Anonymisierungsmöglichkeiten personenbezogener Daten vor dem Hintergrund der Datenschutzgrundverordnung

Marius Golombeck, Henning Orlowski

28. Mai 2018

University of Applied Sciences and Arts Dortmund
Emil-Figge-Straße 42, 44227 Dortmund, Germany
Department of Computer Science
{magol003, heorl001}@stud.fh-dortmund.de

Abstract. Die Bearbeitung personenbezogener Daten ist sowohl technisch als auch juristisch ein aktuelles Thema. So zeigten öffentlichkeitswirksame Vorfälle multinationaler Konzerne in jüngster Vergangenheit, welche Reputationsschäden ein fahrlässiger Umgang mit Daten auslösen kann. Durch die nun strengeren Anforderungen der Datenschutzgrundverordnung sowie deutlich höhere Strafen im Falle eines Verstoßes, wird die finanzielle Gefahr durch einen technisch-organisatorisch ungenügenden Umgang mit personenbezogenen Daten weiter konkretisiert. Möglichkeiten zur Anonymisierung von Daten wie Pseudonymisierung oder vollständige Anonymisierung sind vor dem Hintergrund der Datenschutzgrundverordnung eine rechtssichere Möglichkeit die sichere Weiterverarbeitung von Daten zu gewährleisten.

Keywords: Datenschutz, Datenschutzgrundverordnung, DSGVO, personenbezogene Daten, Datenverarbeitung

1 Einleitung

Einleitend werden in dieser Arbeit die Grundlagen personenbezogener Daten, ihre Bedeutung in der Datenverarbeitung und mögliche Anonymisierungskonzepte vorgestellt. Im Anschluss daran wird die Datenschutzgrundverordnung (DSGVO) vorgestellt und insbesondere hinsichtlich der Gesetzeslage zur Verarbeitung personenbezogener Daten analysiert. In Folge dessen werden Probleme, die durch Anonymisierungsverfahren personenbezogener Daten im Verlauf einer Datenverarbeitung entstehen, charakterisiert und in Szenarien eingeteilt. Im nächsten Schritt werden auf Basis dieser Informationen exemplarische Lösungsansätze vorgestellt sowie ihre jeweilige Tragbarkeit im Rahmen der derzeitigen Gesetzgebung diskutiert. Abschließend werden in einem Fazit die technischen, wie prozessualen Lösungen zur besseren Einhaltung der DSGVO diskutiert.

2 Grundlagen der Verarbeitung von personenbezogenen Daten

Um ein grundlegendes Begriffsverständnis zu erlangen ist es erforderlich die Begriffsdefinitionen des Europäischen Parlaments aus der Verordnung (EU) 2016/679 [...] zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) [...] [1] genauer zu betrachten.

In Artikel 4 werden insgesamt 26 verschiedene Begriffe definiert, ohne die es nach Auffassung der Gesetzgebers nicht möglich ist einen gesetzlichen Rahmen zur Verarbeitung personenbezogener Daten zu liefern[1].

Als **personenbezogene Daten** werden alle Informationen bezeichnet, die sich „auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen". Hierbei gilt eine Person als identifizierbar, wenn sie „direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann"[2].

Der Begriff der **Verarbeitung** beschreibt „jeden [...] Vorgang, [...] wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung"[3].

2.1 Abgrenzung Pseudonymisierung / Anonymisierung

Als **Pseudonymisierung** wird das „Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren"[4] beschrieben.

In Abgrenzung dazu wird der Prozess der **Anonymisierung** als „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können"[5] definiert.

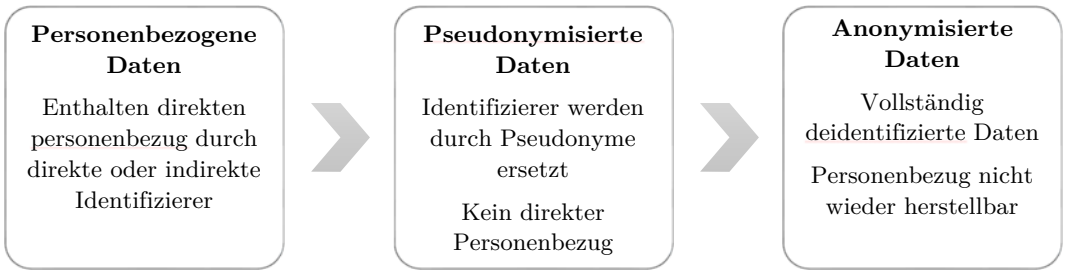


Abbildung 1 - Stufen der Datenverarbeitung nach Anonymisierungsgrad[6]

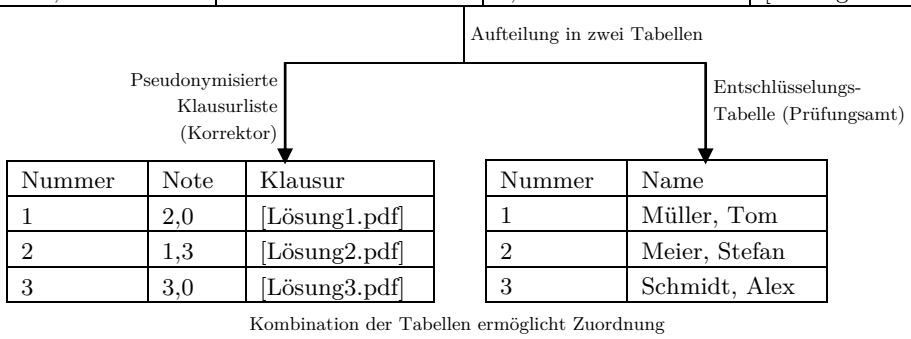
Abbildung 1 beschreibt die Stufen der Datenverarbeitung von personenbezogenen Daten hin zu vollständig anonymisierten Daten. Hierbei ist insbesondere die Entwicklung der Datenidentifizierer von Bedeutung. Werden bei pseudonymisierten Daten noch Pseudonyme verwendet, sind die Daten in der anonymisierten Version vollständig deidentifiziert.

[1] Vgl. [1] Art. 4, Ziff. 1
[2] Vgl. [1] Art. 4, Ziff. 1
[3] Vgl. [1] Art. 4, Ziff. 2
[4] Vgl. [2] §3, Ziff. 6a
[5] Vgl. [2] §3, Ziff. 6
[6] (eigene Darstellung)

2.1.1 Beispiel Pseudonymisierung

In der nachfolgenden Abbildung 2 wird beispielhaft die Pseudonymisierung von Daten beschrieben. Als Ausgangsbasis dient eine Tabelle, welche den Namen, die Matrikelnummer, die Note und einen Anhang als PDF-Datei enthält (hier: eine Klausurlösung).

Name	**Matrikelnummer**	**Note**	**Klausur**
Müller, Tom	7093821	2,0	[LösungMueller.pdf]
Meier, Stefan	7091284	1,3	[LösungMeier.pdf]
Schmidt, Alex	7095986	3,0	[LösungSchmidt.pdf]



Nummer	Note	Klausur
1	2,0	[Lösung1.pdf]
2	1,3	[Lösung2.pdf]
3	3,0	[Lösung3.pdf]

Nummer	Name
1	Müller, Tom
2	Meier, Stefan
3	Schmidt, Alex

Abbildung 2 - Prozess der Pseudonymisierung (Beispiel)[7]

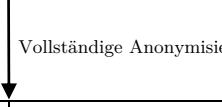
Im Schritt der Pseudonymisierung wird die Ausgangstabelle auf zwei Tabellen aufgeteilt. Die pseudonymisierte Klausurliste enthält einen neutralen Identifizierer (hier: fortlaufende Nummer), die Note und die Klausur als PDF-Datei, welche hinsichtlich der persönlichen Informationen des Prüflings bereinigt wurde.

Die Entschlüsselungstabelle hingegen enthält die Zuordnung von Identifizierer und dem persönlichen Informationsstamm (hier: vollständiger Name). Erst durch die Trennung von pseudonymisierten Daten und Entschlüsselungsmöglichkeit, wird eine Pseudonymisierung geschaffen.

2.2 Beispiel Anonymisierung

Bei der vollständigen Anonymisierung werden die Daten hingegen irreversibel anonymisiert. So werden zum Beispiel wie in Abbildung 3 ersichtlich, der Name, die Matrikelnummer und die Identifizierer aus der PDF-Datei anonymisiert.

Name	**Matrikelnummer**	**Note**	**Klausur**
Müller, Tom	7093821	2,0	[LösungMueller.pdf]
Meier, Stefan	7091284	1,3	[LösungMeier.pdf]
Schmidt, Alex	7095986	3,0	[LösungSchmidt.pdf]



Name	**Matrikelnummer**	**Note**	**Klausur**
a665a45920422f9	e26288bd82e1a976	2,0	[Lösung_a665.pdf]
5a45920422f9db8	a976b0e53bdd7e51	1,3	[Lösung_5a45.pdf]
0a1f3fff1fa07e998	7e584055805cc6309	3,0	[Lösung_0a1f.pdf]

[7] (eigene Darstellung)

Abbildung 3 - Prozess der Anonymisierung (Beispiel)[8]

Sofern ein sicheres Verschlüsselungsverfahren verwendet wurde, gilt eine Entschlüsselung der Identifizierer, oder der Daten sowie eine spätere Verknüpfung der entschlüsselten Daten und der entschlüsselten Identifizierer als schwierig im Sinne der Komplexitätstheorie[9] [3].

3 Datenschutzgrundverordnung

Die Datenschutzgrundverordnung (DSGVO) ist eine von der europäischen Kommission verabschiedete Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, welche am 25. Mai 2018, in Kraft getreten ist[10]. Als Verordnung ist sie auch ohne die direkte Umsetzung in nationales Recht geltend und ergänzt, bzw. ersetzt bereits bestehende nationale Datenschutzrichtlinien[11]. Betroffen sind alle Unternehmen und Einrichtungen, die personenbezogene Daten erheben, verarbeiten, nutzen und speichern[12]. Dabei müssen bei der Verarbeitung stets gewisse Grundsätze eingehalten werden, aus denen eine Vielzahl spezifischer Pflichten entstehen[13]. Die stark verkürzte, für die Zwecke der Ausarbeitung jedoch hinreichend genaue, Form dieser Grundsätze werden in Artikel 5 der Datenschutzgrundverordnung [1] wie folgt beschrieben:

a) Zur Sicherung der Rechtmäßigkeit der Datenverarbeitung müssen personenbezogene Daten auf eine für die betroffene Person **nachvollziehbare Weise** verarbeitet werden […][14].

b) Darüber hinaus dürfen Daten nur stets **zweckgebunden** verarbeitet werden, d.h. Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden […][15].

c) Es gilt stets der Grundsatz der **Datenminimierung**, nach der personenbezogene Daten nur dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein dürfen […][16].

d) Diese Daten müssen **sachlich richtig** sein und erforderlichenfalls auf dem **neuesten Stand** sein. Zu diesem Zwecke sind alle angemessenen Maßnahmen zu treffen, damit unrichtige Daten unverzüglich gelöscht oder berichtig werden […][17].

e) Personenbezogene Daten müssen in einer Form gespeichert werden, die die **Identifizierung der betroffenen Personen** nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist […][18].

f) Die Art und Weise der Verarbeitung muss eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich des **Schutz vor unbefugter oder unrechtmäßiger Verarbeitung** […][19].

---

[8] (eigene Darstellung)
[9] (nicht in polynomieller Zeit lösbar)
[10] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_de#berdieverordnungunddatenschutz
[11] https://www.it-recht-kanzlei.de/neue-datenschutzgrundverordnung-auswirkung-deutsches-datenschutzrecht.html?print=1
[12] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_de#berdieverordnungunddatenschutz
[13] https://www.it-recht-kanzlei.de/alte-grundsaetze-rechtmaessigkeitsvoraussetzungen-neue-datenschutzgrundverordnung.html?print=1
[14] Vgl. [1] Art. 5 Abs. 1a
[15] Vgl. [1] Art. 5 Abs. 1b
[16] Vgl. [1] Art. 5 Abs. 1c
[17] Vgl. [1] Art. 5 Abs. 1d
[18] Vgl. [1] Art. 5 Abs. 1e
[19] Vgl. [1] Art. 5 Abs. 1f

4 Probleme bei der Verarbeitung von personenbezogenen Daten

Das Grundproblem personenbezogener Daten in der Datenverarbeitung ist weniger ein technisches Problem, als ein finanzielles Problem, bzw. ein Praktikabilitätsproblem[20]. Dabei steht der gegenwärtige Trend des Machine Learning und der damit einhergehenden Notwendigkeit des Einsatzes von Big Data Methoden häufig im direkten Widerspruch zu dem Grundsatz der Datenvermeidung und des Anwendungsbezugs[21] [4].

Im Folgenden werden vier grundsätzliche Szenarien klassifiziert, deren Vorkommen im Zuge der Verarbeitung von personenbezogener Daten wahrscheinlich ist.

4.1 Klassifizierung von Problemszenarien

Bei jedem der folgenden Szenarien gilt es im Sinne der DSGVO nicht nur ihre grundsätzliche Zulässigkeit zu überprüfen. Durch die DSGVO entstehen auch funktionale Pflichten, denen ein Unternehmen ggf. gegenüber Kunden entsprechen muss[22].

Besonders zu Beachtenden sind unter anderem die Auskunftspflicht und die Möglichkeit der Löschung sämtlicher personenbezogener Daten[2324]. So muss für einen Kunden zu jeder Zeit die Möglichkeit bestehen, Auskunft über die, über ihn gesammelten, personenbezogenen Daten zu erhalten[25]. Auf Anfrage eines Kunden muss das Unternehmen darüber hinaus sämtliche personenbezogenen Kundendaten entfernen.[26] Dies schließt Druckerzeugnisse oder auch Daten die im Zuge einer Auftragsdatenverarbeitung an Dritte weitergeleitet wurden ein, was vor allem bei Konzernen mit komplexen Datenverarbeitungsprozessen zu kaum lösbaren Konflikten führen kann. Dies kann bestehende Geschäftsmodelle existenziell gefährden[27,28,29].

Als problematisch sind auch die neu eingeführten Rechenschaftspflichten anzusehen[30]. So muss ein Unternehmen in der Lage sein eigenständig nachzuweisen, dass sämtliche von der DSGVO erfassten Datenschutzprinzipien eingehalten werden[31]. Besonders in Unternehmen mit einer vornehmlich funktionalen Organisationsstruktur ist durch eine ggf. vorhandene Neigung zum Ressortegoismus nur schwer der gesamte Prozess der Datenverarbeitung eines einzelnen Kunden im Unternehmen rechtssicher auszuweisen [5][32,33].

---

[20] Vgl. https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD17-2604.pdf

[21] Vgl. [1] Art. 5 Abs. 1c

[22] Vgl. https://www.deutsche-handwerks-zeitung.de/eu-vorgaben-und-digitalisierung-datenschutz-im-umbruch/150/3098/355999

[23] Vgl. [1] Art. 17 Abs. 1

[24] Vgl. [1] Art. 15 Abs. 1

[25] Vgl. [1] Art. 15 Abs. 1

[26] Vgl. [1] Art. 17 Abs. 1

[27] Vgl. http://www.deutschlandfunk.de/eu-datenschutz-grundverordnung-aus-fuer-das-user-tracking.2907.de.html?dram:article_id=418139

[28] Vgl. [1] Art. 24 Abs. 1

[29] Vgl. http://www.sicherheit.info/artikel/2109571

[30] Vgl. [1] Art. 5 Abs. 2

[31] Vgl. https://www.audatis.de/aktuell/die-datenschutz-grundverordnung-und-ihre-dokumentationspflichten-teil-1-verzeichnis-der-verarbeitungstaetigkeiten/

[32] Vgl. [1] Art. 30

[33] Vgl. https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Verarbeitungsverzeichnis-online.pdf

4.1.1 Szenario 1: Allgemeine Verwendung, bereits gesammelte Daten

Szenario 1 (Allgemeine Verwendung, bereits gesammelte Daten): Ein Unternehmen erfasst durch ein bereits bestehendes Produkt Daten und möchte diese im Rahmen einer weiterführenden Analyse zunächst mit Verfahren der explorativen Analyse oder des Machine Learning auswerten, um daraus neue Produkte entwickeln zu können.

4.1.2 Szenario 2: Spezifische Verwendung, bereits gesammelte Daten

Szenario 2 (Spezifische Verwendung, bereits gesammelte Daten): Ein Unternehmen besitzt bereits Daten aus vergangenen Erhebungen, möchte diese nun aber spezifisch nutzen, um auch frühere Produkte im Sinne des Kunden weiterzuentwickeln. Insbesondere Statistiken zur Nutzung verschiedener Funktionen oder gesammelte Fehlerberichte, sollten in diesem Sinne verwendet werden, um die Nutzererfahrung zu verbessern.

4.1.3 Szenario 3: Allgemeine Verwendung, spezifisch gesammelte Daten

Szenario 3 (Allgemeine Verwendung, spezifisch gesammelte Daten): Ein Unternehmen erfasst von Kunden selbst eingegebene, bzw. mit ihrer ausdrücklichen Zustimmung erhobene, Daten zu einem zu diesem Zeitpunkt nicht näher definierten Zweck.

4.1.4 Szenario 4: Spezifische Verwendung, spezifisch gesammelte Daten

Szenario 4 (Spezifische Verwendung, spezifisch gesammelte Daten) Ein Unternehmen erhebt für einen spezifischen, definierten Verwendungszweck Daten von Kunden, die über diesen Zweck ausdrücklich informiert wurden und der Erhebung persönlichen Daten zugestimmt haben.

4.2 Lösungsansätze

Die Szenarien 1 und 2 sind insofern problematisch, als dass es zwar prinzipiell möglich ist auf Grundlage bereits bestehender Datenverarbeitungsvereinbarungen zu operieren, jedoch in der Praxis einige Bereiche nun strenger auslegt werden als in der Vergangenheit[34]. Das die bereits abgeschlossene Datenverarbeitungsvereinbarung den Nutzer ausreichend über seine Rechte informiert und die konkreten Zwecke, für die seine Daten verwendet werden, offenlegt, ist eher unwahrscheinlich[35]. Es ist in diesem Fall also notwendig die betreffenden Personen erneut um ihre Zustimmung zu einer neuen, mit den Grundwerten der DSGVO konformen, Datenverarbeitungsvereinbarung zu bitten.

Dieses Problem ist in den Szenarien 3 und 4 als weniger problematisch zu erachten, da hier die Vereinbarungen im Sinne der DSGVO unmittelbar angepasst werden können. Es werden nur Daten von Personen verwendet, die den Bedingungen auch tatsächlich vollumfänglich zugestimmt haben[36].

---

[34] Vgl. https://www.datenschutzbeauftragter-info.de/datenschutz-bei-marktforschung-was-aendert-die-dsgvo/

[35] Vgl. https://www.datenschutzbeauftragter-info.de/bleibt-eine-bereits-erteilte-einwilligung-auch-mit-der-dsgvo-gueltig/

[36] Vgl. https://www.pingdigital.de/blog/2017/04/05/dsgvo-fortgeltung-von-alteinwilligungen/1098

Unangetastet bleibt bisweilen die Möglichkeit der betroffenen Personen zu jedem Zeitpunkt ihre Einwilligung zur Datennutzung zurückzuziehen[37]. Es müssen hier also ebenso Maßnahmen getroffen werden, die eine lückenlose, vollumfänglich dokumentierte, Löschung der Daten gewährleisten[38].

Eine technische Möglichkeit um diese Funktionalität zu gewährleisten ist die strikte Nutzung einer zentralen Datenbasis, als Grundlage verschiedener Anwendungen. Dabei sollte zu jedem Zeitpunkt eine redundante Speicherung auf Projektebene unterbunden werden, sodass die Löschung des zentralen Datensatzes die redundante Löschung des Datensatzes in allen Bereichen nach sich zieht[39].

Alternativ, wenn auch ungleich komplexer, wäre eine zentrale Prozesslösung mit Zugang zu sämtlichen relevanten Datensätzen[40].

Da die rückwärtige Etablierung zentraler Datenstrukturen in bereits bestehenden, zentralen Datenstrukturen als sehr umständlich und technisch kompliziert anzusehen ist, könnte diese Lösung vor allem bei Unternehmen mit verteilter Datenbasis, wie z.B. in multinationalen Konzernen, der geeignetere Weg sein.

Für die meisten realtypischen Szenarien ist ein dualer Ansatz, bestehend aus einer zentralen Prozesslösung zur Löschung bereits bestehender Datensätze bei gleichzeitiger Nutzung einer zentralen Datenbasis für neue Datensätze, unserer Meinung nach die geeignetste Lösung.

5 Fazit

Die in Kapitel 2 vorgestellten Möglichkeiten zur Anonymisierung und Pseudonymisierung bieten eine hervorragende Möglichkeit, um personenbezogene Daten nach aktuellem Stand der Technik zu sichern. Klar ist dabei jedoch, dass es sich hierbei lediglich um einen kleinen Schritt in einem unternehmensübergreifenden Prozess der Datenvermeidung halten kann.

Unter anderem müssen zusätzliche Sicherungs- und Verschlüsselungsmaßnahmen ebenso, wie eine automatisierte, zeitlich gesteuerte, Löschung von Datensätzen gemäß des „Recht auf Vergessen“[41] umgesetzt werden. Dies stellt gerade für kleine bis mittelständische Unternehmen eine Hürde dar, die derzeit nur schwierig zu überwinden ist, da sie hochgradig spezialisierte Fachkräfte im technischen, als auch im juristischen Bereich, voraussetzt[42].

Eine Pseudonymisierung oder vollständige Anonymisierung ist aus reiner Datenschutzsicht als begrüßenswerte Maßnahme anzusehen. Im gleichen Zug wird jedoch häufig die gesetzliche Schwelle für solche Anonymisierungsverfahren zu hoch angelegt[43].

So gelten Daten, wie in 2.1 und 2.2 beschrieben, erst dann als anonymisiert, wenn eine Re-Identifikation schwierig [3] ist[44]. Besonders im Hinblick auf den derzeitigen Trend des Machine Learning und der immer besseren Nutzbarkeit von Big Data, werden die Re-Identifikationschancen vermeintlich anonymer Daten erhöht [6][45].

---

[37] Vgl. [1] Artikel 7 Absatz 3

[38] Vgl. https://efarbeitsrecht.net/datenschutzgrundverordnung-und-loeschpflichten/

[39] Vgl. https://blog.ec4u.com/sicherheit-datenbanken-dsgvo-datenschutz/

[40] Vgl. https://www.ppi.de/fileadmin/user_upload/Consulting_Banken/Publikationen/Flyer_Data_Clearing_Process.pdf

[41] Vgl. [1] Art. 17

[42] Vgl. https://www.wallstreet-online.de/nachricht/10135208-studie-dsgvo-haelfte-bereit

[43] Vgl. https://www.datenschutzbeauftragter-info.de/pseudonymisierung-was-ist-das-eigentlich/

[44] Vgl. https://www.noerr.com/de/newsroom/News/nutzung-von-patientendaten-ein-ausblick-auf-die-kommende-datenschutz-grundverordnung.aspx

[45] Vgl. https://motherboard.vice.com/de/article/qvvqqq/diese-kunstliche-intelligenz-lernt-gerade-vermummte-demonstranten-zu-identifizieren

Daten stellen das Kapital von Unternehmen des 21. Jahrhunderts dar. Es gilt jedoch zu beachten, dass die Datenverarbeitung unter gesetzlichen Auflagen erfolgen muss. Die Datenschutzgrundverordnung bildet einen ersten europäisch-einheitlichen Standard für den Schutz von personenbezogenen Daten. Jedoch gestaltet sich eine Überprüfung dieser umfänglichen Datenschutzrichtlinien als schwierig, was dazu führt, dass die Politik der Datenverwendung weiterhin undurchsichtig bleibt.

6 Literaturverzeichnis

[1] *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR): Verordnung (EU) 2016/679*, 2016.

[2] *Bundesdatenschutzgesetz: BDSG*, 2003.

[3] M. Golombeck, "Blockchain als Grundlage disruptiver Geschäftsmodelle," Hausarbeit, Fachhochschule Dortmund, Dortmund, 2018.

[4] P. Richter, "Big Data, Statistik und die Datenschutz-Grundverordnung," *Datenschutz und Datensicherheit - DuD*, vol. 40, no. 9, pp. 581–586, 2016.

[5] D. Vahs, *Organisation: Ein Lehr- und Managementbuch,* 9th ed. Stuttgart, Germany: Schäffer-Poeschel Verlag, 2015.

[6] C. Wirnsperger, "Automatic Identifcation of Persons by Using Keyboard Typing Metrics," Bachelor-Thesis, Institut für Informatik, Datenbanken und Informationssysteme, Universität Innsbruck, Innsbruck, 2018.