

Nink [Hrsg.]

# Digitale Sicherheit

Governance | Recht | Technik



# NomosSTICHWORTKOMMENTAR

Dr. Judith Nink, Köln [Hrsg.]

# Digitale Sicherheit

Governance | Recht | Technik

**Andreas G. Barke**, Berater für Informationssicherheit, HiSolutions AG, Berlin | **Prof. Dr.-Ing. Patrick-Benjamin Bök**, Hochschule Rhein-Waal | **Prof. Dr. Matteo Große-Kampmann**, Hochschule Rhein-Waal | RA **Frank Ingenrieth**, LL.M., Berlin | **Ulrich Irnich**, Executive Tech Advisor, Düren | RA **Sascha Kremer**, FAIT-Recht, Köln | **Rudolf Müller**, Geschäftsführer ECKD, Kassel | **Benjamin Neweling**, Berater für Informationssicherheit, HiSolutions AG, Berlin | **Dr. Judith Nink**, Köln | **Margaretha Opalewski**, Beraterin für Informationssicherheit, HiSolutions AG, Nürnberg | RA **Dr. Carlo Piltz**, Berlin | RA **Christoph Y. Pitzer**, LL.M. oec., Köln | **Prof. Dr. Matthias Reintjes**, Hochschule Rhein-Waal | RA **Dr. Tobias Rothkegel**, Hamburg | **Philipp Christopher Rothmann**, Geschäftsführender Gesellschafter IT-Security Coach GmbH, Olpe | RA **Dr. Daniel Walter**, Köln | RA **Alexander Weiss**, Berlin | **Maximilian Wolf**, Berater für Informationssicherheit, HiSolutions AG, Berlin | RA **Dr. Julian Zaudig**, Köln | **Udo Zaudig**, Chief Information Security Officer, Stadt Köln



**Nomos**

**Zitiervorschlag:** SWK-Digitale Sicherheit/Bearbeiter [Stichwort] Rn. ...

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

ISBN 978-3-7560-3030-9

1. Auflage 2026

© Nomos Verlagsgesellschaft, Baden-Baden 2026. Gesamtverantwortung für Druck und Herstellung bei der Nomos Verlagsgesellschaft mbH & Co. KG. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten.

## Vorwort

Die EU versucht mit ihrer Cybersicherheitsstrategie und der damit verbundenen Regulierung die Resilienz der Mitgliedstaaten in allen Bereichen zu stärken und ein konstant hohes und EU-weit einheitliches Cybersicherheitsniveau zu erreichen. Der Weg dahin ist noch lang. Dies zeigen zahlreiche Studien und zuletzt der Lagebericht 2025 des BSI:

Die Bedrohungslage im digitalen Raum bleibt stabil auf hohem Niveau. Im Durchschnitt werden täglich 119 neue Schwachstellen in Deutschland und über 800 neue Phishingseiten weltweit bekannt. Die öffentliche Verwaltung ist das Hauptziel von Cyberspionage. 461 Datenleaks wurden registriert. Rund 80 % aller Cyberangriffe richten sich gegen KMU. Ransomware bleibt dabei die Top-Bedrohung im Bereich Cybercrime: 950 aller gestellten Strafanzeigen hatten Ransomwareangriffe zum Gegenstand. Während Resilienzmaßnahmen im Bereich der Kritischen Infrastrukturen mehr und mehr Wirkung entfalten, sind Maßnahmen zur Stärkung der Cybersicherheit bei KMU überwiegend nicht oder nur unzureichend vorhanden.

Digitale Sicherheit, die dafür notwendige Resilienz bei Wirtschaft und staatlichen Einrichtungen sowie informierte und aufgeklärte Bürgerinnen und Bürgern sind eine Gemeinschaftsaufgabe, die kein Akteur allein stemmen kann. Gleiches gilt für diesen Stichwortkommentar: Er soll einen einfachen Überblick über die wichtigen Themen der digitalen Sicherheit sowohl aus technischer und rechtlicher als auch wissenschaftlicher und praktischer Perspektive geben. Damit dies gelingen kann, ist eine ganzheitliche Betrachtung des Themengebiets der digitalen Sicherheit durch ein interdisziplinäres Autorenteam unerlässlich. Seine konkreten Umsetzungsempfehlungen, Hinweise, Beispiele und Checklisten sollen den Lesern helfen, einen niedrigschwelligen Einstieg in die Querschnittsmaterie zu erhalten.

Nach einem guten Jahr intensiver Arbeit aller Beteiligten, inklusive regelmäßiger Updates aufgrund von gesetzgeberischen Entwicklungen, wie etwa der lang erwarteten Umsetzung der NIS-2-Richtlinie, haben wir das Ziel erreicht. Sicher werden wir in den künftigen Aktualisierungen weitere Stichwörter ergänzen – die ersten sind bereits notiert – und die Schwerpunkte je nach Entwicklung der Cybersicherheitslage anpassen. Ich freue mich bereits jetzt auf die Weiterentwicklung und den Ausbau des Werks.

Mein herzlicher Dank gilt den Autorinnen und Autoren, die viel Engagement, Disziplin und Ideen in die Manuskripte gesteckt haben, sich teils auf interdisziplinäre Ko-Autorenschaften eingelassen haben, ohne einander aus einer vorherigen Zusammenarbeit zu kennen. An dieser Stelle möchte ich auch Dr. Marco Ganzhorn und seinem Team danken, die die Werksentstehung von der Idee bis zur Veröffentlichung stets pragmatisch und konstruktiv begleitet haben.

Januar 2026

*Judith Nink*

## Inhaltsverzeichnis

Vorwort .....	5
Autorinnen und Autoren .....	9
Abkürzungsverzeichnis .....	13
1. Anonymisierung .....	25
2. Audits und Zertifizierungen, allgemein .....	50
3. Audits und Zertifizierungen, Dokumentation .....	63
4. Audits und Zertifizierungen, Vorbereitung .....	65
5. Aufsicht .....	67
6. Authentizität .....	76
7. Bedrohungsszenarien .....	79
8. Behörden, allgemein .....	91
9. Behörden, Befugnisse .....	99
10. Business-Continuity-Management (BCM) .....	106
11. Cyberkriminalität .....	115
12. Cybersicherheit .....	132
13. Data Protection by Design .....	142
14. Datenschutzmanagementsystem .....	152
15. Datenverschlüsselung .....	155
16. Dienstleister, allgemein .....	159
17. Dienstleister, Checkliste Sicherheitsprüfung externe Dienstleister .....	169
18. Dienstleister, Checkliste Auftragsverarbeitung .....	174
19. DORA und finanzaufsichtsrechtliche Auslagerung .....	177
20. Haftung .....	193
21. Informationssicherheit .....	206
22. Informationssicherheitsmanagementsystem (ISMS) .....	218
23. Ko-Regulierung .....	228
24. KRITIS .....	240
25. Künstliche Intelligenz .....	252
26. Löschen .....	269
27. Outsourcing .....	277
28. Privacy by Design .....	288
29. Produktsicherheit .....	295
30. Pseudonymisierung .....	304
31. Resilienz .....	320
32. Risikomanagement .....	325
33. Schutzziele .....	340
34. Security by Design .....	344
35. Sicherheitsbeauftragter .....	357
36. Sicherheitsbewusstsein .....	371
37. Sicherheitsvorfall, allgemein .....	384

## Inhaltsverzeichnis

---

38. Sicherheitsvorfall, Bearbeitung .....	406
39. Sicherheitsvorfall, Prävention .....	420
40. Technische und organisatorische Maßnahmen (TOM) .....	446
41. Verantwortlichkeit: Anwender .....	450
42. Versicherungsschutz .....	467
43. Werbung .....	475
44. Zertifizierung .....	483
Stichwortverzeichnis .....	493

## Autorinnen und Autoren

*Andreas G. Barke*

Berater für Informationssicherheit, HiSolutions AG,  
Berlin

Sicherheitsvorfall, Prävention  
(mit *Wolf*)

*Prof. Dr.-Ing. Patrick-Benjamin Bök*

Hochschule Rhein-Waal

Behörden, allgemein – Behörden, Befugnisse  
(mit *Große-Kampmann/Reintjes*)

*Prof. Dr. Matteo Große-Kampmann*

Hochschule Rhein-Waal

Behörden, allgemein – Behörden, Befugnisse  
(mit *Bök/Reintjes*)

Werbung  
(mit *Nink*)

*Frank Ingenrieth, LL.M.*

Rechtsanwalt, Berlin

Anonymisierung – Ko-Regulierung –  
Pseudonymisierung – Zertifizierung

*Ulrich Irnich*

Executive Tech Advisor, Düren

Bedrohungsszenarien – Security by Design  
– Sicherheitsbewusstsein

*Sascha Kremer*

Rechtsanwalt, Fachanwalt für IT-Recht, Köln

Löschen

*Rudolf Müller*

Geschäftsführer ECKD, Kassel

Künstliche Intelligenz  
(mit *Pitzer*)

Resilienz  
(mit *Rothmann*)

*Benjamin Neweling*

Berater für Informationssicherheit, HiSolutions AG,  
Berlin

Business-Continuity-Management (BCM)  
Informationssicherheitsmanagementsystem  
(ISMS)  
(mit *Opalewski*)

*Dr. Judith Nink*

Köln

Aufsicht – Versicherungsschutz

Cybersicherheit  
(mit *Rothmann*)

Dienstleister, allgemein  
(mit *U. Zaudig*)

Werbung  
(mit *Große-Kampmann*)

## Autorinnen und Autoren

---

<i>Margaretha Opalewski</i> Beraterin für Informationssicherheit, HiSolutions AG, Nürnberg	Informationssicherheitsmanagementsystem (ISMS) (mit <i>Neweling</i> )
<i>Dr. Carlo Piltz</i> Rechtsanwalt, Berlin	Cyberkriminalität – Data Protection by Design – Privacy by Design (mit <i>Weiss</i> )
<i>Christoph Y. Pitzer, LL.M. oec.</i> Rechtsanwalt, Köln	Produktsicherheit Künstliche Intelligenz (mit <i>Müller</i> )
<i>Prof. Dr. Matthias Reintjes</i> Hochschule-Rhein-Waal	Behörden, allgemein – Behörden, Befugnisse (mit <i>Bök/Große-Kampmann</i> )
<i>Dr. Tobias Rothkegel</i> Rechtsanwalt, Hamburg	Outsourcing – Sicherheitsvorfall, allgemein – Sicherheitsvorfall, Bearbeitung DORA und finanzaufsichtsrechtliche Auslagerung (mit <i>Walter</i> )
<i>Philipp Christopher Rothmann</i> Geschäftsführender Gesellschafter IT-Security Coach GmbH, Olpe	Authentizität – Datenschutzmanagementsystem – Datenverschlüsselung – Schutzziele – Technische und organisatorische Maßnahmen (TOM) Cybersicherheit (mit <i>Nink</i> ) Resilienz (mit <i>Müller</i> ) Sicherheitsbeauftragter (mit <i>J. Zaudig</i> )
<i>Dr. Daniel Walter</i> Rechtsanwalt, Köln	DORA und finanzaufsichtsrechtliche Auslagerung (mit <i>Rothkegel</i> )
<i>Alexander Weiss</i> Rechtsanwalt, Berlin	Cyberkriminalität – Data Protection by Design – Privacy by Design (mit <i>Piltz</i> )

*Maximilian Wolf*

Berater für Informationssicherheit, HiSolutions AG,  
Berlin

Sicherheitsvorfall, Prävention  
(mit *Barke*)

*Dr. Julian Zaudig*

Rechtsanwalt, Köln

Haftung – KRITIS – Risikomanagement –  
Verantwortlichkeit: Anwender

Sicherheitsbeauftragter  
(mit *Rothmann*)

*Udo Zaudig*

Chief Information Security Officer, Stadt Köln

Audits und Zertifizierungen, allgemein –  
Audits und Zertifizierungen, Dokumenta-  
tion – Audits und Zertifizierungen, Vor-  
bereitung – Dienstleister, Checkliste Si-  
cherheitsprüfung externe Dienstleister –  
Dienstleister, Checkliste Auftragsverarbei-  
tung – Informationssicherheit

Dienstleister, allgemein  
(mit *Nink*)

# 1. Anonymisierung

Frank Ingenrieth

<b>I. Begriffsbestimmung / Einleitung</b> .....	1	<b>V. Risikoanalyse und Risikomitigation</b> .....	51
1. Begriffsbestimmung .....	1	1. Risikogruppen .....	51
2. Einleitung .....	8	2. Mitigationmethoden .....	52
<b>II. Abgrenzung Pseudonym</b> .....	15	3. Angreifermodell (motivated intruder test) ...	61
<b>III. Wechselwirkung Pseudonym und Anonym</b> ...	21	<b>VI. Anonyme in rechtlichen Kontexten</b> .....	64
<b>IV. Anonymisierungsverfahren und Quasi-Identifikatoren</b> .....	24	1. Datenschutzrecht .....	64
1. Vorüberlegungen/Auswahl des passenden Anonymisierungsverfahrens .....	24	a) Anonyme als (freiwillige) Datenminimierung .....	75
2. Unterschiedliche Anonymisierungsverfahren .....	26	b) Anonyme als notwendige Speicherlimitierung sowie als Umsetzung des Rechts auf Vergessenwerden .....	78
a) Generalisierung .....	27	2. NIS-2-Richtlinie .....	85
b) Randomisierung .....	34	3. EHDS und Gesundheitsforschung im Allgemeinen .....	87
3. Sonderfälle Differential Privacy und Maskierung (Masking) .....	41	4. Anonyme Attributverifikation – zB Altersverifikationssysteme, eIDAS .....	92
4. Anonymauflösung/Quasi-Identifikatoren ...	44		
5. Synthetische Daten .....	50		

## Literatur:

BfDI, Positionspapier zur Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK-Branche, 2020; Britische Datenschutzaufsicht (ICO), Guidance, kontinuierlich aktualisierte Website; CNIL, Sous-traitants : la réutilisation de données confiées par un responsable de traitement, 2022; EDPB-Guidelines (Draft) 01/2025; EDPS, Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research, EDPS/2019/02–08, August 2021; ENISA, Data Pseudonymisation: Advanced Techniques and Use Cases, Januar 2021; European Medicines Agency (EMA), Policy 0070 on publication of clinical data for medicinal products for human use, EMA/144064/2019, 2019, v.1.5; Hornung/Wagner, Anonymisierung als datenschutzrelevante Verarbeitung, ZD 2020, 223; Ingenrieth, Opportunities to reduce bureaucracy under GDPR after CJEU in EDPS v. SRB (C-413/23 P) – Transparency Obligations of Controllers and the Qualification As Personal Data, Computer Law Review International, 2026, Dok.-Nr. CRI0087818 (zitiert als Ingenrieth, Opportunities to reduce bureaucracy under GDPR after CJEU in EDPS v. SRB, CRI, 2026); Irische Datenschutzaufsicht, Guidance on Anonymisation and Pseudonymisation, 2019; ISB1523 Amd 20/2010, Anonymisation Standard for Publishing Health and Social Care Data Specification, v1.0, 2013; ISB1523 Amd 20/2010, Anonymisation Standard for Publishing Health and Social Care Data Specification, v1.0, 2013; Sweeney, k-anonymity: a model for protecting privacy, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002, 557; Laue/Nink/Kremer, European Data Protection Law in Practice, 2025 (zitiert als Laue/Nink/Kremer EDPL); LfDI Baden-Württemberg, Diskussionspapier, Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, v2.0, 2024; Machanavajjhala/Kifer/Gehrke/Venkatasubramaniam,  $\ell$ -Diversity: Privacy Beyond K-Anonymity, 2007 IEEE 23rd International Conference on Data Engineering, Istanbul, Turkey, 2007, S. 106; NIST-Guidelines SP 800–226, März 2025; Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie, Berufsverband der Datenschutzbeauftragten Deutschlands, Bundesverband Gesundheits-IT, Arbeitsgruppe „Datenschutz & IT-Sicherheit“, Praxishilfe zur Anonymisierung/Pseudonymisierung, 2024; Stiftung Datenschutz, Praxisleitfaden zum Anonymisieren personenbezogener Daten, 2022; Roßnagel, Datenlöschung und Anonymisierung, ZD 2021, 188; Spanische Datenschutzaufsicht (AEPD), Anonymity as a Privacy Measure, 2019; Truta/Vinay, Privacy Protection: p-Sensitive k-Anonymity Property, IEEE Computer Society, 2006, 94; WP29, Opinion 05/2014, Anonymisierungsverfahren, 2014.

## I. Begriffsbestimmung / Einleitung

### 1. Begriffsbestimmung

**Anonymisierung** beschreibt den Vorgang der Erzeugung von Anonymen.<sup>1</sup>

1

1 Richtlinie (EU) 2019/1024 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-RL) beinhaltet eine Legaldefinition, wobei eine generelle Übertragung auf alle Rechtsgebiete nicht notwendiger-

## 1 Anonymisierung

---

- 2 **Anonyme** sind Identifikatoren zu einer oder mehreren Informationen, ohne im Rechtssinne einen Rückschluss auf eine konkrete Sache oder Person zu ermöglichen.
- 3 **Anonyme Daten** sind die Gesamtheit der weiteren Informationen (Attribute), die einem Anonym zugeordnet sind. Je nach Komplexität können dem identischen Anonym mehrere Datensätze anonymen Daten zugeordnet sein, entweder durch Parallelisierung, Verkettung oder eine diesbezügliche Kombination.
- 4 **Anonymauflösung** betrifft den Umstand, dass ein Anonym, ganz gleich aufgrund welcher Umstände, einer konkreten Sache oder Person zugeordnet wird. Die durch das Anonym zuvor geschützte (Original-)Information wird somit zugänglich, es liegt kein Anonym mehr vor. Etwaige mit dem Anonym verbundene Attribute können somit auch der (Original-)Information zugeführt werden und stellen somit keine anonymen Daten mehr dar. Attribute können in diesem Falle (nachträglich) ergänzt oder aktualisiert werden.
- 5 Anonyme werden in **unterschiedlichen Kontexten** genutzt. Das Anonym kann **verschiedenartigen Schutzzwecken** dienen. Anonyme können dabei a) das Objekt schützen, über das Attribute abgelegt werden, oder b) die Person schützen, die Informationen ablegt bzw. veröffentlicht.
- 6 Je nach Verwendungskontext kann **jede Information** anonymisiert werden. Dies kann etwa eine Person oder Sache sein.
- 7 Die Verwendung von Anonymen kann **freiwillig** erfolgen, eine **Folge gesetzlicher Verpflichtungen** sein oder eine Möglichkeit, die **Anwendbarkeit bestimmter gesetzlicher Normen zu vermeiden**. Im Nachfolgenden liegt der Fokus auf den wesentlichen Umständen, in denen die Anonymisierung oder die Verwendung von Anonymen gesetzlich vorgeschrieben bzw. jedenfalls angeraten ist oder die Anwendbarkeit von gesetzlichen Normen vermeiden kann.

### 2. Einleitung

- 8 Anonyme und Anonymisierung sind geeignet, sowohl komplexe wie auch leichtgewichtige Konzepte zur **Förderung und Wahrung der Sicherheit und Integrität** zu verwirklichen. Der durch die Anonymisierung resultierende Schutzgrad kann sowohl aufgrund technischer Maßnahmen als auch rein organisatorischer Maßnahmen positiv beeinflusst werden.
- 9 Während die jeweiligen Maßnahmen grundsätzlich unterschieden werden können, erfordert eine effektive Anonymisierung stets das **Zusammenspiel beider Komponenten**, also technischer und organisatorischer Maßnahmen.
- 10 **Organisatorische Elemente** betreffen etwa die Festlegung der Zuständigkeiten, der erforderlichen Zugriffsberechtigungen und Zugriffsbeschränkungen, der Verfahrensrevision, der durch die Anonymisierung intendierten (Schutz-)Zwecke.
- 11 **Technische Elemente** betreffen Aspekte, inwieweit Anonyme erstellt werden, etwa durch kryptografische Verfahren, die Separierung von Datensätzen, Aggregation, technische Konzepte zur Ermöglichung oder Vermeidung nachträglicher Verschmelzung und/oder Verkettung von Datensätzen, technische Konzepte zur Durchsetzung von Rollen- und Zugriffskonzepten etc.
- 12 Terminologisch ist darauf hinzuweisen, dass „**kryptografische Verfahren**“ nicht gleichzusetzen sind mit einer „Verschlüsselung“ bzw. „Encryption“ (→ Datenverschlüsselung Rn. 2 ff.). Die Verschlüsse-

---

weise statthaft ist. Das in dieser Kommentierung zugrunde gelegte Verständnis erscheint jedoch mit der dortigen Definition kompatibel, siehe Art. 2 Abs. 7 PSI-RL.

lung von Daten stellt eine Variante der kryptografischen Verfahren dar. Zudem ist darauf hinzuweisen, dass die isolierte Anwendung kryptografischer Verfahren, insbesondere eine bloße Verschlüsselung, nicht unmittelbar zu anonymen Daten führt. Eine Verschlüsselung integriert konzeptionell die Entschlüsselung. Auch ein Vernichten des Verschlüsselungs-Keys führt nicht als solches zu einer Anonymität der verschlüsselten Informationen.<sup>2</sup>

Gegenstand der Betrachtung sind die anonymen Daten im Kontext derjenigen, die Zugriff auf die (anonymen) Datensätze haben. Besteht Zugriff sowohl auf die Anonyme als auch auf weitere Informationen, die eine **Anonymauflösung ermöglichen** könnten, sind etwaige Schutzziele, zB aus dem Datenschutz oder der IT-Sicherheit, möglicherweise nicht erreichbar. Insbesondere lägen in diesem Fall – im Rechtssinne – vermutlich überhaupt keine anonymen Daten, sondern **allenfalls pseudonyme Daten** vor. 13

Es existiert eine Reihe von (behördlichen) Leitfäden, Stellungnahmen und Standards im Bereich der Anonymisierung. In weiten Teilen ähneln sich die Darstellungen; Abweichungen scheinen eher sprachlicher Stilistik oder zielgruppenorientierter Verallgemeinerung und Granularität geschuldet. Die nachstehende Liste erhebt keinen Anspruch auf Vollständigkeit, erleichtert aber den Zugang für die eigene, intensive Beschäftigung mit der Thematik. 14

- Wissenschaftliche (Überblicks-)Arbeiten
  - k-anonymity: a model for protecting privacy<sup>3</sup>
  - Privacy Protection: p-Sensitive k-Anonymity Property<sup>4</sup>
  - $\ell$ -Diversity: Privacy Beyond K-Anonymity<sup>5</sup>
  - Praxisleitfaden zum Anonymisieren personenbezogener Daten, Stiftung Datenschutz<sup>6</sup>
  - Praxishilfe zur Anonymisierung/Pseudonymisierung, Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie<sup>7</sup>
- Behördliche Leitfäden und Stellungnahmen
  - Opinion 05/2014 der Artikel-29-Gruppe
  - Joint Document der Spanischen Datenschutzaufsichtsbehörde und des Europäischen Datenschutzbeauftragten zu zehn Missverständnissen im Kontext der Anonymisierung<sup>8</sup>
  - Technische Leitlinie der Spanischen Datenschutzaufsicht im Bereich K-Anonymity<sup>9</sup>

2 Siehe auch Joint Document der Spanischen Datenschutzaufsichtsbehörde und des Europäischen Datenschutzbeauftragten zu zehn Missverständnissen im Kontext der Anonymisierung, 2021, [https://www.edps.europa.eu/system/files/2021-04/21-04-27\\_aepd-edps\\_anonymisation\\_en\\_5.pdf](https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf).

3 Sweeney, k-anonymity: a model for protecting privacy, 2002, <https://dataprivacylab.org/projects/kanonymity/kanonymity.pdf>.

4 Truta/Vinay, Privacy Protection: p-Sensitive k-Anonymity Property, 2006, [https://www.researchgate.net/publication/4238176\\_Privacy\\_Protection\\_p-Sensitive\\_k-Anonymity\\_Property](https://www.researchgate.net/publication/4238176_Privacy_Protection_p-Sensitive_k-Anonymity_Property).

5 Machanavajjhala/Kifer/Gehrke/Venkatasubramaniam,  $\ell$ -Diversity: Privacy Beyond K-Anonymity, 2007, <https://www.cs.rochester.edu/u/muthuv/ldiversity-TKDD.pdf>.

6 Praxisleitfaden zum Anonymisieren personenbezogener Daten, Stiftung Datenschutz, 2022, [https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Anonymisierung\\_personenbezogener\\_Daten/SDS\\_Studie\\_Praxisleitfaden-Anonymisieren-Web\\_01.pdf](https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Anonymisierung_personenbezogener_Daten/SDS_Studie_Praxisleitfaden-Anonymisieren-Web_01.pdf).

7 Praxishilfe zur Anonymisierung/Pseudonymisierung, Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie, Berufsverband der Datenschutzbeauftragten Deutschlands, Bundesverband Gesundheits-IT Arbeitsgruppe „Datenschutz & IT-Sicherheit“, [https://gesundheitsdatenschutz.org/download/praxishilfe\\_anonymisierung\\_pseudonymisierung\\_2024.pdf](https://gesundheitsdatenschutz.org/download/praxishilfe_anonymisierung_pseudonymisierung_2024.pdf).

8 Joint Document der Spanischen Datenschutzaufsichtsbehörde und des Europäischen Datenschutzbeauftragten zu zehn Missverständnissen im Kontext der Anonymisierung, 2021, [https://www.edps.europa.eu/system/files/2021-04/21-04-27\\_aepd-edps\\_anonymisation\\_en\\_5.pdf](https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf).

9 Spanische Datenschutzaufsicht (AEPD), Anonymity as a Privacy Measure, 2019, <https://www.aepd.es/guides/k-anonymity-as-a-privacy-measure.pdf>.

## 1 Anonymisierung

- Guidance on Anonymisation and Pseudonymisation der irischen Datenschutzaufsicht<sup>10</sup>
- Guidance der Britischen Datenschutzaufsicht<sup>11</sup>
- European Medicines Agency policy on publication of clinical data for medicinal products for human use<sup>12</sup>
- Guidance der European Medicines Agency, EMA/90915/2016<sup>13</sup>
- Britischer Standard zur Anonymisierung bei der Veröffentlichung von Informationen des NHS<sup>14</sup>
- NIST-Guidelines SP 800–226, Guidelines for Evaluating Differential Privacy Guarantees<sup>15</sup>
- Deutsche Datenschutzbehörde (BfDI), Positionspapier zur Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK-Branche<sup>16</sup>
- LfDI Baden-Württemberg, Diskussionspapier, Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, v2.0<sup>17</sup>
- EDPS, Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research<sup>18</sup>

### II. Abgrenzung Pseudonym

- 15 **Anonyme und Pseudonyme** sind zwar einerseits sehr ähnlich, andererseits weisen beide Konzepte signifikante Unterschiede auf (zur Abgrenzung auch → Pseudonymisierung Rn. 18 ff.). Diese Unterschiede betreffen den absoluten Kern des Zwecks: **Pseudonymen** ist eine Reversibilität inhärent, sprich, die Möglichkeit einer Wiederherstellung oder Rückbeziehung auf die (Original-)Informationen ist konzeptionell ausdrücklich erwünscht.
- 16 **Anonyme Daten** – im strengen Wortsinne – verhindern die Identifikation der (Original-)Informationen bzw. des zugrunde liegenden Bezugspunkts des Anonyms. Eine Anonymauflösung ist konzeptionell unmöglich – im Rechtssinne. Die Einschränkung im Rechtssinne ist notwendig, da es nicht

10 Irische Datenschutzaufsicht, Guidance on Anonymisation and Pseudonymisation, 2019, <https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf>.

11 Ausgestaltet als Website mit mehreren relevanten Unterseiten, Britische Datenschutzaufsicht (ICO), <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/introduction-to-anonymisation/> oder <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/how-do-we-en-sure-anonymisation-is-effective>.

12 European Medicines Agency (EMA), Policy 0070 on publication of clinical data for medicinal products for human use, EMA/144064/2019, 2019, [https://www.ema.europa.eu/en/documents/other/policy-70-european-medicines-agency-policy-publication-clinical-data-medicinal-products-human-use\\_en.pdf](https://www.ema.europa.eu/en/documents/other/policy-70-european-medicines-agency-policy-publication-clinical-data-medicinal-products-human-use_en.pdf).

13 European Medicines Agency (EMA), External guidance on the implementation of the European Medicines Agency Policy 0070 on the publication of clinical data for medicinal products for human use, EMA/90915/2016 in der zuletzt aktualisierten Version 1.5, Mai 2025, [https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/external-guidance-implementation-european-medicines-agency-policy-publication-clinical-data-medicinal-products-human-use-version-15\\_en.pdf](https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/external-guidance-implementation-european-medicines-agency-policy-publication-clinical-data-medicinal-products-human-use-version-15_en.pdf).

14 ISB1523 Amd 20/2010, Anonymisation Standard for Publishing Health and Social Care Data Specification, v. 1.0, 21.2.2013, <https://digital.nhs.uk/binaries/content/assets/website-assets/isce/isb1523/1523202010spec.pdf>.

15 NIST-Guidelines SP 800–226, in der aktuellen Version März 2025, <https://doi.org/10.6028/NIST.SP.800-226>.

16 BfDI, Positionspapier zur Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK-Branche, 29.6.2020, [https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1\\_Anonymisierung/Positionspapier-Anonymisierung.pdf](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf), BfDI.

17 LfDI Baden-Württemberg, Diskussionspapier, Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, v2.0, 17.10.2024, <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/10/Rechtsgrundlagen-KI-v2.0.pdf>, Kapitel X Ziffer 2.

18 EDPS, Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research, EDPS/2019/02–08, August 2021, [https://www.edpb.europa.eu/system/files/2022-01/legalstudy\\_on\\_the\\_appropriate\\_safeguards\\_89.1.pdf](https://www.edpb.europa.eu/system/files/2022-01/legalstudy_on_the_appropriate_safeguards_89.1.pdf). Zwar beschäftigt sich die Studie nicht ausdrücklich mit den Anforderungen an oder der Umsetzung von Anonymisierung. Sie bietet aber einen weiten Überblick über etwaige spezial- und nationalgesetzliche Regelungen, die auf das Konzept der Anonymisierung abstellen.

auf eine absolute Unmöglichkeit ankommen kann<sup>19</sup> (siehe auch vertiefend → Pseudonymisierung Rn. 25 ff.). Diese wäre – unter Heranziehung aller heutzutage theoretisch existierenden Ressourcen – höchstwahrscheinlich nicht mehr zu erreichen. Vielmehr ist auf eine relative Unmöglichkeit abzustellen (siehe auch → Pseudonymisierung Rn. 23 ff.).

Anonymität als **Mischverständnis aus technischer und rechtlicher Würdigung** wird auch in Zukunft bestehen bleiben. Während Positivumstände (identifiziert oder identifizierbar) klar umschrieben und verifiziert werden können, sind demgegenüber Negativumstände schwerlich nachzuweisen bzw. messbar zu machen. Begriff der Anonymität als Antonym zum Personenbezug ist ein solcher Negativumstand.<sup>20</sup> Konzeptionelle Grenzwerte hinsichtlich anonymer Daten werden Abwägungsentscheidungen aus unterschiedlichen Disziplinen sein. Hierzu wird möglicherweise ein – standardisiert quantifizierbares – Risiko der Anonymauflösung<sup>21</sup> gehören sowie andere (Risiko-)Faktoren, möglicherweise bezüglich der potenziellen Verkettungspotenziale. Es ist zu erwarten, dass im Wesentlichen zwei Aspekte die finale Würdigung künftig beeinflussen:

- leicht verfügbare technische Rechenkapazitäten und
- die Existenz (il-)legaler, durchsuchbarer Datensätze.

Es ist davon auszugehen, dass künftig **verfügbare durchsuchbare Datensätze** signifikant ansteigen werden. Einerseits, da bisher unsortierte Datensätze mit Hilfe von Künstlicher Intelligenz mit vertretbarem Aufwand aufbereitet werden können. Andererseits, da auch in Zukunft mit der Veröffentlichung größerer Datenbanken zu rechnen ist; entweder als Folge eines Datenschutz- oder Datensicherheitsvorfalls oder schlicht aufgrund veränderter Verhaltensweisen und verstärkter, freiwilliger Veröffentlichung einst privater Informationen.

Andererseits ist davon auszugehen, dass die **leicht verfügbaren Rechenkapazitäten** ebenso signifikant steigen werden. Dies kann einerseits die Kapazität in Stand-alone-Systemen betreffen; hier ist neben dem allgemeinen Fortschritt auf die künftige Nutzbarmachung von Quantencomputing hinzuweisen. Andererseits ist davon auszugehen, dass die Rechenkapazitäten in Form vernetzter Ressourcen anwachsen werden; etwa als Weiterentwicklung der Ressourcenoptimierung in Business-

19 Diese Auslegung stützt etwa Erwägungsgrund 26 DS-GVO. Dort heißt es unter anderem „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.“ Ergänzend auch der EuGH in seinem Urteil v. 9.10.2016, C-582/14 Rn. 46, <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62014CJ0582>: „[...] die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar wäre, zB weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, sodass das Risiko einer Identifizierung de facto vernachlässigbar erschiene.“ Zwar erfolgt die Rechtsprechung noch unter Anwendung der Datenschutzrichtlinie 95/46; diese Wertung sollte aber, insbesondere vor dem Hintergrund des Erwägungsgrunds 26 DS-GVO, auf die DS-GVO übertragbar sein. Siehe auch Joint Document der Spanischen Datenschutzaufsichtsbehörde und des Europäischen Datenschutzbeauftragten zu zehn Missverständnissen im Kontext der Anonymisierung, 2021, [https://www.edps.europa.eu/system/files/2021-04/21-04-27\\_aepd-edps\\_anonymisation\\_en\\_5.pdf](https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf).

20 So auch Roßnagel ZD 2021, 188 ff., Abschnitt III Abs. 1 mwN.

21 Siehe auch Joint Document der Spanischen Datenschutzaufsichtsbehörde und des Europäischen Datenschutzbeauftragten zu zehn Missverständnissen im Kontext der Anonymisierung, 2021, [https://www.edps.europa.eu/system/files/2021-04/21-04-27\\_aepd-edps\\_anonymisation\\_en\\_5.pdf](https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf), Ziffer 6. Dort wird auf ein quantifizierbares Risiko der Anonymauflösung abgestellt.

## 1 Anonymisierung

---

at-Scale-Konzepten, oder etwa auch in Form etwaiger Second-Life Use-Cases künftig ausgedienter Hardware.<sup>22</sup>

- 20 In der Praxis zielen Anonyme meist darauf ab, die Identifikation natürlicher und juristischer Personen, ggf. einzelner Sachen (Produkte), zu verhindern. Technisch besteht indessen keine Notwendigkeit, das Konzept anonymer Daten derart zu beschränken. Im Weiteren wird sich auf die **Anonymität von Personen** beschränkt. Die Überlegungen können in der Regel auf andere Sachverhalte übertragen werden.

### III. Wechselwirkung Pseudonym und Anonym

- 21 Pseudonyme und Anonyme sind sehr ähnliche Konzepte. Es kann je Verarbeitungskontext und Zugriffsprofil durchaus vorkommen, dass **die gleichen Daten für eine verarbeitende Stelle A anonym** sind, für eine andere verarbeitende **Stelle B** aber lediglich **pseudonym** (siehe auch → Pseudonymisierung Rn. 22 ff.).
- 22 Wird eine **Unterscheidung der Relativität je nach verarbeitender Stelle** vorgenommen, gilt es zu beachten, dass es sich hierbei um grundsätzlich verschiedene verarbeitende Stellen handeln muss.<sup>23</sup> In einer Konstellation, in der ein Unternehmen personenbeziehbare Daten erhoben hat, diese anonymisiert, ohne die Originaldaten zu löschen, bleiben auch die anonymisierten Daten personenbeziehbar, da es sich für das Unternehmen (aufgrund der möglichen Reversion) allenfalls um Pseudonyme handelt. Dies gilt – nach Maßgabe der Aufsichtsbehörden – auch wenn etwaige (Unter-)Abteilungen des Unternehmens im Anschluss ausschließlich Zugriff auf die anonymisierten Daten erhalten.<sup>24</sup> Die Aufwände einer Anonymisierung können dennoch vorteilhaft sein. Da es sich für diese Abteilung um ein sehr starkes Pseudonym handeln dürfte, erscheint es vertretbar, dies im Rahmen der **Risiko- und Interessenabwägung** besonders positiv zu berücksichtigen.
- 23 Die **Risiko- und Interessenabwägung** ist ein essenzieller Bestandteil der datenschutzrechtlichen Bewertung. Sie inkludiert mehrere Aspekte, reflektiert datenschutzrechtliche Grundprinzipien und ist

---

22 Alleine im Jahr 2024 belief sich der Verkauf von Smartphones auf über 1,2 Milliarden Geräte, bei einem beständigen jährlichen Zuwachs, siehe IDC Press Release, 13.1.2025, <https://my.idc.com/getdoc.jsp?containerId=prUS53072325>. Hinzu kommt die jährliche Rechenkapazität, die durch verkaufte Laptops, Wearables und Smart Devices entsteht.

23 Exemplarisch Irische Datenschutzaufsicht, Guidance on Anonymisation and Pseudonymisation, 2019, <https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf>, S. 5 f. Dort heißt, ein Personenbezug bliebe bestehen, wenn nach der Anonymisierung die Informationen zur Anonymauflösung in der Verfügungsgewalt der verantwortlichen Stelle verblieben – „while in the hands of the data controller“. Im Umkehrschluss bedeutet dies, dass der Personenbezug entfällt, wenn die anonymen Daten – ohne die für die Anonymauflösung erforderlichen Informationen – an eine andere verantwortliche Stelle übergeben werden.

24 Bei besonders ausgefeilten technisch-organisatorischen Maßnahmen, auch unter Verwendung von Zugriffs- und Rollenkonzepten, und bei besonders engem Verständnis des Begriffs eines Verantwortlichen, könnte auch vertreten werden, dass es sich bei mehreren Abteilungen um jeweils gesonderte Verantwortliche handelt und insoweit die (Unter-)Abteilung rein anonyme Daten verarbeitet. Einer solchen Ansicht läge zugrunde, dass es nicht ausschließlich auf die formaljuristische Ausgestaltung ankommen könne. Wäre die bloße gesellschaftsrechtliche Ausgestaltung maßgebend, könnte es genügen, eine Tochtergesellschaft bei vollständiger Weisungsgebundenheit und Identität der Mitarbeitenden auszugründen. Wenn einerseits aufgrund der Personalidentität und Weisungsgebundenheit trotz formaljuristischer Trennung eine Zurechnung erfolgen würde, so müssten im Umkehrschluss auch die Privilegierungen Anwendung finden, wenn tatsächlich eine hinreichende technisch-organisatorische Trennung – mit Ausnahme der formaljuristischen Ausgliederung – implementiert wurde. Hierzu finden sich auch Anknüpfungspunkte in Veröffentlichungen der Aufsichtsbehörden, etwa Irische Datenschutzaufsicht, Guidance on Anonymisation and Pseudonymisation, 2019, <https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf>, S. 5 f. Dort heißt es „while in the hands of the data controller, unless the anonymisation process would prevent the singling out of an individual data subject, even to someone in possession of the source data“. Hierdurch wird konzeptionell die Tür geöffnet, dass es weniger auf die formelle Trennung, sondern vielmehr auf die Effektivität der Schutzkonzepte ankommen müsse.

auch mehrmalig ausdrücklich in der DS-GVO erwähnt; etwa Art. 24 Abs. 1 DS-GVO („Berücksichtigung [...] der Risiken für die Rechte und Freiheiten“), Art. 6 Abs. 1 lit. f DS-GVO („Wahrung der berechtigten Interessen des Verantwortlichen [...] sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person [...] überwiegen“). Die Pseudonymisierung ist eine sogar in der DS-GVO ausdrücklich gelistete Maßnahme, um im Rahmen dieser Abwägung einen (wohl grundsätzlich positiven) Einfluss zu nehmen, siehe Art. 6 Abs. 4 lit. e, Art. 25 Abs. 1, Art. 32 Art. 1 lit. a, Art. 89 Abs. 1 DS-GVO.<sup>25</sup>

#### IV. Anonymisierungsverfahren und Quasi-Identifikatoren

##### 1. Vorüberlegungen/Auswahl des passenden Anonymisierungsverfahrens

Bei der Auswahl der passenden **Anonymisierungsverfahren** sind wesentliche Grundprinzipien und Fragen stets zu berücksichtigen und zu beantworten, da diese die **Auswahl der konkreten Verfahren** und technisch-organisatorischen Maßnahmen beeinflussen können. 24

Derartige **Grundprinzipien und Fragen** betreffen etwa Aspekte wie 25

- Welche Attribute begründen **direkt oder indirekt einen Personenbezug**, auch in Kombination mehrerer Attribute?
- Welche **Zwecke** sollen mit den anonymen Daten erreicht werden?
- Gibt es (**frei**) **zugängliche Informationen**, die mit den anonymen Daten verknüpft werden können und somit den Zugriffsberechtigten eine **Anonymauflösung ermöglichen**?
- Gibt es **Risiken eines unberechtigten Zugriffs** auf die anonymen Daten und wurde der Anonymisierungsprozess hinreichend komplex ausgestaltet, um eine unberechtigte Anonymauflösung ausreichend zu vermeiden?
- Werden die anonymen Daten durch **mehrere zugriffsberechtigte Gruppen oder gar Verantwortliche** verarbeitet und genügen die technischen und organisatorischen Maßnahmen, eine unzulässige Anonymauflösung hinreichend zu vermeiden?
- Wann (turnusmäßig oder im Falle bestimmter Ereignisse) sollte die **Wirksamkeit der Anonymisierung evaluiert** werden?

##### 2. Unterschiedliche Anonymisierungsverfahren

**Anonymisierungsverfahren** gliedern sich in zwei große Teilgruppen: 26

- Generalisierung
- Randomisierung

Ogleich sich die Verfahren nach diesen Oberbegriffen unterteilen lassen, kann es zu einer Mischung der Verfahren aus beiden Gruppen kommen. Die Verfahren der jeweiligen Gruppe sind geeignet, bestimmte künftige Verarbeitungen zu ermöglichen, bergen aber zugleich entsprechende Risiken für eine Anonymauflösung. Dies ermöglicht eine Balance zwischen der künftigen, sachdienlichen Verarbeitung der anonymen Daten und einer Vermeidung der Identifizierbarkeit.

##### a) Generalisierung

**Generalisierung** betrifft die Veränderung der Datensätze in der Gestalt, dass die Granularität der enthaltenen Informationen reduziert wird. Eine solche Generalisierung kann sowohl auf Ebene eines konkreten Anonyms stattfinden als auch auf Ebene des gesamten Datensatzes. 27

<sup>25</sup> Siehe auch → Pseudonymisierung Rn. 50 ff., sowie generell zu Funktionen von Pseudonymen im rechtlichen Kontext → Pseudonymisierung Rn. 28 ff.

## 1 Anonymisierung

---

- 28 **Methoden der Generalisierung** im weiteren Sinne sind etwa
- Generalisierung im engeren Sinne und
  - Aggregierung.
- Hierbei sind die Grenzen der beiden Methoden fließend. Eine Generalisierung im engeren Sinne kann mit einer Aggregierung einhergehen.
- 29 **Generalisierung im engeren Sinne** umfasst in der Regel die Verallgemeinerung von einzelnen Attributen auf der Ebene eines konkreten Anonyms. Anstelle eines exakten Geburtsdatums wird etwa das Geburtsjahr oder das Geburtsjahrzehnt, anstelle eines exakten Jahresgehalts wird etwa eine Gehaltsspanne oder ein auf beispielsweise 5.000er-Schritte gerundetes Gehalt, oder anstelle eines exakten Wohnorts wird etwa die Straße, eine Postleitzahl, Gemeinde oder ein Bundesland verwendet.
- 30 Die **Aggregierung** kann auf unterschiedlichen Ebenen stattfinden. Sowohl auf **Ebene eines konkreten Anonyms**, auf **Ebene eines gesamten Datensatzes unter Verlust separierbarer Anonyme** oder bei der **Zusammenstellung eines Datensatzes mit weiterhin separierbaren Anonymen**.
- 31 Erfolgt die Aggregierung auf **Ebene eines konkreten Anonyms**, betrifft dies entweder einzelne Attribute oder mehrere Attribute. Sofern ein einzelnes Attribut betroffen ist, werden beispielsweise anstelle der Tagesverkaufserlöse der Mitarbeitenden größere Zeitspannen aggregiert, etwa Wochen-, Monats- oder Quartalsерlöse. Die Aggregierung kann auch mehrere Attribute betreffen. Angenommen, es lägen einzelne Verkaufserlöse der Mitarbeitenden für unterschiedliche Produktgruppen A, B und C vor. So könnte die Aggregierung die Verkaufserlöse zusammenlegen und nur noch den Gesamtverkaufserlös aus A+B+C ausweisen.
- 32 Erfolgt die Aggregierung auf **Ebene des gesamten Datensatzes unter Verlust der separierbaren Anonyme**, so betrifft dies in der Regel die Bildung simpler Zähl- und Summendaten. Hierbei werden über mehrere Datenreihen (möglicherweise bereits Anonyme) Summen gebildet. Angenommen, die Verkaufserlöse stehen tagesexakt und produktgruppenexakt (A, B, C) in den Rohdaten von 100 Mitarbeitenden zur Verfügung. Eine Aggregierung unter Verlust der Einzeldatenreihen (möglicherweise Anonyme) würde etwa die Summe der Verkäufe aller Mitarbeitenden in einem Zeitraum X für die Produktgruppe B ausweisen oder etwa die Summe der verkauften Produkteinheiten der Produktgruppe A im Zeitraum X. Hierbei haben ggf. nur 30 der 100 Mitarbeitenden überhaupt zu den Verkäufen beigetragen. Dies ist dem aggregierten Wert nicht mehr zu entnehmen.
- 33 Erfolgt die Aggregierung auf **Ebene des gesamten Datensatzes unter Beibehalt separierbarer Anonyme**, so betrifft dies in der Regel eine risikoadäquate Zusammenstellung einer Vielzahl von Datenreihen, bei der jede Datenreihe einem Anonym entspricht. In diesem Fall vermischen sich möglicherweise unterschiedliche Einzelverfahren der Generalisierung im weiteren Sinne sowie der Randomisierung als Folge der erforderlichen Risikomitigation. Streng genommen ist dies keine Aggregierung von Daten im engeren Sinne, da keine Attributwerte zusammengefasst (aggregiert) werden. Verträte man diese terminologische Auffassung, wäre dies auch kein Anonymisierungsverfahren; vielmehr wäre die Ermittlung einer adäquaten Zusammenstellung eines Datensatzes eine Form der Risikomitigation.<sup>26</sup>

### b) Randomisierung

- 34 **Randomisierung** betrifft die Veränderung der Originalwerte. Diese Veränderung kann isoliert für ein Anonym erfolgen oder über mehrere Anonyme hinweg. Gängige Methoden der Randomisierung sind

---

<sup>26</sup> Näheres zur Risikomitigation → Rn. 52 ff.

- Rauschen (Noise) und
- Permutation (Datenaustausch).

**Rauschen** verändert die Grundwerte nach einem bestimmten Schema. Im Gegensatz zur Generalisierung bleibt ein engerer Bezug zum ursprünglichen Wert und ermöglicht daher präzisere Datenanalysen. Die konkrete Bestimmung des Wertes und des Schemas des Rauschens ist mit entsprechenden Experten des Faches zu ermitteln; hierbei sind unterschiedliche Aspekte zu berücksichtigen: 35

- Je größer das Rauschen, umso generischer sind möglicherweise die nachträglichen Ableitungen aus dem Datensatz.
- Je kleiner das Rauschen, umso geringfügiger, möglicherweise aus Sicht der Anonymisierung sogar zu gering, ist die Auswirkung auf die Identitätsschützende Funktion.
- Die durch Rauschen erzeugten Werte müssen weiterhin in einem **realistischen Korridor** verbleiben;<sup>27</sup> ansonsten ist einerseits erkennbar, dass die Werte mit einem Rauschen versehen sind, und andererseits ergeben sich aus den unrealistischen Werten möglicherweise Informationen, die eine Bestimmung des zugrunde liegenden Rauschschemas ermöglichen, sodass das Rauschen nachträglich wieder entfernt werden kann.
- Eine Risikoabwägung zwischen **statischem und dynamischem Rauschen**.<sup>28</sup>
- Ermöglichen die verrauschten Daten ggf. **Fehlidentifikationen**?<sup>29</sup>

Sind mehrere Attribute eines Anonyms geeignet, in ihrer präzisen Kombination einen Quasi-Identifikator darzustellen, kann ein **über mehrere Werte angewandtes Rauschen** diese Identifikationsmöglichkeit vermeiden, während zugleich die statistischen Korrelationen und Ableitungen zwischen den Attributen weiterhin möglich bleiben. 36

Rauschen kann auch **über mehrere Anonyme für einen ganzen Datensatz** eingesetzt werden. In diesem Fall erschwert das Rauschen nicht die **Quasi-Identifikation** aus der Kombination mehrerer Attribute, sondern es erschwert die **Vereinzelnung**. Der möglicherweise konkret bekannte Wert einer identifizierbaren Person zu einem Attribut wird durch das Rauschen unkenntlich gemacht. 37

Rauschen führt zu einem notwendigen **Informationsverlust**. Dieser kann für den Zweck der mit dem Datensatz auszuführenden Analyse kompatibel sein. Die **Rauscheffektivität** kann möglicherweise auch erst dann eintreten, wenn der Informationsverlust für die gewünschten Analysen zu groß wird. Vereinfacht ist der maximale Informationsverlust ein Quotient aus maximalem Rauschwert und Maximalgrundwert (in der jeweils gleichen Einheit). 38

27 Relativ leicht nachvollziehbare Beispiele von zu großen Rauschintervallen betreffen die Körpergröße oder das Alter. Werden diese Werte etwa um ein Rauschen +/- 50 cm bzw. 15 Jahren verändert, ergeben sich – ggf. auch in einem bestimmten Kontext – unrealistische Werte. Das Rauschen würde bei einer Original-Körpergröße von 1,90 m etwa Werte zwischen 1,40 m und 2,40 m ermöglichen. Eine Veränderung des Alters zum Zeitpunkt des Abiturs würde bei einem Originalalter von 19 Jahren Rauschwerte zwischen vier und 34 Jahren erzeugen.

28 Wird ein Attribut immer um den gleichen Wert in der gleichen Art verändert (statisches Rauschen), ist eine Entfernung des Rauschens für alle Datenreihen möglich, wenn in nur einem Fall das Rauschen als Wert ermittelt werden konnte. Ist das Rauschen indessen dynamisch, sprich es wird zufällig ein Wert in einem bestimmten Korridor addiert oder subtrahiert, kann ein für eine Datenreihe ermittelter Rauschwert nicht auf die anderen Datenreihen übertragen werden.

29 Auch wenn ein Anonym nicht mehr der Originalperson zugeordnet werden kann, kann es vorkommen, dass die neuen Zufallswerte den Eindruck einer möglichen Anonymauflösung vermitteln, welche letztlich zu einer anderen Person führt. In diesem Falle könnte vertreten werden, dass es sich um die Verarbeitung von falschen (inaccurate) personenbezogenen Daten handelt, sodass sich nicht nur Fragen im Rahmen der Rechtsgrundlage zur konkrete Verarbeitung stellen könnten, sondern auch, inwieweit die Pflichten aus Art. 5 Abs. 1 lit. d DS-GVO eingehalten wären.

## 1 Anonymisierung

---

- 39 Zudem kann das Rauschen unterschiedlich ausgestaltet werden. Das Rauschen kann **vollständig zufällig** angewendet werden. Insoweit wird für jeden Einzelwert das Rauschen individuell zufällig generiert. Das Rauschen kann aber auch so ausgestaltet werden, dass die ursprüngliche Verteilung der Originalwerte sich auch in einer identischen Verteilung der verrauschten Werte wiederfindet. In diesem Fall würde das Rauschen nicht vollständig zufällig angewendet, sondern **auf eine Zielverteilung** hin ausgerichtet.
- 40 **Permutation** ist eine Methode der Wertvertauschung. Dies ist dann sinnvoll, wenn die exakten Grundwerte eines Attributes erhalten bleiben müssen, die Aufrechterhaltung des Attributwerts zum ursprünglichen Anonym aber eine Anonymauflösung zu sehr vereinfachen würde. Es liegt nahe, die **Permutation über mehrere Anonyme** hinweg anzuwenden. Es ist nicht ausgeschlossen, dass eine **Permutation innerhalb eines Anonyms** zwischen mehreren Attributen erfolgen kann.<sup>30</sup>

### 3. Sonderfälle Differential Privacy und Maskierung (Masking)

- 41 **Differential Privacy** und **Maskierung** stellen jeweils für sich kein Anonymisierungsverfahren dar. Allerdings können beide Vorgehensweisen im Rahmen der Anonymisierung unterstützen oder gleichwertige Ergebnisse erzielen.
- 42 **Differential Privacy** sichert durch eine **Staffelung mehrerer Verfahren** ein ähnliches Schutzniveau.<sup>31</sup> Im Falle von Differential Privacy werden unterschiedliche Grenzwerte definiert, um die Erzeugung von Quasi-Identifikatoren zu vermeiden. Es besteht ein Datensatz mit X Datenreihen und Y Attributen pro Datenreihe. **Grenzwerte** definieren, wie viele Werte aus X und Y zeitgleich eingesehen werden können, um eine korrelierende Analyse zu vermeiden, die letztlich zu Quasi-Identifikatoren führen könnte. Entlang dieser Grenzwerte werden weitere Mechanismen implementiert, etwa in welcher Kombination diese Daten bereitgestellt werden können (bzw. im Umkehrschluss, welche Kombination nicht bereitgestellt werden darf), wie das Rauschen (Noise) hinzugefügt werden muss und ob und inwieweit andere Verfahren (Permutation oder Generalisierung) nötig werden. Aufgrund der **Wechselwirkung zu den Grenzwerten** ist es möglich, dass, je weniger Daten bereitgestellt werden, diese eine **höhere Genauigkeit** beibehalten können. Je nach Verarbeitungszweck ist eine höhere Genauigkeit der anonymen Daten erforderlich. Ein weiterer Grenzwert betrifft die **Wiederholungsrate**. Eine wiederholte Abfrage von anonymen Informationen aus dem ursprünglichen Datensatz darf nicht zu einer **Rekombination der einzelnen Teildatensätze** führen. Es kann auch ein sich veränderndes Rauschen auf das gleiche Anonym bei unterschiedlichen Abfragen angewendet werden, um eine Verkettung der Daten zu diesem Anonym zu vermeiden.
- 43 **Maskierung** betrifft die **Löschung oder Überlagerung von (Teil-)Attributen**. Insoweit besteht eine Nähe zur Generalisierung. Die Maskierung einer deutschen Postleitzahl durch Löschen der letzten 2 Ziffern ist zugleich eine Generalisierung auf eine größere Grundfläche (10117 würde so etwa zu 101xx). Die Generalisierung des Alters kann auch als eine Form der Maskierung betrachtet werden, da anstelle des konkreten Geburtsdatums 17.4.1957 teilmaskierte Werte verwendet werden. Alternativ können auch einzelne Attribute vollständig entfernt werden, zum Beispiel das Geschlecht, Vertrags- oder Kundennummern oder Ähnliches. Dies bietet sich insbesondere für derartige Informationen an, die besonders leicht als Quasi-Identifikator herangezogen werden können.

---

30 Vorstellbar etwa bei Datenreihen zu einem Wert über einen Zeitraum. Während die Zuweisung von exaktem Wert und exakter Zeit eine Identifikation ermöglichen könnte, könnte es genügen, die Zuweisung konkrete Zeit und konkreter Wert zu durchmischen.

31 Für einen umfassenden Überblick an die Anforderungen und Implementierung siehe NIST-Guidelines SP 800-226, in der aktuellen Version März 2025 <https://doi.org/10.6028/NIST.SP.800-226>.

## Stichwortverzeichnis

Die fetten Zahlen bezeichnen die Ordnungszahlen des jeweiligen Stichworts, die mageren Zahlen die Randnummern. Die fett gedruckten Wörter bezeichnen die kommentierten Hauptstichwörter des Werkes mit der jeweiligen Ordnungszahl, unter der sie zu finden sind.

- 3–2–1-Regel **39** 68
- Abbildung vertraglicher Mindestanforderungen **19** 70 f.
- Abfangen von Daten **11** 24 f., 51
- Live-Monitoring **11** 25
- Abhängigkeitsanalyse **27** 9
- Abhilfemaßnahme **29** 37
- Ableitung Risikomitigation **1** 51
- Abmahnung **29** 40
- Abschlussbericht **37** 71, 75, **38** 47 f.
- Abschlussmeldung **37** 53, 91, 101
- Absolute Sicherheit **29** 17
- Abstract **28** 24
- Abweichungserkennung **39** 40
- Adblocker
- Filterliste **43** 28 f.
  - Sperrliste **43** 28
- Ad-hoc-Publizität **37** 109 ff.
- Ad Server
- Grundsatz der Datenminimierung **43** 37
  - Konfiguration **43** 36 ff.
  - Notfall- und Sicherheitskonzept **43** 39
- Adversarial
- Attack **25** 35 ff., 65, **39** 33
  - Risks **25** 38
  - Training **39** 26
- Aggregation **1** 28, 30 ff., **30** 68
- Beibehalt separierbarer Anonyme **1** 33
  - gesamter Datensatz **1** 30, 32
  - konkretes Anonym **1** 30 f.
  - Verlust separierbarer Anonyme **1** 32
- AGI **25** 1, 53
- AI Act *siehe* KI-Verordnung
- Air Gap, Backup **39** 69
- Aktiv ausgenutzte Schwachstelle **37** 27
- Aktualisierungspflicht **29** 35 ff.
- ALE **39** 57
- Alert Fatigue **39** 37
- Algorithmische Integrität **25** 17 ff.
- All-Gefahren-Ansatz **39** 15
- Allgemeine Produktsicherheitsverordnung **29** 9 ff.
- Allgemeines Produktsicherheitsrecht **29** 5 ff.
- Allianz für Cyber-Sicherheit **39** 44
- Altersverifikation, anonym **1** 92 ff.
- Anbieter **25** 4, 10 f., 26, 46
- von Online-Marktplätzen **29** 11 f.
- Anerkennung **8** 35
- Angreifermodell **1** 61 ff.
- Angriffszenarien **1** 62
  - Anonymität **1** 61 ff.
  - Aspekte **1** 63
  - Motivated Intruder Test **1** 61 ff.
  - Ressourcen **1** 62
- Angriffserkennung, System zur **39** 25 ff.
- Angriffsfläche, Minimierung der **39** 24
- Angriffsziele **25** 36
- Annual Loss Expectancy **39** 57
- Anomalieerkennung **39** 36
- Anonym
- Begriffsbestimmung **1** 2
  - Grenzwert **30** 26 ff.
  - Identifizierbarkeit **30** 20, 23 ff.
  - im Rechtssinn **1** 16
  - Relativität **1** 16
  - Zweck **1** 16
- Anonymauflösung **1** 26, 44 ff.
- Angreifermodell **1** 61 ff.
  - Begriffsbestimmung **1** 4
  - Risikofaktor **1** 52 ff., 80
  - Risikomitigation **1** 52 ff.
- Anonyme Daten **30** 20
- Begriffsbestimmung **1** 3
  - Bezugsgröße **1** 47
  - Datensatz **1** 47
  - enthaltenes Pseudonym **1** 47
  - Erforderlichkeitsprinzip **1** 76
  - Ersterhebung **1** 66 ff.
  - freiwillige Maßnahme **1** 75
  - gesetzlicher Schutz **1** 65
  - Granularität **1** 47
  - Grundmenge **1** 47
  - konkretes Anonym **1** 47
  - Löschäquivalent **1** 80

## Stichwortverzeichnis

---

- nachträgliche Anonymisierung 166 ff.
- signifikante Abweichungen 147
- Anonymisierung 1**
- Anonymisierung 13 14, 28 3 f., 30
- Abgrenzung zu Pseudonymisierung 115 ff., 22
- Ableitung 151
- Aggregation 30 68
- als Rechtsgrundlage 183
- Angreifermodell 161 ff.
- Anonym 12
- Anonymauflösung 14, 13, 16, 44 ff., 52 ff., 84
- anonyme Daten 13
- Anonymisierung 11
- Anonymisierungsverfahren 144
- Art. 9 DS-GVO 166 ff.
- Auswahl der Verfahren 124 ff.
- Begriffsbestimmung(en) 11 ff.
- Bestimmtheit des Gesetzes 148
- BSIG 30 64
- Datenanalyse 157 ff., 87
- Datenlöschung 178 ff.
- Datenminimierung 175
- Datenverarbeitung 164 ff.
- Differential Privacy 141, 54
- DS-GVO 123
- EHDS 187 ff.
- Einsatzzweck 157 ff., 75, 77, 87 ff., 30 21
- Einwilligung 171
- Erforderlichkeitsprinzip 178 ff.
- Erinnerungswissen 180
- Forschung 187 ff.
- freiwillige Maßnahme 17
- Gegenstand 120
- Gemeinwohl 187 ff.
- gesetzliche Pflicht 17, 77
- Gesundheitsforschung 187 ff.
- Granularität 147
- Grenzwert 148
- im Konzern 122
- individueller Schutzzweck 125
- Information 16
- informationsagnostisch 16
- Informationsverlust 138
- Interessenabwägung 122 f.
- K-Anonymity 154, 56 ff.
- kaskadierte Datenverarbeitung 179 ff.
- kontextabhängige 15, 30 22 ff.
- kontextuelle Betrachtung 113
- Kryptographie 112
- l-Diversity 154
- Leitfäden 114
- Löschen 26 19 f.
- Löschen der Originaldaten 122
- Maskierung 141
- missbräuchliche 183
- nachträgliche 166 ff., 80
- NIS-2-Richtlinie 185 ff.
- organisatorische Maßnahmen 110
- Quasi-Identifikator 136, 80
- Randomisierung 134 ff.
- Recht auf Vergessen 178 ff.
- rechtfertigungsbedürftige 171
- Rechtsgrundlage 164 ff.
- regelmäßige Prüfung 125
- Relativität 113, 21 ff., 47 f.
- relevante Attribute 131 ff.
- Risikoabwägung 122 f., 26, 47
- Risikofaktor 147, 51 ff., 61 ff.
- Risikomitigation 151
- sachlicher Anwendungsbereich 16
- Schutzgrad 18
- Schutzziel 123, 30 22 ff.
- Schutzzweck 15, 23
- Sicherheit & Integrität 18
- Singling-Out 147
- Speicherlimitierung 178 ff.
- Standards 114
- statistische Auswertung 187
- statistische Kontrolle 155
- Stellungnahmen 114
- synthetische Daten 150 ff.
- T-Closeness 154
- technische Maßnahmen 111
- technisch-organisatorische Maßnahme 18 ff., 24 ff.
- TOM 18 ff., 24 ff., 41
- Transparenzpflichten 168 ff.
- über mehrere Entitäten 122
- Vereinzelung 147
- Verfahren 124 ff.
- verfügbarer Datensatz 151
- Verhältnis zu Pseudonymisierung 113, 21 ff., 77, 30 18 ff., 22 ff., 65
- Verkettung 147, 94

- Verschlüsselung 112
- Wechselwirkung Pseudonymisierung 121 ff.
- Wirksamkeit 184
- Zusammenspiel Technik und Organisation 19
- Zweck 115 f.
- Zweckänderung 168 ff.
- Zweckbindungsgrundsatz 178 ff.
- Anonymisierungsverfahren 124 ff.
- Anonymauflösung 144
- Auswahl 124 ff.
- Datenempfänger 125
- Generalisierung 126 ff.
- Quasi-Identifikator 136
- Randomisierung 126 ff., 34 ff.
- Risikoabwägung 145
- Risikofaktor 152 ff.
- Risikomitigation 152 ff.
- Sonderfälle 141
- technisch-organisatorische Maßnahmen 124 ff., 45
- TOM 124, 45
- Wirksamkeit 125
- Anonymität 144
- Abwägungsentscheidung 117
- Altersverifikation 192 ff.
- Angreifermodell 161 ff.
- Anonymauflösung 152 ff.
- Attributverifikation 192 ff.
- Datenempfänger 125
- Datensatz 127
- Datenschutzrecht 164 ff.
- Educated Guess 148
- Effektivität 145
- eIDAS 192 ff.
- Grenzen negativer Definition 117
- Grenzwert 117, 42
- im Rechtssinne 179
- konkretes Anonym 127
- Quantencomputing 119
- quantifizierbare 117
- Rechenkapazität 119
- Relativität 118, 61 ff.
- relevante Attribute 125
- Risikobetrachtung 117
- Risikofaktor 152 ff.
- Risikomitigation 151 ff.
- synthetische Daten 150 ff.
- standardisierte Betrachtung 117
- verfügbarer Datensatz 118, 51
- Verifikation 192 ff.
- Verkettung 117
- Vermeidung der Identifikation 120
- vernetzte Ressourcen 119
- Zeitablauf 125
- Anonymität, Risikofaktor 151
- Antragsdelikt 1171
- Anwendungen 29 30 f.
- Arbeitgeber 25 27
- Arbeitnehmer 41 47 ff.
- Abmahnung 41 48
- Business Judgment Rule 41 47
- Direktionsrecht 41 47
- Gremien- und Kollegialentscheidungen 35 40
- Haftung 41 50
- innerbetrieblicher Schadensausgleich 35 33 f., 41 50
- Kündigung 41 48
- Scheinselbstständigkeit 35 10 f.
- Verantwortlichkeit, Datenschutz 41 49
- Weisung 41 47
- wichtiger Grund 41 48
- Archivierung, Pseudonymisierung 30 45
- Artificial Intelligence 25 1 ff.
- Asset, Schutzbedarf 39 6
- Asset Recovery 38 31
- Asymmetrische Verfahren
- ECC 15 8
- öffentlicher und privater Schlüssel 15 7
- Quantensicherheit 15 8
- RSA 15 8
- Audit 22 15, 25 18, 28, 30 ff.
- Begriffsbestimmung 44 14
- Überprüfungen der Maßnahmen 14 4
- Auditbericht 25 33
- Auditfeststellungen 22 15
- Auditierung 16 24
- Audits und Zertifizierungen, allgemein 2**
- Audits und Zertifizierungen, Dokumentation 3**
- Audits und Zertifizierungen, Vorbereitung 4**
- Aufbewahrungspflicht, Löschen 26 23
- Aufsicht 5**

## Stichwortverzeichnis

---

- Aufsicht
  - Befugnisse 5 26 ff.
  - informationstechnische Systeme 5 17
- Aufsichtsbehörde 12 19, 13 21
- Auftraggeber 27 5 f.
- Auftragsverarbeiter 13 19
- Auftragsverarbeitung 25 23, 27 20 f.
- Auftragsverarbeitungsvertrag 25 23
- Ausblick 22 24 ff.
- Ausgliederung 19 42 f.
- Auslagerung 19 42 f., 27 8
- Auslagerungsmanagement 27 8
- Auslagerungsvereinbarung 19 61
- Ausnahmetatbestände 37 66
- Ausschlüsse
  - Cyberkrieg 42 32
  - grobe Fahrlässigkeit 42 33
  - hybride Kriegsführung 42 32
  - Lösegelder 42 32
  - Straf- und Bußgelder 42 32
  - Terror, Krieg, kriegsähnliche Handlungen 42 32
  - Vorsatz 42 33
- Ausspähen von Daten 11 17, 19 f., 26, 58
  - Hacking 11 51
- Auswahl des Anonymisierungsverfahrens
  - Grundprinzipien 1 25 ff.
  - Vorüberlegung 1 25 ff.
- Authentifizierungsmethoden 6 7
  - MFA 6 7
- Authentizität 6**
- Autodialer-Programm 11 22
- Automatisierung 10 20, 22 23
- AVB Cyber
  - Cyberrisikoversicherung 42 6
  - Multi-Line-Policen 42 24
- Awareness 31 15
  - Maßnahme 39 20
- B3S, Ko-Regulierung 23 44
- Backdoors 11 22
- Backup
  - Stand der Technik 39 70
  - Strategie 39 68 ff.
- BaFin 9 32
- Bagatellrisiken 29 17
- BAMAD 9 29
- Baselining 39 40
- BBK, zentrale Anlaufstelle 5 12
- BCM-Beauftragte 10 10
- Bedrohung 11 64
- Bedrohungslage 12 19
  - Entwicklung 39 11
- Bedrohungsszenarien 7**
- Bedrohungsszenarien 11 2
  - Advanced Persistent Threat 7 28
  - Angreifer 7 8
  - APT-Gruppen 7 30
  - Aufklärungsquote 7 4
  - Bot-Netz 7 38
  - Bot-Netz Beispiel DDoS 7 39
  - Bot-Netz Beispiel IoT 7 42
  - chinesische APT-Gruppen 7 31
  - DDoS Beispiele 7 36
  - Deepfake 7 17
  - Distributed Denial of Service 7 35
  - Insider-Bedrohung 7 49
  - iranische APT-Gruppen 7 33
  - Jamming 7 26
  - Malware 7 12
  - Phishing 7 10
  - physische Infrastruktur 7 53
  - Ransomware 7 13
  - russische APT-Gruppen 7 32
  - Scamming 7 23
  - Schadenssumme 7 3
  - Social-Engineering 7 16
  - Spoofing 7 19
  - Spoofing-Beispiele 7 21
  - Spoofing-Varianten 7 20
  - Supply-Chain-Angriff 7 55
  - Supply-Chain-Angriffsbeispiele 7 56
  - Zero-Day-Exploit 7 45
  - Zero-Day-Exploit Beispiel 7 46
- Befugnisse
  - Behörden 5 27
  - Durchsetzungsmaßnahmen 5 28
  - Inspektionsrechte 5 27
  - Kompetenz 9 1
  - Korrektur- und Abhilfemaßnahmen 5 27
  - Überwachungsbehörden 5 31
- Behörde 8 1
  - Aufgaben 5 5
  - Befugnisse 5 26 ff.
  - Bund-Länder-Kooperation 5 6
  - Informationsaustausch 5 4

- kritische Einrichtungen 5 11
- Sicherheitsbehörden 5 6
- Zusammenarbeit 5 4
- Zusammenarbeit, grenzüberschreitende 5 5
- Zuständigkeit 5 6 ff.
- Behörden, allgemein 8**
- Behörden, Befugnisse 9**
- Behördenlandschaft, komplexe Netzwerke 8 20
- Behördliche Sanktionen 29 38 f.
- Beinahe-Vorfall 37 17 f.
- BSIG 37 10 ff.
- Cyber Resilience Act 37 31
- Beleidigung 11 62
- Beleihung, CTI-Plattform 39 48
- Beliehene 8 18
- Benachrichtigungspflicht 37 64 ff.
- Berechtigtes Interesse
  - Pseudonym 30 50 ff.
  - Pseudonymisierung 30 50 ff.
- Berechtigungen, Least Privilege 12 12
- Berufsgeheimnis 27 22
- Beschäftigte 25 27
- Beseitigungsanspruch 29 40
- Besondere Aufbauorganisation (BAO) 10 10
- Besondere Kategorien personenbezogener Daten, Anonymisierung 1 67
- Betreiber 25 4, 26, 46
- Betreiber Kritischer Anlagen 16 28, 24 14 ff., 25 ff.
  - Bundesnetzagentur 24 36 ff.
  - Dienstleister 16 22
  - Doppelregulierung 24 36 ff.
  - Energieerzeugung 24 36 ff.
  - Mehrpartenunternehmen 24 36 ff.
  - Nebentätigkeit 24 36 ff.
- Betriebshaftpflichtversicherung, Vermögensschäden, Dritte 42 18
- Betriebsvereinbarung, Log-Analyse 39 37
- Betrug 11 52 f.
  - im Internet 11 67
- Bevollmächtigte 25 26, 29 11 f.
- Beweissicherung 38 44 f.
- Bewertung 25 11, 29 20, 22 ff.
- Bewertungssystem, Ko-Regulierung 23 12
- Bezug von Software 19 45 f.
- BIAS 25 54
- BIA-Vorfilter 10 14
- Big Data 28 31, 39 12
- BKA, Cyberkriminalität 9 22
- Black-Hat-Hacker 11 9
- Börsennotierte AG 32 9
- Botnetz, Bitcoins 43 10
- Branchenspezifischer Sicherheitsstandard, Ko-Regulierung 23 44
- Branchenstandards
  - COBIT 2019 12 10
  - ISO/IEC 27001 12 8
  - IT-Grundschutzkompendium 12 9
- Browser, Tracking-Schutz 43 30
- BSI (Bundesamt für Sicherheit in der Informationstechnik) 37 98
  - Behörde 9 18
  - Betreiber kritischer Anlagen 5 15
  - Cross-Border-Einrichtungen 5 16
  - informationstechnische Systeme 5 17
  - Marktüberwachungsbehörde 5 13
  - Standards 12 9
  - Zuständigkeit 5 14 ff.
  - Zuständigkeit, Ausnahmen 5 16 f.
- BSI C5
  - Entwicklungsstand 23 36
  - freiwillig 23 33 ff., 44 35
  - gesetzliche Pflicht 23 33 ff., 44 35
  - Grundlage 23 36
  - Informationsaustausch 39 44
  - internationale Vergleichbarkeit 23 36
  - ISO 27001 23 36
  - Ko-Regulierung 23 33 ff.
  - Mehrwert 23 33 ff.
  - Reform 23 36
  - Überarbeitung 23 36
  - Zertifizierung 44 34
  - Zertifizierungsprogramm 44 34
- BSI-Gesetz (BSIG) 8 24, 22 4, 37 9 ff.
  - Löschen 26 4
- BSI-Grundschutz-Kompendium 44 39
- BSI Standard 200-4 10 7
- Budapest Convention on Cybercrime 11 7
- Bug-Bounty-Programme 11 9, 21
- Bundesbeauftragte für den Datenschutz 13 6
- Bundesdatenschutzgesetz (BDSG) 11 49, 51, 58, 68, 13 3
- Bundeslagebild Cybercrime 11 11
- Bundesnetzagentur 37 98

- Bundesverband Digitale Wirtschaft e.V. (BVDW) 43 8  
Bundeswehr 9 31  
Bund-Länder-Kooperation, Kooperationsvertrag 5 6  
**Business-Continuity-Management (BCM) 10**  
Business Continuity Management (BCM) 22 17, 27 12, 38 17 ff., 39 63 ff.  
– BCM 31 13  
Business-Continuity-Management-System (BCMS) 10 3  
Business-Impact-Analyse (BIA) 10 11, 39 66  
Business Judgment Rule 38 18 ff.  
Bußgeld 13 21, 25 25, 29 39, 37 58, 67, 80, 87, 107, 111  
  
CEO-Fraud 39 19  
CER-Richtlinie 24 9, 31 5  
– KRITIS-DachG 12 24  
– Resilienz kritischer Einrichtungen 12 24  
CERT-EU 9 13  
Changemanagement 22 22, 27 39 ff.  
Charta der Grundrechte der EU 13 6  
Chief Information Security Officer, Budgetierung 39 4  
Claims-Made-Prinzip, Versicherungsfallprinzip 42 7  
Clickjacking, Abonnements 43 11  
Click-Worker 25 55  
Cloud 22 26  
– Software as a Service 16 1  
Cloud Service Provider 19 54 f.  
COBIT 2019  
– Audits 12 10  
– Bewertungen 12 10  
– Governance 12 10  
– ISACA 12 10  
Computerbetrug 11 22, 35, 42  
– unbefugte Datenverwendung 11 37  
– unrichtige Daten 11 36  
Computerkriminalität 11 3, 12 ff.  
– Erscheinungsformen 11 15  
– Strafgesetzbuch 11 13 ff.  
Computersabotage 11 28, 57  
– Mittäterschaft 11 29  
Computerstrafrecht 11 2  
Computertechnologie 11 5  
  
Computer Vision 25 21, 56  
Conformity Assessment 44 12  
– Body 44 10  
– internationale Standards 44 16  
– Programme 44 13  
Consent-Banner, Dark Pattern 43 14  
Content-Filter 43 32  
Control 28 27  
Cookie-Banner 28 18  
Cookie-Management-Plattform 13 14, 28 30  
Cookies, Consent-Banner 43 14  
Coordinated Vulnerability Disclosure 39 34  
Cost to Society 39 56  
Critical Entities 31 3  
Critical Entities Resilience Group, CyCLONe 31 20  
CRM-Software 13 18  
CSIRT 39 62  
Cyberabwehr, aktive 39 51 f.  
Cyberangriff 13 27, 32  
– Bedrohung, Bedrohungslage 42 1 f.  
– Erkennung 12 13  
– KRITIS 16 3  
– Lieferkette 16 2  
– Prävention 12 13  
– Reaktion 12 14  
– Schäden 42 1 f.  
– Schadenstypen 42 19 ff.  
– Supply Chain 16 2  
– Versicherungen 42 2 f.  
Cyberattacke 11 11  
Cyber-AZ 9 28  
– Plattform 9 19  
– Sicherheitsbehörden 9 19  
Cyberbedrohung  
– BSIG 37 10 ff.  
– Cyber Resilience Act 37 30  
– Erheblichkeit 37 15, 48  
– Verordnung über digitale operationale Resilienz im Finanzsektor 37 48  
Cybercrime 11 2, 4, 12 ff.  
Cybercrime-as-a-Service  
– Angebote 11 11  
– Darknet 12 1  
– Dienstleistung 12 1  
Cyber Deception 39 43  
**Cyberkriminalität 11**

- Cyberkriminalität **11** 66 ff., 74, **28** 31
- Antragsdelikt **11** 71 ff.
  - Arbeitsteilung **39** 14
  - Ökosystem **39** 13
  - Schutzmaßnahmen **11** 73
  - Strafverfolgung **11** 72 f.
- Cybermobbing **11** 59 ff.
- Doxing **11** 65
  - Stalking **11** 64 f.
- Cyberraum **6** 3
- Cyber Resilience Act **11** 77
- Cyber Resilience Act **11** 77, **13** 31, **22** 27, **25** 15, **29** 28 f., **37** 26 ff., **39** 16
- Cybersecurity-Anforderungen **43** 24
  - Hochrisiko-KI-Systeme **5** 13
  - Konformitätserklärung **12** 27
  - Lieferkette **16** 10
  - Löschen **26** 2
  - Marktüberwachungsbehörde **5** 13
  - Nachweispflichten **16** 11
  - Pflichten **12** 27 f.
  - Produkte mit digitalen Elementen **12** 26
  - Produkte mit digitalen Inhalten **16** 10
  - Schwachstellenhandling **12** 27
  - Security by Design **12** 26, **16** 11
  - Sicherheitsupdates **12** 27
  - Software Bill of Materials (SBOM) **12** 27
- Cyber-Resilienz **5** 11, **10** 27
- Cybersecurity Act
- Cybersicherheitszertifizierung **12** 34
  - ENISA **12** 34
- Cybersicherheit 12**
- Cybersicherheit **11** 74 ff., **25** 6, 15, **29** 24 ff., **31** 1
- Abgrenzung IT-Sicherheit **12** 5
  - Branchenstandards **12** 6
  - Datenverarbeitungsprozess **12** 3
  - Definition **12** 3 ff.
  - digitaler Raum **12** 3
  - Kompetenz, Grundgesetz **5** 6
  - Schutzgegenstand **12** 5
  - Schutzziele **12** 7, **33** 1
- Cybersicherheitsanforderungen **13** 31, **29** 28 f.
- Cybersicherheitsarchitektur **8** 21
- (Cyber-)Sicherheitsbehörden **8** 13
- Cybersicherheitsmerkmale **29** 24 ff.
- Cybersicherheitsrisiken **29** 24 ff.
- Cybersicherheitsstrategie EU
- Abschreckung **12** 2
  - Branchenstandards **12** 6
  - Globale Zusammenarbeit **12** 2
  - IT-Sicherheit **12** 5
  - Policy **12** 2
  - Reaktion **12** 2
  - Rechtsakte **12** 2
  - Resilienz **12** 2
  - Souveränität **12** 2
- Cyber Solidarity Act
- Abwehrfähigkeiten **12** 33
  - Cyber-Hub-Nutze **5** 2
  - Cybernotfallmechanismus **5** 2
  - Cybersicherheitsvorfälle **5** 2
  - European Cyber Shields **12** 33
  - Informationsaustausch **12** 33
  - Zusammenarbeit der Mitgliedstaaten **12** 32
- Cyberstalking **11** 54 f.
- Cyber-Threat-Plattform **39** 45
- Cyberversicherung **38** 15 ff., 54
- AGB **42** 26
  - AVB Cyber **42** 27
  - Cyberangriff, Abwehr/Beseitigung **42** 25
  - Deckungsbausteine **42** 16
  - Musterbedingungen **42** 27
  - Rechtsgrundlagen **42** 26
  - Vertragsgestaltung **42** 27
  - Voraussetzung **39** 58
  - Ziel **42** 25
- D&O Versicherung **42** 30
- Darknet **11** 47, 70
- Dark Patterns **28** 18
- Consent-Banner **43** 19 f.
  - Einwilligung **43** 19 f.
- Dark Web, Monitoring **39** 47
- Data Act **11** 80, **13** 30
- Data Breach **20** 17 ff.
- Data-Management-Plattformen
- Cookies **43** 3
  - Fingerprinting **43** 3
- Data Poisoning **25** 42, **39** 33
- Data Protection by Default **13** 5
- Datenschutz **16** 12
- Data Protection by Design 13**

## Stichwortverzeichnis

---

- Data Protection by Design 13 12, 14, 18 ff., 24, 26, 28 ff., 33, 28 6 f.
- Datenschutz 16 12
  - Löschen 26 3
- Daten, Definition 26 10
- Daten, personenbezogene 25 21, 29
- Datenabfluss, Zeitspanne 39 35
- Datenbank 25 12
- Datenhandel 11 47 ff., 68
- Datenhehlerei 11 47 f.
- Verfolgung 11 48
- Datenintegrität, Pseudonymisierung 30 10, 47 ff., 69 ff.
- Datenleck 38 58 f.
- Datenlöschung, Anonymisierung 1 78 ff.
- Datenmanipulation 11 34 ff.
- Inputmanipulation 11 35 ff.
- Datenminimierung 13 3, 16, 18, 26, 28 4, 12
- Pseudonymisierung 30 38, 42 ff., 55
- Datenqualität 25 5
- Datenschutz 11 49, 25 21 ff., 29, 28 1 ff., 10 ff., 17 f., 28, 31
- Bußgelder 43 26
  - Datenschutz durch Technik 28 4
  - Datenschutz-Folgenabschätzung 28 11 ff.
  - Datenschutzmanagement-System 28 11
  - Datenschutzstrategie 28 11
  - Haftung 43 25 f.
  - Schadensersatzansprüche 43 26
- Datenschutz durch Technik 13 1, 3
- Datenschutz durch Technikgestaltung 13 2, 9, 29
- Datenschutz-Folgenabschätzung 13 17, 14 2, 28 13, 29
- Datenschutzfreundliche Voreinstellungen 13 8
- Datenschutzgrundsätze 13 1, 9 ff.
- Datenschutz-Grundverordnung (DS-GVO) 11 79, 13 1 ff., 17 ff., 31 f., 22 3, 25 21, 28 6 f., 9, 16, 18, 37 19 ff.
- Löschen 26 3, 14
  - Sicherheitsvorfall 39 7
  - Wiederherstellung 39 73
- Datenschutzkultur, offene Kommunikation 14 5
- Datenschutzmanagementsystem 14**
- Datenschutzmanagementsystem 22 20, 28 2
- Anforderungen 14 1
  - Einhaltung der Datenschutzgesetze 14 1
  - Maßnahmen 14 1
  - Richtlinien 14 1
  - Risikoreduktion von Datenschutzverletzungen 14 1
  - Vorgaben 14 1
- Datenschutzrecht 25 21 ff., 29
- Datenschutzrichtlinie 13 3
- Datenschutzverletzung 37 24 f.
- Datenschutzvorfälle
- Behebung 14 3
  - Identifizierung 14 3
  - Meldung 14 3
- Datensicherheit 37 22, 34
- Datenübermittlung
- Pseudonymisierung 30 54 ff.
  - Risikomitigation 30 54 ff.
  - TOM 30 54 ff.
- Datenvalidität, Pseudonymisierung 30 10
- Datenveränderung 11 31, 46, 58
- Datenbank 11 40
- Datenverarbeitung
- Anonymisierung 1 64 ff.
  - Grundsatz der Datenminimierung 43 37
  - Pseudonymisierung 30 30
  - Zweckbindungsgrundsatz 30 43
- Datenverarbeitungssystem 13 3
- Datenverschlüsselung 15**
- Datenverschlüsselung
- Abgrenzung Pseudonymisierung 30 35
  - Algorithmen 15 1
  - Schlüssel 15 1
- DDoS-Angriff 11 2, 11, 27 ff.
- Datenverlust 11 31 ff.
  - Nation-State-Actors 11 32 f.
  - Wettbewerbsrecht 11 33
- Decision Analysis 39 6
- Deckungsbausteine
- Drittschäden 42 24
  - Eigenschäden 42 24
  - Service und Kosten 42 24
- Deep Learning 25 1, 16, 57
- Defense in Depth Modell 12 11 f.
- Deliktische Haftung
- Meldepflicht 20 23
  - Schutzgesetz 20 21 ff.
  - Verkehrssicherungspflichten 20 13 ff., 35 36
- Demand-Side-Plattformen (DSP), Einkauf von Werbeflächen 43 6

- Demilitarisierte Zone 39 23  
Demonstrate 28 29  
Detektion  
– Dwell Time 39 49  
– Prepositioning 39 49  
– Threat Hunting 39 49  
Determinierung, Anonymisierung 1 75  
Dienstleister 38 14  
– Auditierung 16 23 f.  
– Auftragsverarbeitungsvertrag 16 20  
– Auswahl 16 2  
– BSI-IT-Grundschutz 44 40  
– gemeinsame Verantwortlichkeit 16 21  
– Joint Controller 16 21  
– Kontrolle 16 18 ff.  
– Kontrollmechanismen 16 4  
– Lieferkette 16 6  
– Maßnahmen, technische und organisatorische 16 5  
– Mindestanforderungen, technische und organisatorische 16 13 ff.  
– Mindestmaßnahmen 16 5, 7  
– NIS-2-Richtlinie 16 7  
– Prozesse 16 31  
– Steuerung 16 18 ff.  
– Überprüfung 16 19  
– Vereinbarung über die gemeinsame Verantwortlichkeit 16 21  
– Versicherungsschutz Kunden 42 31  
– Zertifizierung 16 23  
**Dienstleister, allgemein 16**  
**Dienstleister, Checkliste Auftragsverarbeitung 18**  
**Dienstleister, Checkliste Sicherheitsprüfung externe Dienstleister 17**  
Dienstleistersteuerung 22 19  
Differential Privacy 1 41, 54, 28 14  
– Datenanalyse 1 42  
– Einsatzzweck 1 42  
– Genauigkeit 1 42  
– Grenzwert 1 42  
– Kombination mehrerer Verfahren 1 42  
– Rekombination 1 42  
– Risikoabwägung 1 42  
– Teildatensatz 1 42  
– Wechselwirkung 1 42  
Digitale Plattformen 6 1  
Digitale Sicherheit 13 1, 28 2, 31  
Digitales Produkt 29 8  
Digitale Vernetzung 29 23  
Digitalisierung 12 1, 29 3  
Digital Operational Resilience Act 37 89 ff.  
– Sicherheitsvorfall 39 7  
Digital Services Act, informierte Entscheidung 43 20  
Digitalwirtschaft, digitale Ökonomie 6 4  
DIN 66398 26 27  
Diskriminierung, Pseudonymisierung 30 71  
Distributoren 25 15  
DNS4-EU-Initiative 13 28  
DNS-Filter, Domain-Namen 43 31  
Dokumentation 19 26, 25 11, 32, 34, 38, 29 21, 38 44 f.  
– Pseudonymisierung 30 45  
– Wiederherstellungstest 39 74  
Dokumentationspflicht 29 21, 37 63  
DORA 9 33, 11 76, 19 4 ff., 31 21  
– Finanzunternehmen 16 9  
– IKT-Geschäftskontinuitätspolitik 10 4  
– IKT-Reaktions- und Wiederherstellungspläne 10 4  
– Lieferkette 12 25  
– Mindestvertragsinhalt 19 33  
– Risikomanagementpflichten 12 25  
– Vertragsgestaltung 19 30 ff.  
**DORA und finanzaufsichtsrechtliche Auslagerung 19**  
DoS-Attacke 11 28  
Doxing 11 65  
Drittanbieter 25 28  
Dritte 25 28  
Drittsschäden, Informationssicherheitsverletzungen 42 22  
Drittstaatenentransfer  
– Interessenabwägung 30 54 ff.  
– Pseudonymisierung 30 54 ff.  
– Risikomitigation 30 54 ff.  
– TOM 30 54 ff.  
Due Diligence 19 23, 60, 27 14  
Durchsetzungsmaßnahmen, Sanktionen 5 28  
Dwell Time 39 67  
EBA, Finanzsektor 9 14  
EC3, Cybercrime 9 17  
ECCC, NAC 9 12  
EDR 39 26

## Stichwortverzeichnis

---

- Educated Guess  
– Anonymität 148  
– Identifizierbarkeit 148  
EHDS, Anonymisierung 187 ff.  
Ehrendelikte 11 62  
eIDAS 192 ff., 6 17  
Eigenbetriebe 24 29 ff.  
Eigenschäden  
– entgangener Gewinn 42 20  
– Ertragsausfallschäden 42 20  
– Wiederherstellungsaufwände 42 20  
Einflussnahme Dritter 29 27  
Einführer 25 4, 26, 46, 29 11 f.  
Eingriffs- und Sicherheitsverwaltung 9 1  
Einrichtungen der Bundesverwaltung 24 23  
EIOPA, Versicherungen 9 15  
Embedded Software 29 8  
Energieerzeugung 24 38 ff.  
Enforce 28 28  
ENISA, Agentur 9 11  
Entscheidung, automatisierte 39 41  
ePrivacy-Richtlinie 13 26  
Ereignis, sicherheitsrelevantes 39 6  
Erfinder 25 51  
Erfolgsfaktoren 22 21 ff.  
Erforderlichkeitsgrundsatz, Pseudonymisierung 30 38 ff., 42 ff.  
Erforderlichkeitsprinzip  
– Anonymisierung 1 75, 78 ff.  
– TOM 1 79 ff.  
Erfüllungsaufwand, NIS-2 39 60  
Erhebliche Störungen 37 95  
Erpressung 11 30, 57  
Ersatzfähiger Schaden 20 24 ff.  
– Art. 82 DS-GVO 20 26  
– besondere Schadensanlage 20 35  
– Betriebsausfallschaden 20 27  
– Datenschutzverletzung 20 26  
– haftungsausfüllender Tatbestand 20 28  
– kausaler Schaden 20 28  
– Kausalität 20 28  
– Liquidierung 20 24  
– mass claims 20 26  
– Mitverschulden 20 29 ff.  
– Schadensabwendung 20 33 f.  
– Schadensersatz in Geld 20 24  
– Schadensminderung 20 33 f.  
– Verbraucherschäden 20 26  
Ersteinschätzung 38 5 ff.  
Erstmeldung 37 51, 91, 99  
ESA, federführende Überwachungsbehörde 5 24  
Escape Rate 39 20  
ESMA, Finanzmarkt 9 16  
EU 9 9  
EU5G 23 38, 41  
– Ko-Regulierung 23 41  
EUCC 23 38 f.  
– Ko-Regulierung 23 39  
EUCS 23 36, 40  
– BSI C5 23 40  
– Entwicklungsstand 23 40  
– ISO 27001 23 40  
– Ko-Regulierung 23 38  
– Kritik 23 40  
– SecNumCloud 23 40  
– Verhältnis zu nationalen Zertifizierungsprogrammen 23 40  
EU-Cybersicherheitsstrategie  
– Behörden 5 1  
– Rechtsakte 5 1  
– Regulierung 5 1  
Europäische Cybersicherheitsstrategie 13 28  
Europäische Datenschutzbeauftragte 13 6  
Europäische Zertifizierungsprogramme 44 34, 43 ff.  
– EU5G 44 43  
– EUCC 44 43  
– EUCS 44 43  
Europarat-Übereinkommen zu Cyberkriminalität 11 18  
European Cybersecurity Scheme  
– Harmonisierung 23 37  
– Ko-Regulierung 23 37 ff.  
– Mehrwert 23 37 ff.  
– Rechtsgrundlage 23 37 ff.  
– Verhältnis zu nationalen Zertifizierungsprogrammen 23 37  
European Platform on Rare Disease 1 90  
European Rare Disease Registry Infrastructure 1 90  
Evasion Attack 39 26  
Exfiltration 39 35  
Exit Management 27 39 ff.  
Exitstrategie 19 18  
Explainable AI 25 19