**Blockchain und Datenschutz – alles (k)ein Problem?**
Hashwerte von Personenbezogenen Daten

## 1. Einführung

Die Blockchain-Technologie ist vor allem durch die Verbreitung von Kryptowährungen wie dem Bitcoin bekannt geworden. Jedoch sind die Anwendungsbereiche für Blockchain-basierte Systeme äußerst vielfältig. Da die Blockchain im Kern ein dezentral verteiltes Datenregister ist, können auf ihr fast alle in Betracht kommenden Arten von Daten hinterlegt werden. So ist es in der Praxis immer wieder der Fall, dass personenbezogene Daten im Sinne der DSGVO Gegenstand des jeweiligen Use-Cases sind und demzufolge auf der Blockchain abgelegt werden sollen. Hierbei stellt sich immer die Frage, ob und mit welchen Folgen die DSGVO Anwendung findet.

Dabei besteht auf den ersten Blick ein wesentlicher Unterschied zwischen Blockchain-Technologie und Datenschutz: Während eine Blockchain die verwendeten Daten ohne Intermediär regelmäßig (öffentlich) einsehbar und irreversibel speichern möchte, statuiert die DSGVO verschiedene Betroffenenrechte wie vor allem das Recht auf Löschung und weitere Pflichten gegen einen (zentralen) Verantwortlichen. Daher wird in der Praxis im Regelfall versucht, dass der Anwendungsbereich der DSGVO dadurch umgangen wird, dass nicht die personenbezogenen Daten selbst, sondern deren Hashwerte on-chain gespeichert werden.

Die Annahme, dass durch die Verwendung von kryptografischen Hash-Funktionen der Anwendungsbereich der DSGVO ausgeschlossen ist, erweist sich aber unter gewissen Voraussetzungen als Trugschluss. So ist es möglich, dass auch Hashwerte von personenbezogenen Daten selbst personenbezogene Daten im Sinne der DSGVO darstellen. Korrekterweise werden Hashwerte im Rahmen der DSGVO als „Grauzone“ bezeichnet.[1] Im Folgenden soll daher herausgearbeitet werden, unter welchen Umständen auch Hashwerte Personenbezug aufweisen können. Im Anschluss sollen technische Verfahren präsentiert werden, welche eine solche Klassifizierung ausschließen können.[2]

Um diese Ausführungen zu veranschaulichen, soll dabei folgender Datensatz als Beispiel dienen:

| Vorname | Nachname | Geburtsdatum |
|---|---|---|
| Max | Mustermann | 02.11.1976 |

Ein Grundverständnis für die Funktionsweise der Blockchain-Technologie wird nachstehend vorgesetzt. Daher sollen – auch dem Schwerpunkt entsprechend – keine Ausführungen hierzu vorangestellt werden, sondern es wird vielmehr auf die entsprechende Literatur verwiesen.[3]

## 2. Kryptografische Hashwerte

Nicht speziell wegen der (vermeintlichen) Anonymität, sondern vielmehr zur Vermeidung eines rasanten Anstiegs der Datenmenge innerhalb einer Blockchain, werden keine großen Dateien on-chain gespeichert, sondern oftmals nur die Referenzen in Form von Hash-Werten der jeweiligen Datenmengen, welche selbst off-chain innerhalb einer externen Datenbank gespeichert werden.[4]

Hashwerte sind eindeutige Bit-Zeichenfolgen von bestimmter Länge, welche aus jeder digitalen Information durch die Verwendung spezieller (kryptografischer) Hash-Funktionen generiert werden können.[5] Das bedeutet, dass eine beliebig große Datenmenge in eine immer gleichgroße und ihr zuordenbare Bit-Zeichenfolge umgewandelt werden kann.

Kryptografische Hash-Funktionen sind demzufolge mathematische Funktionen, die eine beliebig lange Zeichenfolge (Input) in eine gleichlange Zeichenfolge (Output) umwandeln, wobei die Berechnung des Outputs aus dem Input mit wenig Aufwand möglich ist, während es umgekehrt keine praktikable Möglichkeit gibt, den urspr. Input aus dem Output zu berechnen (sog. Hiding).[6] Eine weitere Eigenschaft von kryptografischen Hash-Funktionen ist die Kollisionsresistenz, was bedeutet, dass derselbe Output für zwei verschiedene Inputs praktisch

[1] EU Blockchain Observatory and Forum, Blockchain and the GDPR, S. 21.
[2] Es sei darauf hingewiesen, dass dieser Beitrag kein Rechtsgutachten, sondern die persönliche Rechtsauffassung des Autors darstellt.
[3] Hierzu etwa *Narayanan et al.*, Bitcoin and Cryptocurrency Technologies; *Prinz/Schulte*, Blockchain und Smart Contracts; *Schlatt et al.*, Blockchain: Grundlagen, Anwendungen und Potenziale.
[4] Vgl. *Prinz/Schulte*, Blockchain und Smart Contracts. S. 16.
[5] *Schlatt et al.*, Blockchain: Grundlagen, Anwendungen und Potenziale, S. 31.
[6] *Narayanan et al.*, Bitcoin and Cryptocurrency Technologies, S. 2 ff.

nicht auffindbar ist (was nicht bedeutet, dass es diese Kollision nicht theoretisch gibt).[7] Die letzte wesentliche Eigenschaft von kryptografischen Hash-Funktionen ist, dass sie eine sog. *Puzzle friendliness* aufweisen, was bedeutet, dass es keinen effizienteren Weg zur Identifizierung des Inputs aus dem Output gibt als schlichtes Ausprobieren.[8] Im Hinblick auf die Ausgangsfrage bedeutet dass, dass man mittels Hashing eine Art digitaler Fingerabdruck eines Inputdatensatzes generiert werden kann, aus welchem sich der ursprüngliche Datensatz nicht einfach ermitteln lässt.[9] Da jeder Input einen faktisch einzigartigen Output generiert, kann der jeweilige Hash-Wert zur Prüfung der Datenintegrität genutzt werden.[10]

Kernpunkt für die besonderen datenschutzrechtlichen Fragen sind die vorangestellten Besonderheiten der Outputs von kryptografischen Hash-Funktionen. Es wird ein Output geschaffen, aus dem man den Ausgangsdatensatz jedoch nicht einfach herausfinden kann – außer durch reines Ausprobieren. Gleichzeitig kann nur der exakt gleiche Input den gleichen Hashwert als Output generieren, sodass für den Inhaber beider Werte eine Überprüfungsmöglichkeit der on-chain-Datenintegrität besteht. Letzteres kann auch in umgekehrte Richtung verwendet werden, sodass verifizierte und auf die Blockchain abgelegte Hashwerte als Referenz für die Korrektheit von Datensätzen wie etwa Zeugnissen genutzt werden können.[11]

Um diesen Vorgang zu illustrieren, soll der Hash-Wert des Beispielsdatensatzes gebildet werden. Hierfür wird die SHA-256 Funktion als gängige kryptografische Hash-Funktion genutzt. Der Input „MaxMustermann02.11.1976" ergibt demzufolge den Output „4c47d811647f76d33690ac3b69b826fe81cbaf6e7bb1999529ed90295b716273".[12] Ändert man nur ein Zeichen wie etwa das Geburtsjahr, also als Input „MaxMustermann02.11.1975", entsteht der völlig andere Hash-Wert „794c1db566efb665d0d21d460393f525b309575b19a8115967aab5bae7bc630b".

Das wesentliche Trugschluss ist – und dieser kommt in der Praxis durchaus häufiger vor – aber, dass oftmals angenommen wird, dass Hash-Werte aufgrund ihrer Eigenschaften selbst keinen Personenbezug aufweisen können und das auch dann, wenn ihr Input aus personenbezogenen Daten besteht. Auf dieser Grundlage wird geschlussfolgert, dass die on-chain Daten keine DSGVO-relevanten Daten abgelegt werden. Demzufolge werden auch keine Überlegungen angestrengt, wie man die jeweilige Blockchain-Applikation – etwa mit Zero-Knowledge-Proofs oder Chameleon-Hashes – derart datenschutzkonform ausgestalten muss, damit Betroffenenrechte geltend gemacht werden können.

### 3. Personenbezogene Daten nach der DSGVO

Neben der Verarbeitungshandlung [13] fordert die DSGVO für ihre Anwendbarkeit das Vorliegen personenbezogener Daten nach Art. 2 Abs. 1 DSGVO. Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO „*alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen*". Eindeutig ist, dass bei Hash-Werten von personenbezogenen Daten kein Bezug auf eine (direkt) identifizierte natürliche Person besteht.

Relevant für die Fragestellung dieser Arbeit ist aber, wann eine Identifizierbarkeit vorliegt. Art. 4 Nr. 1 DSGVO spricht im Bezug darauf davon, dass eine Person dann identifizierbar ist, 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*".

Vor dem Hintergrund dieser – durchaus sperrigen – Definition ist eine Person grundsätzlich also dann identifizierbar, wenn die Information mit weiteren Informationen (Referenzdaten) verknüpft werden kann und durch diese Verknüpfung ein Personenbezug entsteht.[14] Wesentlich ist also die Möglichkeit zur Bestimmbarkeit.[15]

---

[7] *Narayanan et al.*, Bitcoin and Cryptocurrency Technologies, S. 2 f.
[8] *Narayanan et al.*, Bitcoin and Cryptocurrency Technologies, S. 8.
[9] *Prinz/Schulte*, Blockchain und Smart Contracts. S. 16.
[10] *Prinz/Schulte*, Blockchain und Smart Contracts. S. 16.
[11] Etwa bwi Blockchain for Education, siehe *Gräther et al.*, Blockchain for Education: Lifelong Learning Passport, abrufbar unter: https://dl.eusset.eu/bitstream/20.500.12015/3163/1/blockchain2018_07.pdf (zuletzt aufgerufen am 31.7.2021).
[12] Der Hash-Wert wurde mithilfe von hashgenerator.de erzeugt.
[13] Da die Verarbeitung nicht der Schwerpunkt dieser Arbeit ist, soll sie nicht lehrbuchartig wiedergegeben werden, sondern vielmehr auf die Kommentarliteratur hierzu wie etwa *Schild*, in: BeckOK Datenschutzrecht, Art. 4 DSGVO, Rn. 29 ff.
[14] *Klar/Kühling*, in: Kühling/Buchner, DSGVO BDSG, Art. 4 Abs. 1 DSGVO, Rn. 19.
[15] *Ernst*, in: Paal/Pauly, DSGVO BDSG, Art. 4 DSGVO, Rn. 9.

Wann aber besteht diese Möglichkeit? Diese Frage ist untrennbar mit der Frage verknüpft, welche Mittel zur Identifizierbarkeit der Person zu berücksichtigen sind.

Der Erwägungsgrund 26 der DSGVO gibt hierfür eine erste Hilfestellung. Demnach sollen bei der Frage nach der Identifizierbarkeit einer Person 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. Wann bestimmte Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, soll von objektiven Faktoren, wie etwa den Kosten für die Identifizierung und den dafür notwendigen Zeitaufwand, herangezogen werden.[16] Dabei sind ebenfalls die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen.[17]

Der Erwägungsgrund 26 der DSGVO stellt folglich klar, dass eine reine Pseudonymisierung keine Wirkung auf den Personenbezug haben kann.

Erwähnenswert ist in diesem Zusammenhang auch Folgendes. Ein Datensatz kann nicht als anonym gelten, wenn weiterhin Kopien des Ausgangsdatensatzes mit Personenbezug bestehen bleiben, weil in diesem Fall der Inhaber weiter über die Mittel für die Herstellung eines Personenbezugs erfüllt.[18] Die Anonymität lässt sich aber dann durch Löschung dieser Ausgangsdatensätze tatsächlich dann herstellen, wenn eine Re-Identifikation ohne diese nicht mehr möglich ist, weil diese nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft erfolgen könnte.[19] Das gilt nicht für die Pseudonymisierung, denn hier ist es immer möglich, die betroffene Person – gegebenenfalls durch weitere Verarbeitungsmaßnahmen – wieder zu identifizieren.

In Bezug auf Hash-Werte von personenbezogenen Daten bedeutet das, dass sie zu einer Anonymisierung und nicht lediglich zu einer Pseudonymisierung führen müssten, um nach der Löschung des Ausgangsdatensatzes als Input Datensätze darzustellen, die nicht von der DSGVO umfasst sind.

**4. Risiken für Anonymisierungsverfahren**

Die juristischen Grundlagen vorangestellt, stellt sich die praktische Frage, wann im Falle von Hash-Werten lediglich eine Pseudonymisierung und gerade keine Anonymisierung vorliegt. Anknüpfungspunkt in der juristischen Literatur ist überraschend oft eine Arbeit der Art. 29 Datenschutzgruppe.[20] In der Stellungnahme zu Anonymisierungstechniken (WP 216) hat sich die Art. 29 Datenschutzgruppe u. a. Hash-Funktionen sowie schlüsselabhängige Hash-Funktionen (sog. Peppered Hashes) als Pseudonymisierungstechniken klassifiziert und zugleich 3 grundlegende Gefahren (Verknüpfung, Herausgreifen und Inferenz) benannt.[21] Im Folgenden sollen diese Gefahren zunächst vorgestellt werden.

1. Herausgreifen

   Es ist nach wie vor möglich, Datensätze einzelner Personen herauszugreifen, da die Person weiterhin anhand eines einzigartigen Merkmals identifiziert wird, das im Zuge der Pseudonymisierungsfunktion erzeugt wurde (das pseudonymisierte Merkmal).[22] Der Hashwert sperrt nämlich nur die Identifikation in eine Richtung, sodass die umgekehrte Richtung (das Auffinden eines Datensatzes zu einer bestimmten Person) weiterhin möglich ist.[23] In diesem Zusammenhang ist auch die Eigenschaft von kryptografischen Hashfunktionen zu betonen, wonach die Berechnung des Outputs aus dem Input einfach, d. h. ohne nennenswerten Rechenaufwand, möglich ist. Das bedeutet, dass vor allem Inputs mit einer geringen Entropie durch Erraten schlicht aufgefunden werden können. Lassen sich die infrage kommenden Inputs durch die Eigenart der Verwendung der Blockchain gar weiter einkreisen, ist demzufolge keineswegs von einer Unverhältnismäßigkeit auszugehen. Dies muss auch immer vor dem folgenden Hintergund gesehen werden: Um den Hashwert aller weltweit vorhandenen E-Mail-Adressen (ca. 5 Milliarden) zu bilden, würde es cirka 10 Millisekunden dauern und die hierfür notwendigen Kosten wurden 2018 auf unter 100

[16] *Schild*, in: BeckOK Datenschutzrecht, Art. 4 DSGVO, Rn. 15.
[17] *Schild*, in: BeckOK Datenschutzrecht, Art. 4 DSGVO, Rn. 15.
[18] *Klabunde*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 4 DSGVO, Rn. 20.
[19] *Schild*, in: BeckOK Datenschutzrecht, Art. 4 DSGVO, Rn. 15a.
[20] So etwa *Erbguth*, MMR 2019, 654 (657); European Parliament, Blockchain and the General Data Protection Regulation, S. 31.
[21] *Art. 29 Datenschutzgruppe*, WP216 – Stellungnahme 5/2014 zu Anonymisierungstechniken, S. 24 ff.
[22] *Art. 29 Datenschutzgruppe*, WP216 – Stellungnahme 5/2014 zu Anonymisierungstechniken, S. 25.
[23] *Erbguth*, MMR 2019, 654 (657).

US-Dollar geschätzt.[24] Vor allem für das Auffinden des ursprünglichen Inputs von Hashwerten können sog. Rainbow-Tables verwendet werden.[25] Diese kann man sich als eine Art Tabelle mit Datensätzen und ihren korrespondierenden Hashwerten vorstellen.[26]

2. Verknüpfbarkeit

Datensätze, in denen für eine bestimmte Person dasselbe pseudonymisierte Merkmal verwendet wird, können ganz einfach verknüpft werden. Selbst wenn für ein und dieselbe betroffene Person unterschiedliche pseudonymisierte Merkmale verwendet werden, kann eine Verknüpfung mittels anderer Merkmale unter Umständen nach wie vor möglich sein.[27] Diese Gefahr besteht vor allem, wenn – wie im Beispiel der Art. 29 Datenschutzgruppe – Hashwerte zusammen mit Klardaten abgelegt werden.[28] Kommt der Hashwert also an mehreren Stellen vor, können Verknüpfungen zwischen diesen Stellen hergestellt werden.[29]

3. Inferenz

Angriffe mittels Inferenztechniken zwecks Ermittlung der wahren Identität einer betroffenen Person sind innerhalb eines Datenbestands sowie über mehrere unterschiedliche Datenbanken, die für eine Person dasselbe pseudonymisierte Merkmal verwenden, hinweg möglich.[30] Diese Gefahr ist letztlich eng mit der Verknüpfbarkeit verbunden. Im Unterschied dazu werden nicht (nur) die Stellen der Hashwerte, sondern weitere mit ihnen abgelegte Klardaten zur Identifizierung genutzt werden. So ist es mit Hilfe dieser Klardaten etwa möglich, dass durch einen Abgleich mit externen Daten ein Personenbezug hergestellt werden kann.[31]

**5. Lösungsmöglichkeiten**

Vorweg muss gesagt werden, dass es in der juristischen Literatur keinen Konsens oder gar eine Art best practice gibt, wann ein Hashwert derart „sicher" ist, dass durch ihn eine Anonymisierung des personenbezogenen Inputs erfolgt.

Vor dem Hintergrund der aufgeführten Erläuterungen und Anforderungen der DSGVO lassen sich jedoch zwei grundlegende Voraussetzungen erschließen:

Es muss eine möglichst hohe Entropie des Ausgangsdatensatzes der Hashwert-Funktion, also des Inputs, gewährleistet werden.[32] In diesem Zusammenhang beschreibt der Begriff Entropie der Informationsgehalt des Inputs. Je niedriger dieser ist, desto anfälliger ist der daraus gebildete Hashwert für Brute-Force-Angriffe oder Rainbow-Tables. Eine nicht nur hinreichend hohe, sondern auch komplexe Entropie kann u. U. hierbei durch die Anwendung von sog. Salted-Hashes oder Peppered-Hashes erreicht werden.[33] In beiden Fällen wird dem personenbezogenen Datum ein weiterer Wert, „Salz" oder „Pfeffer", hinzugegeben, um die Entropie des Ausgangsdatensatzes möglichst komplex zu erhöhen. Der Unterschied liegt einzig in dem Umstand, dass bei einem Peppered-Hash dieser Zusatzwert („Pfeffer") nicht nur lediglich off-chain gespeichert, sondern geheim gehalten oder gar überhaupt nicht gespeichert wird.[34] Diese zwei Eingabewerte können durch weitere, jeweils einzigartige Daten weiter angereichert werden. Bei Transaktionen kann so z. B. die Uhrzeit der jeweiligen Transaktion Teil des Inputs sein. Dadurch wird erreicht, dass jeder Hash-Wert an sich einzigartig und dadurch eine Verknüpfbarkeit

[24] *Acar*, Four cents to deanonymize: Companies reverse hashed email addresses, abrufbar unter https://freedom-to-tinker.com/2018/04/09/four-cents-to-deanonymize-companies-reverse-hashed-email-addresses/ (Zuletzt aufgerufen am 14.7.2021).
[25] *Art. 29 Datenschutzgruppe*, WP216 – Stellungnahme 5/2014 zu Anonymisierungstechniken, S. 24.
[26] *Tetelbaum*, Hashed Passworts, Rainbow Tables, and Salted Hashes Simply Explained, abrufbar unter: https://medium.com/geekculture/hashed-passwords-rainbow-tables-and-salted-hashes-simply-explained-1736d431af78 (zuletzt aufgerufen am 14.7.2021).
[27] *Art. 29 Datenschutzgruppe*, WP216 – Stellungnahme 5/2014 zu Anonymisierungstechniken, S. 25 f.
[28] Siehe *Art. 29 Datenschutzgruppe*, WP216 – Stellungnahme 5/2014 zu Anonymisierungstechniken, S. 27.
[29] Vgl. *Erbguth*, MMR 2019, 654 (657).
[30] *Art. 29 Datenschutzgruppe*, WP216 – Stellungnahme 5/2014 zu Anonymisierungstechniken, S. 26.
[31] *Erbguth*, MMR 2019, 654 (657).
[32] Ebenfalls *Erbguth*, MMR 2019, 654 (655); European Parliament, Blockchain and the General Data Protection Regulation, S. 30.
[33] So ebenfalls EU Blockchain Observatory and Forum, Blockchain and the GDPR, S. 22.
[34] EU Blockchain Observatory and Forum, Blockchain and the GDPR, S. 22.

umgangen wird.[35] Salted-Hashes haben des Weiteren den Vorteil, dass man das „Salt“ zwar grds. off-chain speichert, bei Geltendmachung von Betroffenenrechten wie etwa dem Löschungsanspruch aus Art. 17 DSGVO diesen Wert aber sicher löschen kann. Dadurch wird die eigene Möglichkeit vernichtet, dass aus dem jeweiligen Ausgangsdatensatz und dem dazugehörigen Salt auf den Hashwert geschlossen werden kann und damit eine Identifizierbarkeit u. U. nicht mehr mit verhältnismäßigem Aufwand möglich ist. Denn nur die Kenntnis des Salts kann etwa das Erraten der eigentlichen Information ermöglichen (vorausgesetzt, dass das Salt komplex genug ist).[36]

Ein weiterer grundlegender Punkt betrifft das jeweilige Blockchain-Design, vor allem die Auswahl und Art der on-chain gespeicherten Daten. Werden Hash-Werte mit anderen Klardaten gekoppelt auf der verwendeten Blockchain angelegt, wird die Gefahr der Inferenz deutlich erhöht.

Dennoch können auch bei Erfüllung dieser Punkte Gefahren hinsichtlich einer (verhältnismäßigen) Identifizierbarkeit bestehen. So weist die Art. 29 Datenschutzgruppe in Bezug auf Salted Hashes darauf hin, dass auch bei ihnen unter Umständen möglich ist, dass der durch den Salted Hash verborgene Ursprungswert errechnet werden kann.[37] Die Gefahr etwa der Verlinkung kann auch bei sich (nach Plan) ändernden Hash-Werten bestehen, wenn dabei gewisse Muster erkennbar sind.[38] Auch die Verwendung desselben Attributes für die Hashwertbildung innerhalb verschiedener Datenbanken kann das Risiko der Verknüpfung erhöhen – es ist daher wichtig, dass eine Einzelperson in unterschiedlichen Kontexten verschiedenen pseudonymisierten Merkmalen entspricht.[39]

**6. Zusammenfassung**

Die feste Überzeugung, dass es sich mit der on-chain Verwendung von Hashwerten von personenbezogenen Daten mit der Anwendbarkeit der DSGVO erledigt hat, kann sich teuer rächen. Ohne die Beachtung der vielseitigen Identifizierungsrisiken ist gar davon auszugehen, dass Hashwerte regelmäßig zu einer Pseudonymisierung führen.

Aus der juristischen Literatur hierzu ist nur zu entnehmen, dass Einigkeit darüber besteht, dass hier eine Art „rechtliche Grauzone“ existiert. Klare Grenzen zwischen Anwendbarkeit und Nichtanwendbarkeit der DSGVO sind nicht vorhanden. Dennoch wurde in diesem Beitrag der Versuch gewagt, dass einerseits die Risiken und andererseits grundlegende Aspekte für die Erhöhung der Sicherheit aufgezeigt werden.

Dennoch, es bleibt dabei: Es ist eine komplexe Frage des Einzelfalls, ob Hashwerte von personenbezogenen Daten selbst personenbezogene Daten im Sinne der DSGVO sind. Umso wichtiger ist es, sich einerseits der Risiken und zumindest grundlegenden Sicherheitsmaßnahmen bewusst zu sein und sich andererseits mit Blockchain-Experten zu diesem Thema aktiv auszutauschen.

[35] EU Blockchain Observatory and Forum, Blockchain and the GDPR, S. 22.
[36] *Erbguth*, MMR 2019, 654 (655).
[37] *Art. 29 Datenschutzgruppe*, WP216 – Stellungnahme 5/2014 zu Anonymisierungstechniken, S. 24 f.
[38] *Art. 29 Datenschutzgruppe*, WP216 – Stellungnahme 5/2014 zu Anonymisierungstechniken, S. 24 f.
[39] *Art. 29 Datenschutzgruppe*, WP216 – Stellungnahme 5/2014 zu Anonymisierungstechniken, S. 26.