Nomos **STICHWORTKOMMENTAR**

Nink [Hrsg.]

Digitale Sicherheit

Governance | Recht | Technik

Nomos

Nomos **STICHWORTKOMMENTAR**

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

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

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*)

Margaretha Opalewski
Beraterin für Informationssicherheit, HiSolutions AG, Nürnberg

Informationssicherheitsmanagementsystem (ISMS)
(mit *Neweling*)

Dr. Carlo Piltz
Rechtsanwalt, Berlin

Cyberkriminalität – Data Protection by Design – Privacy by Design
(mit *Weiss*)

Christoph Y. Pitzer, LL.M. oec.
Rechtsanwalt, Köln

Produktsicherheit

Künstliche Intelligenz
(mit *Müller*)

Prof. Dr. Matthias Reintjes
Hochschule-Rhein-Waal

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

Dr. Tobias Rothkegel
Rechtsanwalt, Hamburg

Outsourcing – Sicherheitsvorfall, allgemein – Sicherheitsvorfall, Bearbeitung

DORA und finanzaufsichtsrechtliche Auslagerung
(mit *Walter*)

Philipp Christopher Rothmann
Geschäftsführender Gesellschafter IT-Security Coach GmbH, Olpe

Authentizität – Datenschutzmanagementsystem – Datenverschlüsselung – Schutzziele – Technische und organisatorische Maßnahmen (TOM)

Cybersicherheit
(mit *Nink*)

Resilienz
(mit *Müller*)

Sicherheitsbeauftragter
(mit *J. Zaudig*)

Dr. Daniel Walter
Rechtsanwalt, Köln

DORA und finanzaufsichtsrechtliche Auslagerung
(mit *Rothkegel*)

Alexander Weiss
Rechtsanwalt, Berlin

Cyberkriminalität – Data Protection by Design – Privacy by Design
(mit *Piltz*)

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, Dokumentation – Audits und Zertifizierungen, Vorbereitung – Dienstleister, Checkliste Sicherheitsprüfung externe Dienstleister – Dienstleister, Checkliste Auftragsverarbeitung – Informationssicherheit

Dienstleister, allgemein
(mit *Nink*)

1. Anonymisierung

Frank Ingenrieth

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/Venkitasubramaniam, ℓ-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.[1] 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-

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 anonymer 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, Aggregierung, 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.[2]

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[3]
  - Privacy Protection: p-Sensitive k-Anonymity Property[4]
  - ℓ-Diversity: Privacy Beyond K-Anonymity[5]
  - Praxisleitfaden zum Anonymisieren personenbezogener Daten, Stiftung Datenschutz[6]
  - Praxishilfe zur Anonymisierung/Pseudonymisierung, Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie[7]
- 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[8]
  - Technische Leitlinie der Spanischen Datenschutzaufsicht im Bereich K-Anonymity[9]

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.

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.

5 Machanavajjhala/Kifer/Gehrke/Venkitasubramaniam, ℓ-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.

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.

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.

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

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

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-ensure-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.

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.

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, 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. 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[19] (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.[20] Konzeptionelle Grenzwerte hinsichtlich anonymer Daten werden Abwägungsentscheidungen aus unterschiedlichen Disziplinen sein. Hierzu wird möglicherweise ein – standardisiert quantifizierbares – Risiko der Anonymauflösung[21] gehören sowie andere (Risiko-)Faktoren, möglicherweise bezüglich der potenziellen Verkettungspotenziale. Es ist zu erwarten, dass im Wesentlichen zwei Aspekte die finale Würdigung künftig beeinflussen: 17

- 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. 18

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

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.

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, Ziffer 6. Dort wird auf ein quantifizierbares Risiko der Anonymauflösung abgestellt.

at-Scale-Konzepten, oder etwa auch in Form etwaiger Second-Life Use-Cases künftig ausgedienter Hardware.[22]

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.[23] 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.[24] 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.[25]

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

Obgleich 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

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

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 Quartalserlöse. 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.[26]

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

26 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;[27] 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**.[28]
- Ermöglichen die verrauschten Daten ggf. **Fehlidentifikationen**?[29]

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 **Vereinzelung**. 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.

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.[30]

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.[31] 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.