UNIKASSEL
VERSITÄT

WS 2023/24

FB Wirtschaftswissenschaften

Modul „Verwaltungsrecht“

Hausarbeit zum Thema

# Die Anonymisierung von personenbezogenen Daten im Kontext von BIG DATA

**Dozent/Dozentin: Prof. Dr. Uta Hildebrandt**

Datum der Abgabe: 25.11.2023

Wörter: 3326

Verfasser Benjamin Bleske
Studiengruppe: MPA 53B NRW
Matrikelnummer: 36104066

# INHALTSVERZEICHNIS

Abkürzungsverzeichnis ..... iii

1 Einleitung ..... 1

2 Datenschutzrecht ..... 2

2.1 Historie ..... 2

2.2 Eröffnung des Anwendungsbereichs der DS-GVO ..... 5

2.3 Die Personenbezogenheit ..... 6

2.4 Identifizierbarkeit innerhalb der Personenbezogenheit ..... 7

2.4.1 Die direkte und indirekte Identifizierbarkeit ..... 7

2.4.2 Absoluter Ansatz ..... 8

2.4.3 Relativer Ansatz ..... 9

3 Anonymisierung von personenbezogenen Daten ..... 10

3.1 Die Anonymisierung im Vergleich zur Pseudonymisierung ..... 10

3.2 Rechtliche Anonymisierung ..... 11

3.3 Technische Anonymisierung ..... 11

3.4 Essenz der Anonymisierung ..... 12

4 Big Data ..... 12

5 Fazit ..... 13

Literaturverzeichnis ..... 15

Eidesstattliche Erklärung & Einwilligungserklärung Nutzung von Plagiatssoftware ..... 19

## Abkürzungsverzeichnis

DS-GVO ..... *Datenschutz-Grundverordnung*
BDSG ..... *Bundesdatenschutzgesetz*
EuGH ..... *Europäischer Gerichtshof*

Hinweis im Sinne des Gleichbehandlungsgesetzes:

Aus Gründen der leichteren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung verzichtet. Die in dieser Arbeit verwendeten Begriffe gelten im Sinne der Gleichbehandlung für alle Geschlechter.

# 1 Einleitung

Die digitale Datenflut schwillt unaufhaltsam an. Big Data als treibende Dynamik des Informationszeitalters hat ein komplexes Ökosystem geschaffen, in der das Recht des Individuums auf informationelle Selbstbestimmung[1] mit dem mantrischen Verlangen, immer mehr Daten miteinander zu vernetzten, kollidiert.[2] Dabei beschreibt Big Data zunächst nur den Umstand von großen und vielfältigen Datenbeständen, die ohne spezifische Technologien und analytische Methoden wertlos sind.[3] Dennoch gilt Big Data als das Ende der Anonymität, denn im Zeitalter von Big Data sind alle Daten personenbezogen. [4]

In diesem Kontext stellt sich die Frage nach der heutigen Legitimität von Anonymisierungsvorgängen, um personenbezogene Daten in anonyme Daten zu transformieren. Denn rückblickend galt das Arbeiten mit ehemals personenbezogenen Daten, die anonymisiert worden waren, als juristisches Heilmittel, um nicht den weiten sachlichen Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO)[5] zu eröffnen.[6]

Genau an diesem Punkt hat das Big Data Konzept eine unzweifelhaft existenzbedrohende Wirkung auf das höchstpersönliche Datenschutzrecht: die strukturell prägende Differenzierung zwischen personenbezogenen Daten und nicht-personenbezogenen Daten wird aufgebrochen.[7]

Es bleibt daher die Frage, ob und inwieweit eine Anonymisierung den datenschutzrechtlichen Anforderungen, die eine Anonymisierung im Big Data Zeitalter voraussetzt, Rechnung trägt.[8] Wohlmöglich wird das Erreichen der kritischen Menge, an dem ein Datenschutzkalkül im Big Data Ökosystem tatsächlich kippt, irrtümlich eingeschätzt und die Auswirkungen, die Individuen erleben müssen, sind auf „[…] personalisierte Werbung, personalisierte

[1] BVerfG Urt. v. 15.12.1983 – 1 BvR 269/83, BeckRS 1983, 107398, beck-online, Ls. 1.
[2] Hoeren/ Uphues, in: Frenz, Big Data in Industrie 4.0, S. 116f.
[3] De Mauro/Greco/Grimaldi, Library Review 2016, 122, 131.
[4] Boehme-Neßler, DuD 2016, 419, 423.
[5] Datenschutz-Grundverordnung (DS-GVO) Verordnung Nr. 2016/679 des Europäischen Parlaments und Rates vom 27.4.2016 (ABl. 119 vom 4.5.2016, S. 1)
[6] Hölzel, DuD 2018, 502, 502.
[7] Boehme-Neßler, DuD 2016, 419, 423.
[8] Hölzel, DuD 2018, 502, 502.

Trefferlisten und fortlaufend aktualisierte Informationsangebote (sogenannte newsfeed) sowie personalisierte Preise […]“[9] begrenzt, aber wohlmöglich befinden wir uns auch zeitgeschichtlich erneut an einem *The Right to Privacy*[10] Moment, der eine datenschutzrechtliche Anpassung an eine technologische Neuerung fordert.[11]

# 2 Datenschutzrecht

## 2.1 Historie

Datenschutz ist omnipräsent. Dabei wird oft die Tatsache verkannt, dass Datenschutz nicht unmittelbar für Datenschutzrecht oder als ein Synonym für DS-GVO steht. Denn mit einer steigenden Bekanntheit der DS-GVO in den Unternehmen und in der Bevölkerung[12] rückt die Rechtsverordnung vielerorts in das ausschließliche Zentrum des Blickfeldes.

Vielmehr ist der Datenschutz das Versprechen eines abstrakt-generellen Wirkungsgefüges, das sich im konkret-generellen Anwendungsbereich des Datenschutzrechts organisiert. Dabei ist insbesondere die DS-GVO eine der konkret-individuellen Ausprägungen, um ein Versprechen des Datenschutzes einzufordern. Um die Individualisierung dieser Ausprägung zu rekonstruieren, ist hierzu ein Blick hinter dem blickdichten Dickicht des Datenschutzes zu werfen.[13]

Bereits in der Antike können die ersten Wurzeln des Datenschutzes gefunden werden.[14] Wäre das Publikmachen der Beschwerden eines Patienten durch den behandelnden Arzt gängige Praxis gewesen, hätten die Patienten der Antike wohlmöglich aus Angst vor sozialer Ausgrenzung auf einen Arztbesuch verzichtet.[15] Auch im Mittelalter entwickelte man ein Gefühl für die Macht von Informationen und gleichermaßen für das Erfordernis, Informationsmonopole zu verhindern.[16] Der Schutz der Privatsphäre genießt demnach einen historisch hohen Stellenwert.

---

[9] Biesenbach, in: Frenz, Aspekte digitaler Transformation der Justiz, S. 13f.
[10] Warren/Brandeis, Harvard Law Review 1890, 193, 193-220.
[11] ebd., 193, 195.
[12] DDV, Datenschutz-Report 2022, Pressemitteilung v. 29.04.2022
[13] Zimmermann, Datenschutz und Demokratie, S. 18.
[14] Lewinski, in: Lewinski/Rüpke/Eckhardt, §2, Rn. 6ff.
[15] Zimmermann, Datenschutz und Demokratie, S. 21.
[16] Lewinski, in: Arndt et al., S. 206ff.

1890 wird von Warren und Brandeis in *The Right to Privacy*[17] der Privatsphärenschutz in ein subjektives Recht gegossen.[18] Die Notwendigkeit für die Individualisierung des Privatsphärenschutzes wurde bereits damals aus dem zwingenden Erfordernis der Anpassung des Rechts an den technischen Fortschritt und den gesellschaftlichen Wandel hergeleitet.[19] Warren und Brandeis zogen als Katalysator die Entwicklung von Sofortbildkameras und dem damit einhergehenden boomenden Zeitungsgeschäft heran.[20] Dass ihre Gedanken später als ein Ausgangspunkt des heutigen Datenschutzrechts als Ausprägung des allgemeinen Persönlichkeitsrechts darstellen würden, konnten sie nicht ahnen.[21]

Datenschutzrechtliche Geschichte im engeren Sinne wurde in den Jahren 1970 – 1983 geschrieben.[22] Mit Erlass des weltweit ersten Datenschutzgesetzes[23] setzt Hessen 1970 neue Maßstäbe.[24] Die Absicht war es, den negativen Folgen der Digitalisierung entgegenzuwirken.[25] Es folgte das Inkrafttreten des Bundesdatenschutzgesetztes im Jahre 1978.[26] Trotz des steigenden Interesses des Gesetzgebers am Datenschutz war das Datenschutzrecht noch nicht ausschließlich auf den Schutz des Individuums gerichtet.[27]

Die *Konvention 108* des Europarats von 1981 ist das erste internationale Vertragswerk, das auf den Schutz von personenbezogen Daten abzielt.[28] Kurz danach folgt 1983 das Volkszählungsurteil des Bundesverfassungsgerichts[29], das der staatlichen Datenverarbeitung durch die Prinzipien der Zweckbindung und Erforderlichkeit enge Grenzen setzt.[30] Von nun an gewährleistet das Recht auf informationelle Selbstbestimmung „die Befugnis des Einzelnen, grundsätzlich über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

---

[17] Warren/Brandeis, Harvard Law Review 1890, 193, 193-220.
[18] Zimmermann, Datenschutz und Demokratie, S. 23f.
[19] Warren/Brandeis, Harvard Law Review 1890, 193, 195.
[20] ebd.
[21] Zimmermann, Datenschutz und Demokratie, S. 25.
[22] Von dem Bussche, in: Frenz, Datenschutz 4.0, S. 156.
[23] GVBl. I 1970, 625.
[24] Von dem Bussche, in: Frenz, Datenschutz 4.0. S. 156.
[25] Schaar, Informatik Spektrum 2020, 179, 181.
[26] BGBl. I 1977, S. 201ff.
[27] Zimmermann, Datenschutz und Demokratie, S. 36.
[28] Counsil of Europe v. 28.1.1981, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
[29] BVerfG Urt. v. 15.12.1983 – 1 BvR 269/83, BeckRS 1983, 107398, beck-online.
[30] Kubicek/Breiter/Jarke, in: Klenk/Nullmeier/Wewer, Handbuch Digitalisierung, S. 2.

Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung“ sind nur im überwiegenden Allgemeininteresse zulässig.“[31], so konstatieren die Leitsätze des Volkszählungsurteils. Der Vollständigkeitshalber ist an dieser Stelle noch auf das Inkrafttreten des Bundesdatenschutzgesetzes a.F. (BDSG) im Jahre 2003 hinzuweisen.[32]

Das Datenschutzrecht stammt demnach aus den 1970er Jahren und kann schon systemlogisch nicht allen technischen Erfindungen der Neuzeit wirksam begegnen.[33]

Daher musste das Datenschutzrecht erneut angepasst werden. Seit dem 25. Mai 2018 ist die DS-GVO in allen Mitgliedsstaaten der europäischen Union direkt anwendbares Recht. Neben der harmonisierenden Wirkung für das Datenschutzrecht innerhalb der Union erhalten die Datenschutzbehörden die Möglichkeit, Datenschutzverstöße direkt zu ahnden. Dazu können die ahnenden Stellen Geldbuße bis zu 20 Millionen Euro oder darüber hinaus bis zu 4 % des Konzernumsatzes erheben.[34]

Zeitgleich mit dem Eintreten der DS-GVO trat das neue Bundesdatenschutzgesetz (BDSG)[35] in Kraft. Die Subsidiarität des BDSG führte zu einem kaum zu durchdringenden dichtbesiedelten Forst aus bereichsspezifischen, speziellen datenschutzrechtlichen Rechtsgrundlagen.[36] Neben spezielleren bundesrechtlichen Datenschutzregelungen in Fachgesetzen, erschweren 16 Landesdatenschutzgesetzte, und weitere speziellere Datenschutzregelungen in den Fachgesetzten der Länder, die Prüfung eines wohlmöglich datenschutzrechtlich relevanten Sachverhaltes.[37]

Mithin ist das gegenwärtige Datenschutzrecht ein klares Ergebnis der Fortentwicklung des Datenschutzrechts der 1970er Jahre, allerdings lassen sich die Ursprünge des Datenschutzes mindestens 1500 Jahre bis zu den antiken Ärzten zurückverfolgen. Mitnichten ist es daher eine Entwicklung des 20. Jahrhunderts oder des Informationszeitalters.

---

[31] BVerfG Urt. v. 15.12.1983 – 1 BvR 269/83, BeckRS 1983, 107398, beck-online, LS. 1f.
[32] BGBl. I 2003, S. 66ff.
[33] Boehme-Neßler, DuD 2016, 419, 423.
[34] Schaar, Informatik Spektrum 2020, 179, 181.
[35] BGBl. I 2017, S. 2097ff.
[36] Wolff/Brink/v. Ungern-Sternberg-Gusy/Eichenhofer, § 1 BDSG, Rn. 78a.
[37] Schlingloff, Juristische Ausbildung 2022, 1255, 1255f.

## 2.2 Eröffnung des Anwendungsbereichs der DS-GVO

Die DS-GVO enthält nach Artikel 1 Absatz 1 Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr derartiger Daten.

Ihr sachlicher Anwendungsbereich ist nach Artikel 2 Absatz 1 eröffnet, sobald personenbezogene Daten verarbeitet werden. Für das Vorliegen eines personenbezogenen Datums ist es nach Artikel 4 Satz 1 Nummer 1 ausreichend, dass sich mithilfe einer Information jedweder Art eine Person identifizieren[38] lässt. Zusätzlich muss das personenbezogene Datum nach Artikel 2 Absatz 1 verarbeitet werden. Dieses Tatbestandsmerkmal ist im Wesentlichen unbeachtlich, da im Grunde jeder Vorgang, der nur schon ein personenbezogenes Datum enthält, eine Verarbeitung im Sinne der Norm darstellt. Es kann sogar ausreichen, dass ein Vorgang nur im Zusammenhang mit personenbezogenen Daten steht, um den Anwendungsbereich zu eröffnen.[39]

Der räumliche Anwendungsbereich der Verordnung findet nach Artikel 3 Absatz 1 Anwendung, soweit dieser im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der europäischen Union erfolgt. Das sogenannte Niederlassungsprinzip erstreckt sich ausschließlich auf den Ort der Niederlassung.[40] Demnach schützt das Outsourcing von Vorgängen in Drittländer nicht vor der Eröffnung des räumlichen Anwendungsbereichs der DS-GVO.[41] Sofern der Verantwortliche im Sinne der Norm nicht ansässig in der Union ist, kann die DS-GVO dennoch nach Artikel 3 Absatz 2 Anwendung finden. Bei dem sogenannten Marktortsprinzip kommt es darauf an, ob die Datenverarbeitung im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen an Personen in der Union steht oder ob es um Verhaltensbeobachtung betroffener Personen geht, soweit ihr Verhalten in der Union erfolgt.[42]

---

[38] Das BDSG a.F. nutzte die Begriffskonstruktion der Bestimmbarkeit anstelle der Identifizierbarkeit von Personen, um eine Personenbezogenheit herzustellen. Im Wesentlichen ist teleologisch dasselbe gemeint, siehe dazu Bernauer, BRJ 01/2018, 12, 12f., 15.

[39] Simitis/Hornung/Spiecker gen. Döhmann-Roßnagel, Art. 4 DS-GVO, Rn. 10-13.

[40] Von dem Bussche, in: Frenz, Datenschutz 4.0. S. 163.

[41] Simitis/Hornung/Spiecker gen. Döhmann-Hornung, Art. 3 DS-GVO, Rn. 27.

[42] Von dem Bussche, in: Frenz, Datenschutz 4.0. S. 163.

### 2.3 Die Personenbezogenheit

Personenbezogene Daten sind im Sinne von Art. 4 Nummer 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Identifizierbar ist eine natürliche Person, sobald sie mittels der Zuordnung zu einer Kennung wie einem Namen, einer Nummer, einem Standort oder anderen besonderen Merkmalen bestimmt werden kann. Demnach ist jede Information, die nach einem normalen Lauf der Dinge potenziell mit anderen Informationen zusammen die Identifikation einer natürlichen Person ermöglicht, personenbezogen.[43]

Nach Auffassung des Europäischen Gerichtshof (EuGH) ist der Begriff des Personenbezugs gemäß seines Schutzzwecks weit auszulegen.[44] Demnach seien personenbezogene Daten potenziell alle Arten von Informationen, und zwar unabhängig davon, ob sie einen objektiven oder subjektiven Ursprung haben.[45] Daher können auch Stellungnahmen und Beurteilungen oder auch abgeleitete Informationen der original erhobenen Daten personenbezogenen sein.[46] Besondere Brisanz entfalten personenbezogene Daten im Kontext von Einschätzungen zur Kreditwürdigkeit einer Person, die wohlmöglich auf Grund einer schlechten Bewertung einen künftigen Vertrag nicht abschließen kann.[47] Die Weite des Begriffs schließt auch die Eigenschaften einer Person, ihre Verhaltensweisen, ihre Beziehungen oder spezielle identifizierende Angaben ein.[48]

Die vielseitigen Erscheinungsformen von personenbezogenen Daten sind unbegrenzt. So mögen Geodaten wie zum Beispiel Luft- oder Satellitenbilder auf den ersten Anschein nicht wie typische personenbezogene Daten wirken. Dabei kann bei Geodaten ein Personenbezug über die Ortsfunktion (1. Aufenthalt 2. Nutzungsbeziehung (Bewohner oder wirtschaftlich Nutzender) 3. Eigentum) hergestellt werden und dabei gilt, je hochauflösender das Luft- oder Satellitenbild, desto höher ist die Chance, eine Person zu identifizieren und damit den Anwendungsbereich der DS-GVO zu eröffnen.[49] Der systemische Rückschluss ist hierbei, dass es sich ab einer bestimmten Auflösung nicht mehr um personenbezogene Daten handeln

---

[43] Niemann/Kevekordes, CR 2020, 17, 18f.
[44] EuGH, Urteil vom 4. Mai 2023 – *F. F./Österreichische Datenschutzbehörde*, C-487/21, NJW 2023, 2254f., beck-online, Rn. 23-26.
[45] ebd.
[46] ebd.
[47] Boehme-Neßler, DuD 2016, 419, 419f.
[48] ebd.
[49] Weichert, DuD 2009, 347, 350.

kann. Praktisch bedeutetet das, dass das Bild, das bei einer bestimmten Zoomstufe betrachtet wird, nur noch aus wenigen Pixeln besteht, sodass man darauf keine Person mehr erkennen kann und sogar einzelne Häuser zu einer einfarbigen Masse verschwimmen.

Bei diesem Beispiel wird klar, dass bestimmte Anforderungen an eine Identifizierbarkeit gestellt werden müssen, um einen Personenbezug zu bejahen.

## 2.4 Identifizierbarkeit innerhalb der Personenbezogenheit

### *2.4.1 Die direkte und indirekte Identifizierbarkeit*

Für fast alle Bestimmungen des Datenschutzes ist die Frage, wie Artikel 4 Nummer 1 DS-GVO in Verbindung mit Erwägungsgrund 26 auszulegen ist, relevant.[50] Dabei stürzt sich der Diskurs auf das Merkmal identifizierbar bzw. Identifizierbarkeit.[51]

Bei der Identifizierbarkeit handelt es sich um die Frage, ob zwischen der Person und der Information eine Verbindung hergestellt werden kann.[52] Dabei wird zwischen der direkten und indirekten Identifizierbarkeit unterschieden.[53] Direkt identifizierbar ist eine natürliche Person durch ihren Namen in Verbindung mit weiteren Merkmalen wie dem Geburtsdatum, dem Geburtsort, einer Adresse, einem Foto oder der Namen der Eltern.[54] Weitere direkte Merkmale sind die Sozialversicherungsnummer und die Steueridentifikationsnummer.[55]

Eine natürliche Person ist indirekt identifizierbar durch beispielsweise ihre Telefonnummer, ihre Personalausweisnummer oder durch das Autokennzeichen. Hierzu gehören alle Daten, die ein Wiedererkennen ermöglichen, auch wenn die Daten auf Anhieb keine Identifizierbarkeit herstellen.[56] Daher können Luft- und Satellitenbilder ab einer bestimmten hochauflösenden Darstellung ebenfalls personenbezogene Daten darstellen, denn sie lassen den Schluss auf eine sich auf einem Grundstück befindliche Person zu, zu dem es eine eindeutige Adresse gibt. Denn die Identifizierbarkeit einer Person setzt nicht die Kenntnis eines Namens

[50] Assion, NJW 2023, 2619, 2619.
[51] ebd.
[52] Von dem Bussche, in: Frenz, Datenschutz 4.0. S. 159f.
[53] Wolff/Brink/v. Ungern-Sternberg-Schild, Art. 4 DS-GVO, Rn. 14ff.
[54] ebd.
[55] ebd.
[56] ebd.

voraus.[57] Das Wissen um den Aufenthaltsort dieser unbekannten Person ist dabei ausreichend.[58]

Es ist daher stets im Einzelfall zu prüfen, ob und wie hoch die Wahrscheinlichkeit ist, dass ein Personenbezug über eine Identifizierbarkeit herstellbar ist.[59] Zu dieser Weichenstellung herrscht ein annähernd historischer Streit, ob bei der Frage, ob eine natürliche Person identifizierbar ist, ein absoluter oder ein relativer Ansatz anzusetzen ist.[60] Im Kern dreht es sich hierbei um die Frage, ob es für die datenverarbeitende Stelle praktisch möglich sein muss, einen Personenbezug herzustellen oder ob die Herstellung eines Personenbezugs nur theoretisch denkbar sein muss. Diese Frage ist vor allem interessant für alle datenverarbeitenden Stellen, die nicht originär personenbezogene Daten erheben, sondern nur mit den regelmäßig reduzierten Derivaten ebendieser Daten arbeiten. Hier wird durch die originären datenhaltenden Stellen der Datensatz mittels Anonymisierungstechniken dergestalt verändert, dass dieser vermeintlich nicht mehr personenbezogen ist. Daher beantwortet die Wahl des absoluten oder relativen Ansatzes die Frage, ob Anonymisierung als „legale Möglichkeit zur Flucht aus dem Datenschutzrecht“[61] rechtmäßig ist.

### *2.4.2 Absoluter Ansatz*

Der absolute Ansatz (vor Inkrafttreten der DS-GVO auch als objektive Theorie im Kontext der indirekten Bestimmbarkeit bezeichnet) folgt der Auffassung, dass es für die Bejahung der Identifizierbarkeit - und damit für das Vorliegen eines personenbezogenen Datums - ausreichend ist, sofern eine dritte Stelle über ausreichend Wissen verfügt, um bei einem Datum einen Personenbezug herzustellen.[62] Es kommt danach nicht darauf an, ob die datenverarbeitende Stelle das Wissen hat, den Personenbezug herzustellen. Vielmehr wird der datenverarbeitenden Stelle das Wissen einer dritten Stelle zugerechnet.[63] Dabei wird gänzlich auf

[57] ebd.
[58] Weichert, DuD 2009, 347, 350.
[59] Von dem Bussche, in: Frenz, Datenschutz 4.0. S. 159f.
[60] EuG Urt. v. 26.4.2023 – T-557/20, ZD 2023, 399, 402 beck-online.
[61] Pohle/Hölzel, BfDI, Stellungnahme d. Alexander von Humboldt Institut für Internet u. Gesellschaft v. 29.06.2020, S. 4.
[62] Boehme-Neßler, DuD 2016, 419, 420.
[63] Bergt, ZD 2015, 365, 370.

das Einpreisen des ökonomischen, zeitlichen oder technologischen Aufwands der datenverarbeitenden Stelle verzichtet, den ebenjene datenverarbeitende Stelle einsetzen müsste, um einen Personenbezug herzustellen.[64]

Die europäischen Datenschutzaufsichtsbehörden - insbesondere die deutschen – und der Europäische Datenschutzbeauftragte tendieren zum absoluten Ansatz.[65]

### *2.4.3 Relativer Ansatz*

Die rechtsprechende Gewalt Europas folgt dem relativen Ansatz.[66] Das Europäische Gericht geht davon aus, dass eine Identifizierung praktisch durchführbar sein muss.[67] Das ist insbesondere nicht der Fall, wenn die Identifizierung einen unverhältnismäßig hohen Aufwand darstellen würde, sodass das Risiko einer Identifizierung gering und daher vernachlässigbar ist.[68] Auch der Europäische Gerichtshof folgt dem relativen Ansatz. So lässt sich das Wissen eines Dritten nicht unbegründet einer datenverarbeitenden Stelle zurechnen.[69] Sofern kein gesetzlicher oder vertraglicher Anspruch besteht, das identifizierendes Zusatzwissen in den Besitz der datenverarbeitenden Stelle gelangt, kann kein Personenbezug über die Zurechnung des Wissens hergestellt werden. Eine hypothetische Möglichkeit reicht daher nicht mehr aus.

Demnach gilt die Faustformel, je schwieriger die Personenbestimmung für die datenverarbeitende Stelle ist, desto weniger bestimmbar ist eine Person nach dem relativen Ansatz.[70] Die Wahrscheinlichkeit für die Personenbestimmung hängt insbesondere und vor allem vom personellen, finanziellen und technologischen Aufwand ab, der von der datenverarbeitenden Stelle investiert werden müsste, um einen Personenbezug herzustellen.[71] Der relative Ansatz

---

[64] Boehme-Neßler, DuD 2016, 419, 420.
[65] EuG Urt. v. 26.4.2023 – T-557/20, ZD 2023, 399, 403 beck-online.
[66] EuG Urt. v. 26.4.2023 – T-557/20, ZD 2023, 399, 399 beck-online, auch EuGH, Urteil vom 19. Oktober 2016 – *Breyer/ Deutschland,* C-582/14, NJW 2016, 3579, beck-online.
[67] EuG Urt. v. 26.4.2023 – T-557/20, ZD 2023, 399, 403 beck-online.
[68] ebd.
[69] ebd.
[70] ebd.
[71] ebd.

geht davon aus, dass es absolute Anonymität nicht geben kann.[72] Demnach erfolgt eine klassische Abwägung. Boehme-Neßler etwa bezeichnet den relativen Ansatz als den pragmatischen Weg im Kontrast zum absoluten Ansatz.[73]

Wenn man beide Ansätze miteinander vergleicht, kommt man zu dem Ergebnis, dass die Ansätze bei einem niedrigem Bestimmbarkeitsaufwand dasselbe Ergebnis haben. Es handelt sich sodann um Daten, die Personen indirekt identifizierbar machen. Bei einem hohen Bestimmbarkeitsaufwand geht der absolute Ansatz von einer Identifizierbarkeit aus, da es für diesen Ansatz unerheblich ist, wie hoch der Bestimmbarkeitsaufwand ist. Der relative Ansatz hingegen geht andersherum davon aus, dass das Datenschutzrecht wegen des fehlenden Personenbezugs nicht anwendbar ist, weil der Aufwand der betrieben werden müsste, um eine Identifizierbarkeit herzustellen, unverhältnismäßig groß ist.

# 3 Anonymisierung von personenbezogenen Daten

## 3.1 Die Anonymisierung im Vergleich zur Pseudonymisierung

Anonyme Daten sind das genaue Gegenteil von personenbezogenen Daten, außer für die Stelle, die die Daten anonymisiert hat, da sie wohlmöglich über das nötige Zusatzwissen verfügt, die Daten wieder zu de-anonymisieren.[74] Eine Anonymisierung ist demnach ein Vorgang, der den Personenbezug eines Datums neutralisiert.[75] Dieser Umstand führt dazu, dass die Anwendbarkeit datenschutzrechtlicher Regelungen hinfällig wird.[76] Die Anonymisierung ist jedoch abzugrenzen von der Pseudonymisierung. Die Pseudonymisierung wird explizit in der DS-GVO in Art. 4 Nummer 5 erwähnt.[77] Hiernach handelt es sich um Daten, die unter Heranziehung zusätzlicher Informationen einen Personenbezug herstellen. Bei der Pseudonymisierung ist die Möglichkeit zur Umkehr ihrer gewollt, aber sie dient dennoch primär dazu, die Wahrscheinlichkeit der Bestimmbarkeit einer Person zu reduzieren.[78] So kann ein Klarname durch ein Pseudonym ersetzt werden, während bei einer Anonymisierung

[72] ebd.
[73] ebd.
[74] Selzer/Timm, DuD 2021, 816,817.
[75] ABl. L 119/1 Erwgr. 26.
[76] Ulbricht, in: Dorschel, Anonymisierung und Pseudonymisierung; Verschlüsselung, S. 186.
[77] Die Anonymisierung wird nur im Erwägungsgrund 26 zur DS-GVO erwähnt.
[78] Esayas, EJLT 2015, S.8.

der Klarname wohlmöglich gelöscht wird. Demnach ermöglicht die Pseudonymisierung Datensätze mit demselben Pseudonym zu verketten (und große Datensammlungen zu einem Pseudonym zu bilden), während dies bei der Anonymisierung explizit nicht gewollt ist.[79] Daher sind pseudonymisierte Daten insbesondere im Kontext von Big Data Anwendung äußerst nützlich.[80]

### 3.2 Rechtliche Anonymisierung

Die rechtliche Begrifflichkeit der Anonymisierung aus dem Erwägungsgrund 26[81] zur DS-GVO bedient sich exklusiv der Rechtskonstruktion zur Identifizierbarkeit. Demnach sind Daten, die direkt oder indirekt eine Person identifizierbar machen, keine anonymen Daten, die einer vorherigen Anonymisierung unterlagen, sondern personenbezogen. Da nach der rechtlichen Betrachtung ein relativer Ansatz bei der Identifizierbarkeit zugrunde gelegt werden muss, handelt es sich hierbei also ebenfalls um eine rechtlich pragmatische Abwägung zwischen dem nötigen Mitteleinsatz und der Wahrscheinlichkeit der Bestimmbarkeit einer Person.[82]

### 3.3 Technische Anonymisierung

Unabhängig des gewählten Verfahrens transformiert die technische Anonymisierung ein Input-Datum, in diesem Fall ein personenbezogenes Datum, in ein Output-Datum, in diesem Fall ein nicht personenbezogenes Datum. Das Verfahren hat zunächst nichts mit den daraus folgenden Implikationen für die Weiterverarbeitung mit (dann) nicht mehr personenbezogenen Daten zu tun.[83] Eine Anonymisierung im technischen Sinne stellt daher ebenfalls der Vorgang des Löschens eines Datensatzes dar, denn es transformiert einen personenbezogenen Input (z.B. Name in Zelle) in einen nicht mehr personenbezogenen Output (z.B. Leerzeile).[84] Der Erfolg einer Anonymisierung in technischer Hinsicht bestimmt sich negativ.[85] Sofern innerhalb des anonymisierten Ergebnisdatenbestandes nicht (mittels sog. „Record

[79] Ulbricht, in: Dorschel, Anonymisierung und Pseudonymisierung; Verschlüsselung, S. 188.
[80] ebd.
[81] ABl. L 119/1 Erwgr. 26.
[82] Hierzu näher in Kapitel 2.4.1 und 2.4.3.
[83] ebd, S. 4.
[84] ebd, S. 2.
[85] Hölzel, DuD 2018, 502, 503f.

Linkage“-Verfahren) Identitäten offengelegt werden können, handelt es sich mithin um anonymisierte Daten.[86]

### 3.4 Essenz der Anonymisierung

Das erklärte Ziel ist es, jede Möglichkeit die einen Rückschluss auf eine Person zulässt, zu unterbinden.[87] Der Erfolg der rechtlichen als auch technischen Anonymisierung bestimmt sich durch einen hinreichenden Grad der Unwahrscheinlichkeit einer Identifizierbarkeit. Dabei sind die nach allgemeinem Ermessen zur Verfügung stehenden Mittel einer datenverarbeitenden Stelle oder eines Angreifers zu berücksichtigen. Demnach rechnen beide Domänen per Definition mit einem akzeptablen Identifikationsrisiko.[88]

## 4 Big Data

Die rasant ansteigende Digitalisierung in der Unternehmenswelt und die zunehmenden Datenbestände verändern die Wertschöpfung entscheidend.[89] Big Data bzw. Massendatenbestände sind in der Lage die Wertschöpfungskette der gegenwärtigen Industrie völlig neu zu initialisieren.[90] Dabei bezeichnet Big Data als Sammelbegriff jene Informationen, die so voluminös, vielfältig und dynamisch sind, dass spezielle Technologien und Methoden erforderlich sind, um sie in Wert zusetzen.[91] Daher ist es auch fundamental wichtig für Big Data, dass massenhaft Daten vorliegen.[92] Dabei ist es Sinn und Zweck von Big Data Entscheidungen auf Basis von Datenanalysen zu treffen.[93] Systemlogisch wird Big Data zum Motor des Wettbewerbs, da sich bei näherer Betrachtung der kommerziellen Aspekte der Nutzung und Verkettung von Massendatenbeständen (z.B. bestehend aus Markt-,Kunden- und Nutzerdaten), ein mittelbarer Zwang ergibt, das Potential dieser neuen Methoden und Techniken zu nutzen.[94] Hiernach sind Ergebnisse dieser Datenanalysen in der Regel die Erkennung zusammenhängender Muster, Trends und Verbindungen in Bezug auf die Verhaltensweisen

[86] ebd.
[87] Ulbricht, in: Dorschel, Anonymisierung und Pseudonymisierung; Verschlüsselung, S. 186.
[88] Hölzel, DuD 2018, 502, 504ff.
[89] Hanika, in: Pfannstiel/Da-Cruz/Mehlich, Digitalisierung, Big Data und Big To-dos aus Sicht der Rechtswissenschaft, S. 74.
[90] Hoeren/ Uphues, in: Frenz, Big Data in Industrie 4.0. S. 117.
[91] De Mauro/Greco/Grimaldi, Library Review 2016, 122, 131.
[92] Dander, in: Iske/Fromme/Verständig/Wilde, Eine Kritische Politische Ökonomie von ‚Big Data‘, S. 85.
[93] Dorschel, in: Dorschel, Automatisierte Entscheidungen und Scoring, S. 211.
[94] Dorschel, in: Dorschel, Einführung, S. 4.

und die Interaktionen zwischen Kunden und Unternehmen.[95] Wertschöpfung kann so völlig neu gedacht werden. Dabei zählt, je mehr qualitativ hochwertige Datenbestände vorliegen, desto besser für die Muster- und Trenderkennung. So können Werbung, Trefferlisten, Informationsangebote oder Preise optimal und individuell für jedermann präsentiert werden.

# 5 Fazit

Sofern die Anonymisierung von personenbezogenen Daten weiterhin eine legale Flucht aus dem Datenschutzrecht bietet, werden die handelnden Akteure ungebremst und ungehindert diverse Datenbestände miteinander verknüpfen. Denn im Augenblick der Anwendung jener Akteurslogik, dass hinter der nächsten Analyse von neu verknüpften oder neu angebundenen Datenbeständen wohlmöglich der nächste große Trend schlummern könnte, um großartige Informationen (oder Gewinne) zu generieren, transformiert sich eine vormals innovative Produkt- oder Prozessentwicklung in ein rein abwägendes, eiskaltes Kalkül.

Dieser glücksspielartige, die Kreativität ausrottende Mechanismus und vor allem die daraus folgenden Implikationen für den grundrechtlich gewährten Datenschutz verbergen sich derzeit vor Legislative und Judikative. Die rechtsprechende Gewalt versteckt sich derzeit hinter dem so oft von der Exekutive geforderten Pragmatismus. Insoweit, als dass die Gerichte mit einer pragmatisch folgerichtigen, aber dennoch sachfremden Abwägung kontrollieren, ob ein Personenbezug hergestellt werden kann. Dabei wird unterstellt, dass derzeit eine natürliche oder juristische Person, sobald der Aufwand zu hoch wird, den Versuch, einen Personenbezug herzustellen, abbrechen. Die Entscheidung, ob ein personenbezogenes Datum (nach dem relativen Ansatz) vorliegt, hängt demnach von der Willkür und dem Einsatz derjenigen juristischen oder natürlichen Person ab, die das Datum verarbeitet. Und zwar wohlwissend, dass das Risiko eines identifizierenden Wiederherstellungsprozesses ewig währt und dass eine De-anonymisierung wohlmöglich nur einen technischen Fortschritt weit weg ist.

Sofern jedoch selbst die ausführende Gewalt ihre oberste Maxime opfert, die der Forderung nach Pragmatismus und realitätsnahem Verwaltungshandeln bei handelsüblichen Problemen entspricht, ist höchste Zurückhaltung geboten.

---

[95] Krämer/Mauer, Datenschutz für Entscheider in Marketing und Vertrieb 2023, S. 4f.

Das Naturgesetz von Big Data ist die Verkettung von Massendatenbeständen, um großartige Analysen abzufragen und bahnbrechende Erkenntnisse abzuleiten. Systemlogisch werden diejenigen handelnden Akteure die größte Macht in ihrer jeweiligen Domäne entfalten, die am meisten Datenbestände verknüpfen können, um die qualitativ hochwertigsten Erkenntnisse abzuleiten. Eine einmalig erlangte Poleposition ist sodann (beispielsweise aus der Marktsicht) unaufhaltbar.

Dieses Szenario wird zwangsläufig zu Lasten des derzeitigen Datenschutzrechts gehen. Und dabei wird es nicht um den Aufwand gehen, der betrieben werden muss, um eine Person zu identifizieren, da das Identifizieren der Person nicht im Zentrum der handelnden Akteure stehen wird. Dabei geht es einzig und allein um machtzentrierte Mechanismen, die Akteure dazu zwingen werden, Datenbestände aufzubauen, die seines gleichen suchen, um (im Duktus des Marktes zu bleiben) wettbewerbsfähig zu bleiben. Dass dabei unweigerlich das Risiko einer Identifizierbarkeit exponentiell steigt, ist hier nur eine nebulöse Nebenerscheinung, da die handelnden Akteure regelmäßig kein Interesse an einer Einzelperson haben werden. Hiernach wäre es also pragmatisch zu sagen, dass das Risiko einer Identifizierbarkeit gering ist, da die handelnden Akteure ausschließlich Trends erkennen wollen. Dennoch sind pragmatische Ansichten und die Eröffnung des Anwendungsbereichs der DS-GVO zwei verschiedene Stoßrichtungen.

Dabei ist es für die Einsicht, dass personenbezogene Daten immer personenbezogene Daten bleiben, unwesentlich, ob die Gerichte sich zunächst für einen relativen bzw. pragmatischen Ansatz entscheiden. Ein personenbezogenes Datum bleibt personenbezogen, unabhängig davon, wie stark es reduziert worden ist oder wie komplex der Umkehrmechanismus ist.

Insbesondere vor dem Hintergrund, dass die Mittel der Anonymisierung eines personenbezogenen Datums begrenzt sind, aber die Möglichkeiten, vermeintlich anonymisierte Datenbestände zu verknüpfen schier unmöglich sind, verfehlt der derzeitige Rechtsdiskurs seinen ursprünglich datenschutzrechtlichen Bezug im Kontext der Anonymisierung eines personenbezogenen Datums.

## Literaturverzeichnis

Assion, Simon, Die Entwicklung des Datenschutzrechts, in Neue Juristische Wochenschrift, Heft 36, 2023, S. 2619-2624.

Bergt, Mattias: Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag, in Zeitschrift für Datenschutz, Heft 8, 2015, S. 365-371.

Bernauer, Corinna: Die „neuen" personenbezogenen Daten in der DSGVO – Kontinuität und Änderungen, in Bonner Rechtsjournal, Ausgabe 01/2018, S. 12-15.

Biesenbach, Peter: Aspekte digitaler Transformation der Justiz; in Frenz, Walter (Hrsg.), Handbuch Industrie 4.0: Recht, Technik, Gesellschaft, Berlin 2020. https://doi.org/10.1007/978-3-662-58474-3_1.

Boehme-Neßler, Volker, Das Ende der Anonymität: Wie Big Data das Datenschutzrecht verändert, in Datenschutz und Datensicherheit, Ausgabe 7, 2016, S. 419–423.
Coucil of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data v. 28.01.1981. Onlinequelle bei: https://rm.coe.int/1680078b37. Abrufdatum: 2. November 2023.

Dander, Valentin: Grundzüge einer Kritischen Politischen Ökonomie von Big Data Analytics – und ihre bildungstheoretischen Implikationen; in Iske, Stefan / Fromme, Johannes / Verständig, Dan / Wilde, Katrin (Hrsg.), Big Data, Datafizierung und digitale Artefakte, Band 42, Wiesbaden 2020, S. 75-95. https://doi.org/10.1007/978-3-658-28398-8_5.

De Mauro, Andrea / Greco, Marco / Grimaldi, Michele, A formal definition of Big Data based on its essential features, Library Review, Vol. 65, No. 3, 2016, S. 122–135. https://doi.org/10.1108/LR-06-2015-0061.

Dorschel, Joachim / Dorschel, Werner: Einführung; in Dorschel, Joachim (Hrsg.), Praxishandbuch Big Data: Wirtschaft – Recht – Technik, Wiesbaden 2015. https://doi.org/10.1007/978-3-658-07289-6.

Dorschel, Joachim: Automatisierte Entscheidungen und Scoring; in Dorschel, Joachim (Hrsg.), Praxishandbuch Big Data: Wirtschaft – Recht – Technik, Wiesbaden 2015. https://doi.org/10.1007/978-3-658-07289-6.

Deutscher Dialogmarketing Verband (2022) Datenschutz-Report 2022: Die überwiegende

Mehrheit der Deutschen unterstützt die Data Economy, Pressemitteilung v. 29.04.2022. Onlinequelle bei: https://www.verbaende.com/news/pressemitteilung/datenschutz-report-2022-die-ueberw iegende-mehrheit-der-deutschen-unterstuetzt-die-data-economy-147819/. Abrufdatum: 2. November 2023.

Ehmann, Eugen / Selmayr, Martin (Hrsg.): Datenschutz-Grundverordnung, 2. Auflage, 2018 München.

Esayas, Samson, The Role of Anonymisation and Pseudonymisation Under the EU Data Privacy Rules: Beyond the ‚All or Nothing' Approach, in European Journal of Law and Technology, Vol. 6, No.2, 2015, S. 502–509.

Hanika, Heinrich: Digitalisierung, Big Data und Big To-dos aus Sicht der Rechtswissenschaft; in Pfannstiel, Mario A. / Da-Cruz, Patrick / Mehlich, Harald (Hrsg.), Digitale Transformation von Dienstleistungen im Gesundheitswesen VI, Band 6, 2019 Wiesbaden. https://doi.org/10.1007/978-3-658-25461-2.

Hoeren, Thomas / Uphues, Steffen: Big Data in Industrie 4.0; in Frenz, Walter (Hrsg.), Handbuch Industrie 4.0: Recht, Technik, Gesellschaft, Berlin 2020. https://doi.org/10.1007/978-3-662-58474-3_7.

Hölzel, Julian, Anonymisierungstechniken und das Datenschutzrecht, in Datenschutz und Datensicherheit, Ausgabe 8, 2018, S. 502–509.

Krämer, Andreas / Mauer, Reinhold, Datenschutz für Entscheider in Marketing und Vertrieb: Die DSGVO – Vom Spielverderber zum Wettbewerbsvorteil, Wiesbaden 2023. https://doi.org/10.1007/978-3-658-41902-8.

Kubicek, Herbert / Breiter, Andreas / Jarke, Juliane, Daten, Metadaten, Interoperabilität; in Klenk, Tanja / Nullmeier, Frank / Wewer, Göttrik (Hrsg.), Handbuch Digitalisierung in Staat und Verwaltung, Wiesbaden 2020. https://doi.org/10.1007/978-3-658-23669-4_1-1.

Lewinski, Kai V.: Geschichte des Datenschutzrechts von 1600 bis 1977; in Arndt, Felix et al. (Hrsg.), Freiheit – Sicherheit – Ordnung, Baden-Baden 2019. doi.org/10.5771/9783845215532.

Niemann, Fabian / Kevekordes, Johannes, Machine Learning und Datenschutz (Teil 1): Grundsätzliche datenschutzrechtliche Zulässigkeit, in Computer und Recht, Band 36, Heft 1, 2020, S. 17-24. https://doi.org/10.9785/cr-2020-360110.

Pohle, Jörg / Hölzel, Julian, Anonymisierung aus Sicht des Datenschutzes und des Datenschutzrechts, in Stellungnahme 29.06.2020 zum Konsultationsverfahren des BfDI zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Alexander von Humboldt Institut für Internet und Gesellschaft. Onlinequelle bei: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Stellungnahmen/Alexander-von-Humboldt-Institut.html. Abrufdatum: 21 November 2023.

Rüpke, Giselher / Lewinski, Kai / Eckhardt, Jens (Hrsg.): Datenschutzrecht: Grundlagen und europarechtliche Neugestaltung, 2. Auflage, München 2022. https://doi.org/10.17104/9783406759727.

Schaar, Peter, Datenschutz und Internet – Es ist kompliziert!, in Informatik Spektrum, Heft 43, 2020, S. 179–185. https://doi.org/10.1007/s00287-020-01275-2.

Schlingloff, Sebastian, Einführung in das Datenschutzrecht, in Juristische Ausbildung, Band 44, Heft 11, 2022, S. 1255-1264. https://doi.org/10.1515/jura-2022-3195.

Selzer, Annika / Timm, Ingo J., Potenziale anonymer Datenverarbeitungen nutzen, in Datenschutz und Datensicherheit, Ausgabe 12, 2021, S. 816–820.

Simitis, Spiros / Hornung, Gerrit / Spiecker genannt Döhmann, Indra (Hrsg.): Datenschutzrecht: DSGVO mit BDSG, Baden-Baden 2019.

Ulbricht, Carsten: Anonymisierung und Pseudonymisierung; Verschlüsselung; in Dorschel, Joachim (Hrsg.), Praxishandbuch Big Data: Wirtschaft – Recht – Technik, Wiesbaden 2015. https://doi.org/10.1007/978-3-658-07289-6.

Von dem Bussche, Axel F., Datenschutz 4.0; in Frenz, Walter (Hrsg.), Handbuch Industrie 4.0: Recht, Technik, Gesellschaft, Berlin 2020. https://doi.org/10.1007/978-3-662-58474-3.

Warren, Samuel D. / Brandeis, Louis D., The Right to Privacy, in Harvard Law Review, Vol. 4, No. 5, 1890, S. 193-220. https://www.jstor.org/stable/1321160.

Weichert, Thilo, Geodaten – datenschutzrechtliche Erfahrungen, Erwartungen und Empfehlungen, in Datenschutz und Datensicherheit, Ausgabe 6, 2009.

Wolff, Amadeus / Brink, Stefan / v. Ungern-Sternberg, Antje (Hrsg.): BeckOK Datenschutzrecht: DS-GVO, DGA, BDSG. Datenschutz und Datenordnung, 45. Edition, München 2023.

Zimmermann, Sören, Datenschutz und Demokratie: Überlegungen zu einem reziproken Bedingungszusammenhang, Band 60, Baden-Baden 2021. https://doi.org/10.5771/9783748923060.

# Eidesstattliche Erklärung &
# Einwilligungserklärung Nutzung von Plagiatssoftware

| | | | |
|---|---|---|---|
| Name: | Bleske | Studiengang: | WiSe 2023/24 MPA |
| Vorname: | Benjamin | Mtk.-Nr.: | 36104066 |
| Geb.-Ort: | Witten | Geb.-Datum: | 11.02.1997 |

Mir ist bekannt, dass bei meiner Arbeit eine Prüfung auf nicht kenntlich gemachte übernommene Textpassagen und sonstige Quellen stattfinden kann (vgl. u.a. § 16 Abs. 7 der Allgemeinen Bestimmungen für Fachprüfungsordnungen mit den Abschlüssen Bachelor und Master der Universität Kassel). Ich stimme zu, dass dafür gegebenenfalls ein Upload auf eine externe Datenbank des jeweiligen Software-Anbieters erfolgt und die Arbeit dafür auch gespeichert wird, sofern meine Arbeit dafür vorab ausreichend anonymisiert wird (i.d.R. genügt dafür die Entfernung des Deckblatts und der Unterschriftenseite). Ich stimme ebenfalls zu, dass zukünftig umgekehrt auch andere Arbeiten auf Plagiate aus meiner anonymisierten Arbeit überprüft werden.

Ich versichere hiermit, dass ich meine Hausarbeit, Die Anonymisierung von personenbezogenen Daten im Kontext von BIG DATA selbständig und ohne fremde Hilfe angefertigt habe. Alle von anderen Autoren wörtlich oder sinngemäß übernommenen Stellen sind entsprechend gekennzeichnet.

Mir ist bewusst, dass bei einem Verstoß gegen obige Erklärung nicht nur die betreffende Prüfungsleistung mit der Note – 5,0 – gewertet wird, sondern auch eine Exmatrikulation erfolgen kann.

Der Prüfungsausschuss entscheidet im Einzelfall.

| | |
|---|---|
| Bottrop, 25.11.2023 | Benjamin Bleske, Bleske |
| Ort, Datum | Unterschrift |