

INF	Infrastruktur, Bausteine des BSI-IT-Grundschutzes
IP	Internet Protocol
IPC	Industrial Personal Computer, d.h. ein PC, der in den rauen Produktionsumgebungen der Industrie(-fertigung) eingesetzt wird
i.S.d.	im Sinne des
ISMS	(Informations-)Sicherheitsmanagement, Bausteine des BSI-IT-Grundschutzes
ISO	International Organization for Standardization, Internationale Organisation für Normung
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
i.S.v.	im Sinne von
IT	Informationstechnik
IT-SiG	IT-Sicherheitsgesetz, Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme v. 17.7.2015
IoT	Internet of Things, Internet der Dinge
IuKT	Informations- und Kommunikationstechnik
i.V.m.	in Verbindung mit
JA	Juristische Arbeitsblätter (Zeitschrift)
JuS	Juristische Schulung (Zeitschrift)
JZ	Juristenzeitung (Zeitschrift)
Kap.	Kapitel
K[+Zahl]	Kriterium (und dessen Nummer)
KI	Künstliche Intelligenz
KMU	Kleine und Mittlere Unternehmen
KORA	Konkretisierung rechtlicher Anforderungen, Methode zur (interdisziplinären) rechtsverträglichen Informationstechnik-Gestaltung
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
LAN	Local Area Network, lokales Netzwerk
lit.	littera, Buchstabe
MAC	Mandatory Access Control, zwingend erforderliche Zugangskontrolle
MES	Manufacturing Execution System, Typ eines Fertigungsmanagementsystems
MMR	MMR (Zeitschrift für IT-Recht und Recht der Digitalisierung [Multimedia und Recht])
MRP	Material Resource[Requiring] Planning, Material-[Anforderungs-] bedarfsplanung
m.w.N.	mit weiteren Nachweisen
NC	Numerical Control, numerische Steuerung
NET	Netze und Kommunikation, Bausteine des BSI-IT-Grundschutzes

NIS-RL	Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
NIS-2-RL	Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1772 sowie zur Aufhebung der Richtlinie (EU) 2016/1148
NJW	Neue Juristische Wochenschrift
NZKart	Neue Zeitschrift für Kartellrecht
NZV	Neue Zeitschrift für Verkehrsrecht
OAuth	Open Authentication, Protokolltyp
OP	Operational Technology, informationstechnische Steuerung der Sensoren und Aktoren auf der Feld-/Fertigungsebene
OPC-UA	Open Platform Communication Unified Architecture
Open ID	Open Identification, Protokolltyp
PC	Personal Computer
PDA	Personal Digital Assistant, persönliche digitale Assistenz
PDCA	Plan, Do, Check, Act = planen, umsetzen, überprüfen, gemäß der Prüfung handeln ist ein typischer sich wiederholender Zyklus zur Aufrechterhaltung von z.B. Sicherheitsmaßnahmen in einem sich ständig verändernden Umfeld
PKI	Public Key Infrastructure, spezielle Infrastruktur zum Verschlüsseln
PPS	Produktionsplanung- und Steuerung
RA	Registration Authority, Registrierungsstelle im Rahmen einer PKI
RDA	Recht der Arbeit (Zeitschrift)
RFID	Radio Frequency Identification, funkfrequenzbasierte Identifikation
RiLi 95/46/EG	Richtlinie 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
s.	siehe
S.	Satz
SchiedsVZ	Zeitschrift für Schiedsverfahren
SDM	Standard Datenschutzmodell der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
SED	Sozialistische Einheitspartei Deutschlands
SPS	Speicherprogrammierbare Steuerungen
SVR	Straßenverkehrsrecht (Zeitschrift)
SWP	Stiftung Wissenschaft und Politik
SWR	Slushba Wneschnej Raswedki, Auslandsnachrichtendienst der Russischen Föderation

SYS	IT-Systeme, Bausteine des BSI-IT-Grundschutzes
TCG	Trusted Computing Group (ehemals TCPA: Trusted Computing Platform Alliance)
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security, Internetprotokoll zur Verschlüsselung auf der Transportschicht
TMG	Telemediengesetz
TOM	Technische und organisatorische Maßnahmen
TOV	Technische und organisatorische Vorkehrungen
TPM	Trusted Platform Module, häufig ein Chip als zentrales Sicherheitsmodul
TPS	Toyota Production System
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz, Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien
UAbs.	Unterabsatz
UPR	Umwelt- und Planungsrecht (Zeitschrift)
URL	Uniform Resource Locator, vereinheitlichter Quellenverortner
USA	United States of America
v.	vom
vgl.	vergleiche
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
V[+Zahl]	technischer Gestaltungsvorschlag (und dessen Nummer)
WLAN	Wireless Local Area Network, örtliches Drahtlosnetzwerk
www	world wide web
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZD-aktuell	Newsdienst der Zeitschrift für Datenschutz
ZfPW	Zeitschrift für die gesamte Privatrechtswissenschaft
ZRP	Zeitschrift für Rechtspolitik
Z[+Zahl]	technisches Gestaltungsziel (und dessen Nummer)
3D	dreidimensional
4/5/6G	umgangssprachliche Bezeichnung der entsprechenden Generation des Mobilfunks