www.jusletter-it.eu

Barbara Anita Möri

Blockchain und Datenschutz

Technische Möglichkeiten und rechtliche Herausforderungen anhand eines Use Cases

Blockchain and data protection are in a tense relationship due to the technology of immanent invariability. Contrary to the prevalent opinion that these two institutes are not compatible with each other, the author concludes that it's possible to find a technical solution to bring the technology in line with data protection and to use it accordingly. (kg)

Category: Articles
Region: Switzerland
Field of law: Data Protection; Blockchain

Citation: Barbara Anita Möri, Blockchain und Datenschutz, in: Jusletter IT 23 May 2019

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

EDITIONS WEBLAW

Inhaltsverzeichnis

I. Einleitung

[Rz 1] Viele Autoren haben sich bereits mit der Thematik Blockchain[1] befasst, meist mit dem Augenmerk auf Anwendungen im Finanzsektor. Gegenstand dieses Beitrages ist das Spannungsfeld zwischen der Blockchain-Technologie und den Anforderungen des Datenschutzes, dargestellt an einem konkreten Fallbeispiel, das nicht im Finanzbereich angesiedelt ist.

[Rz 2] Vorliegend soll gezeigt werden, wie sich die fachlichen Qualifikationen unter Verwendung einer Blockchain-basierten Lösung nachweisen lassen. Ob dies die beste technische Umsetzung darstellt, wird nachfolgend nicht bewertet. Vorab ist ebenfalls zu erwähnen, dass über die gängigen Denkweisen hinausgegangen werden soll. Namentlich wird versucht, die rechtlichen Aspekte auch etwas aus einer technischeren Sichtweise zu beleuchten sowie neue bzw. andere Wege aufzuzeigen, wie die Problemstellungen gerade im Zusammenhang mit dem Datenschutz betrachtet werden könnten.

II. Use Case Zertifizierungsnachweise

[Rz 3] In gewissen Bereichen, namentlich in sicherheitssensitiven Arbeitsumgebungen, müssen Mitarbeiter über entsprechende Ausbildungen, Zeugnisse und Zertifizierungen verfügen, die sie vorweisen und auf deren Gültigkeit überprüfen lassen müssen. Gerade auf gesicherten Baustellen, welche spezielle Zertifizierungen erfordern, gestaltet sich heute die Überprüfung sowie die

[1] Siehe zur Begrifflichkeit unter https://www.heise.de/tipps-tricks/Was-ist-eine-Blockchain-3860869.html (Abruf 6. Februar 2019).

Dokumentation bei der üblichen Durchmischung von internen und externen Mitarbeitern aufwändig. Periodisch zu erneuernde Zertifizierungen verursachen dabei zusätzlichen Aufwand im bereits aufwändigen Umgang mit den meist in Papierform bestehenden Legitimationen.

[Rz 4] Unnötige Prozesse entstehen jedoch nicht nur bei der Zulassung zu einem gesicherten Bereich, sondern auch beim vorgelagerten und allenfalls periodischen (Neu-) Erwerb sowie bei der Verwaltung der Zertifikate, Ausbildungen und medizinischen Untersuchungen. Ebenso sind auch diejenigen Aufwände nicht zu vernachlässigen, die im Zusammenhang mit Nachweispflichten entstehen.

[Rz 5] Folgende Lösung wird für die Vereinfachung der genannten Prozesse in casu näher diskutiert und beleuchtet: Mit Hilfe einer Applikation soll ein Mitarbeiter seine Zulassung basierend auf entsprechenden Zertifikaten direkt beim Zutritt zum gesicherten Bereich belegen können. Hierzu ist eine Kommunikation zwischen seinem Gerät und dem Gerät der Kontrollperson erforderlich, welche beispielsweise mittels QR Code initiiert und über die Internetverbindung der Geräte abgewickelt wird. Der von der Anwendung der Kontrollperson generierte Code erfragt dabei die notwendigen Informationen für den Eintritt und gibt gleichzeitig an, wohin die Informationen geliefert werden sollen. Nach dem Scannen des Codes durch den Mitarbeiter mittels Smartphone-App wird auf der Applikation des Mitarbeiters ersichtlich, welche Informationen konkret verlangt werden und wer die Informationen wünscht. Er hat sodann die Möglichkeit, den Zugriff auf die angeforderten Informationen freizugeben oder zu verweigern. Die Bestätigung löst den Datenfluss in Richtung einer Datenbank (Logbuch) aus, in der sämtliche relevante Ereignisse zur späteren Nachvollziehbarkeit gespeichert werden.

[Rz 6] Grundsätzlich handelt es sich bei der beispielhaft in einem Proof of Concept umgesetzten Lösung um eine Kombination von Self Sovereign Identity (nachfolgend SSI) bzw. Distributed Identity (DID und Distributed Claims). Was bedeutet dies konkret? Vereinfacht dargestellt ist dieser Prozess mit der Betrachtung der eigenen Brieftasche und der Verwendung deren Inhaltes gleichzusetzen – nur ist in diesem Falle alles digital und basierend auf Smartphone, Kryptografie und Distributed Ledger.[2]

[Rz 7] An erster Stelle steht eine digitale Identität für alle Beteiligten (Mitarbeiter, Zertifizierer, Prüfer usw.) in Form eines Public/Private Key Paares[3], das erstellt wird, sobald einer der Beteiligten am System teilnehmen will. Die Public Keys werden bei diesem Lösungsansatz unveränderlich auf einem Distributed Ledger (z.B. Ethereum Blockchain) abgelegt. Das Public/Private Schlüsselpaar, welches gleichzeitig die Grundlage der digitalen Brieftasche (Wallet) auf dem Smartphone darstellt, muss als nächstes mit einer realen Person verknüpft werden. Dies sollte analog der heutigen Passstellen, durch eine staatlich autorisierte Instanz erfolgen. Jedoch wäre auch eine andere Stelle denkbar, sofern sie das entsprechende Vertrauen innehat. Die Passstelle, welche ebenfalls über entsprechende Private/Public Keys verfügt, verifiziert die Identität anhand von biometrischen Merkmalen und dem Einwohnerregister und bestätigt die Identität

2 Zur Veranschaulichung hierzu noch ein Beispiel: Für den Zutritt wird man nach dem Ausweis gefragt. Nun hat man die Option diesen vorzuzeigen oder nicht. Im zweiten Fall muss jedoch mit der Verweigerung des Einlasses gerechnet werden.

3 Bei dem asymmetrischen Verschlüsselungsverfahren hat jeder Nutzer ein eigenes Schlüsselpaar, von welchem je ein Schlüssel geheim (sog. Private Key) und einer öffentlich ist, bzw. bekannt gegeben werden muss (sog. Public Key). Der Private Key ermöglicht es, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren. Aufgrund dessen ist er somit auch unter allen Umständen geheim zu halten; vgl. sic! 2018 S. 439; siehe hierzu weiterführend: https://www.mycryptopedia.com/public-key-private-key-explained/ (Abruf 6. Februar 2019).

durch Signatur der Eigenschaften mittels Private Key. Die so signierte Identität wird im Wallet der identifizierbaren Person gespeichert. Ausbildungsbestätigungen, Tests und Zertifizierungen wiederum würden von den entsprechenden Ausbildungsstellen, Veranstaltern und medizinischen Zentren/Ärzten durch ihre eigenen Signaturen bestätigt und auch im Wallet des Mitarbeiters gespeichert. Weil nicht eine zentrale Stelle die Zertifizierungen bestätigt, spricht man hier vom «Distributed Claims» Verfahren. Mit der gleichzeitig fehlenden zentralen Stelle ist nun der Mitarbeiter auch selbst für die Speicherung der signierten Identität und der Bestätigungen auf seinem Gerät verantwortlich (SSI), wie das auch mit der Brieftasche der Fall ist, die bspw. Zahlkarten, Identitätskarte oder Führerausweis enthält.

[Rz 8] Eine Überprüfung läuft technisch wie folgt ab: Der Überprüfende verlangt vom Überprüften die Bestätigung bestimmter «Claims» (Anspruch, Behauptung), wie beispielsweise, dass eine Zertifizierung absolviert wurde. Falls der Überprüfte einwilligt, dem Prüfenden die angeforderten Informationsansprüche zu bestätigen, übermittelt er die entsprechenden Informationen, welche durch die Zertifizierungsstelle signiert wurden. Der Prüfende kann mit Hilfe des im Distributed Ledger gespeicherten Public Keys der Zertifizierungsstelle prüfen, ob der übermittelte Claim gültig ist. Dieses Verfahren entspricht dem «analogen» bei dem ein Autofahrer einem Polizisten auf Verlangen den eigenen Führerausweis aushändigt, welcher durch die autorisierte Stelle (Strassenverkehrsamt) ausgestellt wurde und sich (normalerweise) in der Brieftasche des Autofahrers befindet. Der Polizist ist in der Lage, an Ort und Stelle die Behauptung «Führerprüfung bestanden» des Autofahrers zu prüfen, in dem einerseits der Ausweis selbst geprüft wird (= prüfen der Signatur) und andererseits der Eintrag «Führen von Personenfahrzeugen» (= Claim) eingesehen werden kann, ohne die autorisierte Stelle anrufen zu müssen.

[Rz 9] Die Prüfung der Signatur erfolgt mit einem kryptografischen Verfahren mit Hilfe des zur jeweiligen Zertifizierungsstelle gehörendem Public Keys. Der Überprüfer muss/kann jederzeit entscheiden, welche Zertifikatsaussteller akzeptiert werden. Zu diesem Zweck können Zertifizierungen, welche durch andere als den vom Überprüfer akzeptierten Stellen signiert wurden, abgelehnt werden.

[Rz 10] Da in sicherheitsrelevanten Bereichen, in welchen nur Spezialisten oder bestimmte Personen Zugang erhalten dürfen, der Verantwortliche jederzeit die Einhaltung der Vorschriften nachweisen können muss, besteht die Möglichkeit aus den Protokollen periodisch einen Hash[4] zu generieren (Hash = Prüfwert, mit welchem Veränderungen am Originalinhalt festgestellt werden können). Dieser Hash kann sodann auf einer Blockchain unveränderbar hinterlegt werden. Damit wird ein Nachweis bezüglich der Einhaltung der Sicherheitsvorschriften basierend auf den Protokollen des Verantwortlichen möglich, da durch die Verifikation gegen den in der Blockchain abgelegten Prüfwert sichergestellt wird, dass nachträgliche Manipulationen des Protokolls entdeckt werden können.

4 Ein Hash ist ein Wert der durch eine Hashfunktion oder in unserem Fall durch eine (kollisionsresistente) Einwegfunktion zu Stande kommt. Die Verwendung als Prüfwert ist nur eine von vielen möglichen Funktionen. Siehe hierzu im Detail: https://blockchainwelt.de/hash-hashpower-und-hashfunktion/ (Abruf 6. Februar 2019).

III. Rechtliche Aspekte

A. Datenschutz

1. Einleitende Bemerkungen

[Rz 11] Datenschutz ist nunmehr ein allgegenwärtiges Thema. Vom erstmaligen Auftauchen von Regelungen zwischen 460 und 360 v.Chr. bis hin zur ersten Kodifizierung 1970 hat er sich von Vorschriften betreffend ärztlicher Schweigepflicht hin zu einer allgegenwärtigen Normierung entwickelt. Er dient dem Kontrollbedürfnis über die eigenen Daten, über die Informationen hinsichtlich seiner eigenen Person. Eine Verletzung dieses Bedürfnisses hat nicht nur die Verletzung gegen die Prämisse des Datenschutzes an sich zur Folge, sondern stellt jeweils auch eine Verletzung der freien Persönlichkeitsentwicklung dar. Ursprünglich wurden die Vorgaben zum Schutz der Personendaten auf der Prämisse festgelegt, dass etwaige Verletzungen unmittelbar festgestellt und die verantwortlichen Personen auch ohne weitere Mühen zur Rechenschaft gezogen werden können. Dieses Konzept wurde jedoch durch die Globalisierung, des hohen und auch automatisierten Informationsaustausches schlicht vom technischen Fortschritt überholt.[5]Die Fortentwicklung der Kodifizierungen wurde nötig und in diesem Zuge fanden offenere Formulierungen Eingang in die Gesetzgebung, um die Entwicklungen und Neuerungen zu berücksichtigen. In jüngster Zeit bildeten jedoch gerade diese offenen Formulierungen dem technischen Fortschritt und den damit einhergehenden Möglichkeiten einige Probleme.

[Rz 12] Im Folgenden werden die für den Use Case und die Einordnung der technischen Aspekte relevanten Normen des Schweizerischen Datenschutzes und der DSGVO kurz beleuchtet.

2. Datenschutz nach DSG

[Rz 13] Das Datenschutzgesetz kommt gemäss Art. 2 DSG immer dann zum Tragen, wenn Daten von natürlichen und juristischen Personen bearbeitet werden. Dabei sind die dem Datenschutz inhärenten Grundsätze, welche in Art. 4 DSG verankert wurden, zu beachten. Diese sind namentlich das Verhältnismässigkeitsprinzip, das Prinzip von Treu und Glauben, die Rechtmässigkeit und Erkennbarkeit der Bearbeitung, die Zweckbestimmung sowie die Richtigkeit der Daten.[6]

[Rz 14] Nach Art. 3 lit. a DSG sind Personendaten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.[7] Die Begrifflichkeit ist sehr weit gefasst, da lediglich ein Informationsgehalt vorliegen muss, der sich auf eine Person bezieht (direkt)[8]oder beziehen lässt (indirekt)[9]. Angaben stellen jedoch erst Personendaten dar, wenn dadurch unmittelbar oder aus dem Kontext der Information bzw. durch Kombination mit anderen Daten, die Identität der Per-

5 Vgl. Sandra Husi-Stämpfli, Stämpflis Handkommentar SHK, Datenschutzgesetz (DSG), 1. A., Bern 2015 (zit. SHK-Verfasser), Ziff. I, N. 1 ff.; vgl. auch Cornelia Stengel, Roman Aus der Au, Blockchain: Eine Technologie für effektiven Datenschutz? sic! 2018, S. 439 ff.

6 Siehe hierzu im Einzelnen: SHK-Baeriswyl, Art. 4 N. 1 ff.

7 Art. 3 lit. a DSG.

8 Bspw. Eintragung in das Personaldossier, in eine Mitgliederliste eines Vereins, Ranglisten bei Wettkämpfen oder auch GPS Daten eine Person betreffend etc.

9 Bspw. Schätzung einer Immobilie, die einer gewissen Person gehört.

son bestimmt werden kann. Der Bezug ist dabei nur solange gegeben, wie die Identifizierung ohne unverhältnismässigen[10] Aufwand möglich ist.[11]

[Rz 15] Die Bestimmbarkeit besteht, solange Personendaten nicht anonymisiert[12] werden. Sobald eine Reversibilität gegeben ist, handelt es sich um eine Pseudonymisierung. Die pseudonymisierten Daten bleiben für jene, die Zugang zum Schlüssel haben, weiterhin Personendaten. Für Aussenstehende jedoch, die weder einen Schlüssel besitzen noch Zugang zu ebendiesem haben, sind es analog der anonymisierten Daten keine Personendaten mehr.[13]

[Rz 16] Eine Verletzung der eingangs erwähnten Grundsätze nach Art. 4 DSG stellt eine Verletzung der Persönlichkeit der betroffenen Person dar. Die Rechtswidrigkeit entfällt jedoch bei Vorliegen eines Rechtfertigungsgrundes nach Art. 13 DSG, d.h. durch die Einwilligung des Verletzten, ein überwiegendes privates oder öffentliches Interesse oder eine Gesetzesvorschrift.

3. Datenschutz nach DSGVO

[Rz 17] Die Legaldefinition der personenbezogenen Daten in Art. 4 DSGVO entspricht – mit Ausnahme, dass die Bestimmbarkeit hier nun ausdrücklich definiert ist – jener des DSG. Gleiches gilt für die Verarbeitung und Pseudonymisierung der Daten und es kann an dieser Stelle auf die obigen Ausführungen verwiesen werden.

[Rz 18] Es sind nach Art. 5 lit. d DSGVO alle angemessenen Massnahmen zu treffen, damit Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.[14] Dieser Anspruch an die Richtigkeit wurde denn auch in den Art. 16 und 17 DSGVO kodifiziert, wonach die Betroffenen einerseits ein Recht auf Berichtigung und andererseits auf Löschung ihrer Daten haben. Jedoch ist dabei der Erwägungsgrund 65 zu beachten, wonach diese Rechte nur bestehen, wenn die Speicherung der Daten der DSGVO oder einem anderen Recht der Mitgliedstaaten nicht entgegenläuft. Ist etwa die Speicherung von fehlerhaften Daten gesetzlich vorgeschrieben, so besteht kein Anspruch nach Art. 16 DSGVO.[15]

[Rz 19] Die Speicherung hat in einer Form zu erfolgen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Art. 5 lit. e DSGVO); personenbezogene Daten dürfen länger gespeichert werden, soweit sie ausschliesslich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäss Artikel 89 Absatz 1 verarbeitet werden.

[Rz 20] Anders als unter dem DSG verlangt die DSGVO für jede Datenbearbeitung eine Rechtsgrundlage ähnlich der Rechtfertigungsgründe von Art. 13 DSG. Die Verarbeitung ist gemäss

---

10 Unverhältnismässigkeit liegt vor, wenn nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird. Dabei sind die technischen Möglichkeiten und die wirtschaftliche Sinnhaftigkeit aus Sicht des Interessenten (Aufwand/Ertrag) zu berücksichtigen.

11 SHK-Rudin, Art. 3 N. 10 f.

12 Anonymisierung ist gegeben, wenn der Personenbezug irreversibel aufgehoben wird und ohne unverhältnismässigen Aufwand keine Rückschlüsse auf Personen möglich sind. Dabei darf jedoch auch kein Schlüssel bestehen, der die Anonymisierung rückgängig machen kann.

13 SHK-Rudin, Art. 3 N. 13 ff.

14 Art. 5 Abs. 1 lit. d Verordnung (EU) 2016/679 des Europäischen Parlaments und Rates vom 27. April 2016 (DSGVO).

15 Jörn Erbguth, Datenschutz auf öffentlichen Blockchains, erbguth.ch, Ziff. 3.1.

Art. 6 DSGVO nur rechtmässig, wenn die betroffene Person ihre Einwilligung gibt oder sie für die Erfüllung eines Vertrags oder einer rechtlichen Verpflichtung erforderlich ist. Ebenfalls ist eine Rechtmässigkeit gegeben, wenn die Verarbeitung notwendig ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen. Darüber hinaus auch, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Schliesslich ist die Verarbeitung zulässig, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.[16]

4. Self-Sovereign-Identity

a. Einleitende Bemerkungen

[Rz 21] Das Modell der sog. SSI gibt dem Nutzer die Kontrolle über die eigene digitale Identität.[17] Der Benutzer hat mit anderen Worten die Herrschaft über die Gesamtheit seiner eigenen Identitäts-Daten, wodurch er selbst bestimmen kann, welche Informationen bei einem Authentifizierungsvorgang übermittelt werden. Die Bestätigung der Identität ist heute bereits mit den bestehenden Identitätsprovidern wie Google-Login oder Facebook-Login durch «Consent-Screen» möglich. Der Unterschied zu den bestehenden IDP (Identity Providern) ist, dass die «Identifiers» nun dezentral, ohne Zuhilfenahme der IDPs möglich ist, weil diese mit Hilfe der DLT dezentral gespeichert werden können.

[Rz 22] Authentifizierung und Autorisierungen werden in der Regel durch Überprüfung von durch den Prüfer gewünschten Attributen abgewickelt. Man spricht hier von Attributsnachweis bzw. verifiable claims. Die verifiable claims sind Eigenschaften über ein Subjekt (wie bspw. Alter, Geburtsdatum, Diplome etc.). Mit Hilfe von digitalen Signaturen werden diese digital verifizierbar. Dritte können mit Hilfe eines Public Keys die Signatur überprüfen. Vorausgesetzt wird somit, dass eine entsprechend anerkannte Autorität durch Signatur den claim bestätigt hat und der Prüfer über den (nachweislich) zur anerkannten Autorität gehörenden Public Key verfügt oder diesen beschaffen kann.[18]

---

16 Vgl. Michael Isler, Datenschutz auf der Blockchain, in: Jusletter 4. Dezember 2017, Rz. 36 ff.; Gabriel Jaccard/Adrien Tharin, GDPR & Blockchain: the Swiss take, in: Jusletter IT 4. Dezember 2018, m.w.H.

17 Bei der Definition der SSI ist folgendes zu beachten: «One of the first self-sovereign identity initiatives was the Open Mustard Seed framework. It proposed an extra layer on top of the internet, enabling users to become their own central authority. Over the last two years, many more parties worked on a self-sovereign identity management framework.» Dies zeigt, dass der ursprüngliche Gedanke die pure Selbständigkeit des Individuums im Blick hatte. In den weiteren Lösungen wurden jedoch aufgrund der praktischen Notwendigkeit die entsprechenden Stakeholder wieder einbezogen: «To retain a holistic view of the Self-Sovereign Identity concept, and develop the most exhaustive system requirements as possible, the results of the introspection should be validated by a diverse set of stakeholders. At the very least, input from Government, Financial Services, and R&D/Academia is needed.» Zum Ganzen: https://www.researchgate.net/profile/Marvin_Van_Wingerde2/publication/326914271_BLOCKCHAIN-ENABLED_SELF-SOVEREIGN_IDENTITY_An_exploratory_study_into_the_concept_Self-Sovereign_Identity_and_how_blockchain_technology_can_serve_the_fundamental_basis/links/5b6c10bb299bf14c6d97a85b/BLOCKCHAIN-ENABLED-SELF-SOVEREIGN-IDENTITY-An-exploratory-study-into-the-concept-Self-Sovereign-Identity-and-how-blockchain-technology-can-serve-the-fundamental-basis.pdf.

18 Vgl. Jakob Zanol/Alexander Czadilek/Kaspar Lebloch, Self-Sovereign Identity und Blockchain, in: Jusletter IT 22. Februar 2018; siehe hierzu unter https://www.netzwoche.ch/news/2018-05-30/die-blockchain-als-vermittlerin-der-e-id (Abruf 6. Februar 2019).

b. Rechtliche Ausführungen

[Rz 23] Wie oben bereits erwähnt, hat der Nutzer die vollständige Kontrolle über seine digitalen Daten und ist zu jeder Zeit grundsätzlich in der Lage über deren Löschung, Änderung und Freigabe zu entscheiden. Eine Ausnahme davon besteht betreffend dem Public Key, wenn die Blockchain als Speicherungsmedium für diesen fungieren soll. Das gleiche gilt für in der Blockchain gespeicherte Claims, wie es DID vorsieht (vgl. ERC 780 und ERC 1056 bzw. uPort «Claims Registry»)[19].

[Rz 24] Je nach Ausgestaltung kann die SSI weitergehen, als die Gesetzgebung dies durch den Datenschutz nach DSG sowie DSGVO verlangt, da der Nutzer auch über Daten wie Mailadressen verfügen könnte, welche nach wie vor im Rahmen des Marketings genutzt werden. Datenschutzrechtlich bietet diese technische Lösung somit gewisse Vorteile, denn die Datenhaltung liegt nunmehr beim Nutzer und Fragestellungen hinsichtlich Recht zur Bearbeitung, Speicherung und Herausgabe erübrigen sich dahingehend zu einem gewissen Teil.[20] Jedoch darf nicht vergessen werden, dass obwohl im Prozess der Authentifizierung bestimmt werden kann, ob bestimmte Informationen preisgegeben werden, kaum eine Kontrollmöglichkeit darüber besteht, was danach mit den freigegebenen Daten geschieht. Der Empfangende kann diese immer noch missbrauchen, ungenügend sichern oder gegen Vereinbarungen bzw. die jeweils getroffene Datenschutzerklärung verstossen. Auch diese Lösung bietet dahingehend keine absolute Sicherheit.

c. Nutzung der SSI mit Blick auf Blockchain

[Rz 25] Gemäss Zanol, Czadilek, Lebloch zeichnen sich zwei Ansätze ab, wie die Nutzung der SSI mitunter vornehmlich erfolgen wird: Einerseits würde sich die Speicherung von Hashwerten der jeweiligen Identitätsattribute auf der Blockchain einiger Beliebtheit erfreuen. Auf der anderen Seite sei die entsprechende Speicherung der Metadaten (Public Keys und sogenannte Service-Endpoints, an welchen mit Services des Identitätseigentümers in Kontakt getreten werden kann)[21], welche ausschliesslich die Kommunikation mit dem Agent[22] ermöglichen sollen, eine gängige Variante.[23]

[Rz 26] Auch im vorliegenden Use Case hat die Person selbst die Hoheit über die Herausgabe der Daten. Sie hat somit auch die Verantwortung betreffend ihrer persönlicher Informationen. Darüber hinaus soll in dieser Lösung sowohl der Public Key als auch der Hash des An- und Abwesenheitsprotokolls auf der Blockchain abgelegt werden. Diese beiden technischen Aspekte werfen datenschutzrechtliche Fragen auf, die in der Folge beleuchtet werden.

---

19 Joel Torstensson, ERC1056 ERC780 an open identity and claims protocol for Ethereum, https://medium.com/uport/erc1056-erc780-an-open-identity-and-claims-protocol-for-ethereum-aef7207bc744 (Abruf 6. Februar 2019).

20 Vgl. Fabian Kirstein/Manuel Polzhofer/Klaus-Peter Eckert, Digitale Identitäten in der Blockchain – Erfahrungen aus der Entwicklung, Digital Public Services (DPS), Berlin 2018; vgl. Zanol/Czadilek/Lebloch (Fn. 18), 1 ff.

21 «Ein DID-Dokument ist eine JSON-Datenstruktur, die den Identitätseigentümer beschreibt. Um Privacy by Design sicherstellen zu können, beschränkt sich diese Beschreibung auf die Metadaten, Public Keys (öffentliche Schlüssel) und sogenannte Service-Endpoints, an welchen mit Services des Identitätseigentümers in Kontakt getreten werden kann. Es gibt jedoch auch Konzepte, die ein erweiterbares DID-Dokument vorsehen, und somit das tatsächliche Ablegen von persönlichen Daten auf dem öffentlichen Ledger erlauben sollen.» Zanol/Czadilek/Lebloch (Fn. 18), 10.

22 Der Agent speichert die überprüfbaren Daten des Identitätseigentümers und ist somit für deren Nachweis zuständig.

23 Vgl. Zanol/Czadilek/Lebloch (Fn. 18), 17 ff.

5. Blockchain und Datenschutz

[Rz 27] Das Design der Blockchain sieht vor, dass durch die Verkettung von Blöcken mittels Hash jegliche Manipulation sofort ersichtlich ist. Es kann somit keine Änderung oder Löschung erfolgen, ohne dass der Originalitätswert der Blockchain verloren geht. Im Lichte des DSG und der DSGVO bedarf somit die Verwendung dieser Technologie im Bereich von Personendaten einer vertieften Prüfung.

[Rz 28] Primär ist die Ausgestaltung der Blockchain zu beachten: Man unterscheidet im Allgemeinen zwischen public und private Blockchain. Public Blockchains stehen jedem, der über die notwendige Software verfügt, offen und sind somit öffentlich einsehbar.[24] Aufgrund des allgemeinen Zugangs der öffenlichen Blockchain und der damit einhergehenden generellen Sichtbarkeit der Daten, die weder gelöscht noch verändert werden können, stehen diese in einem besonderen Spannungsverhältnis mit dem DSG und der DSGVO. Demgegenüber hat bei einer private Blockchain nur ein konkret bestimmter Kreis Zugang zu den Daten. Dieser Einschränkung zufolge weist die private Blockchain weniger Problemfelder auf.

[Rz 29] Eine weitere Unterscheidung liegt in der Regulation der Schreib- und Validierungsberechtigung. Es gibt die Möglichkeit, diese Kompetenzen nur einem beschränkten Kreis von Teilnehmern zu erlauben; in diesen Fällen spricht man von einer permissioned Blockchain. Wenn keine Beschränkung besteht, so liegt eine permissionless Blockchain vor. Der Vorteil bei der private permissioned Blockchain ist, dass aufgrund der Notwendigkeit einer zentralen Instanz eine Verantwortlichkeit klar definiert werden kann. Ebenfalls kann im Zuge der Registrierung den datenschutzrechtlichen Vorgaben entsprochen, bzw. die Informationspflichten erfüllt sowie die erforderlichen Einwilligungen eingeholt werden. Je nach Ausgestaltung birgt die Blockchain somit in Hinblick auf den Datenschutz unterschiedlich ausgeprägte Fragestellungen.[25]

[Rz 30] Im Folgenden wird die public Blockchain und die damit verbundenen Fragen diskutiert. Die Unterscheidung permissioned/permissionless wird jeweils (sofern relevant) nur kurz beleuchtet.

6. Public Key auf der Blockchain

a. Einleitende Bemerkungen

[Rz 31] Wie oben dargestellt, ist der Begriff «Personendaten» sowohl im Rahmen des DSG als auch der DSGVO weit gefasst. Da im vorliegenden Use Case der Public Key auf der Blockchain gespeichert werden soll, stellt sich die Frage nach dessen rechtlicher Qualifikation. Um diese Einordnung vorzunehmen, ist zunächst die Funktion des Schlüsselpaares (Public und Private Key), bzw. die dadurch ermöglichte asymmetrische Verschlüsselung zu betrachten.

[Rz 32] Dieses sog. asymmetrische Kryptosystem ist ein Verschlüsselungsverfahren, bei dem die Parteien keinen gemeinsameen Schlüssel zur Dechiffrierung benötigen. Jeder Nutzer erzeugt ein eigenes Schlüsselpaar, der private und der öffentliche Schlüssel, die mathematisch miteinander verbunden sind. Mit dem Private Key können Dokumente, die mit dem öffentlichen Schlüssel verschlüsselt wurden, entschlüsselt werden und umgekehrt. Der private Schlüssel ist geheim zu

24 Als Beispiel kann an dieser Stelle auf Kryptowährung/Bitcoin verwiesen werden.

25 Siehe hierzu weiterführend Stengel/Aus der Au (Fn. 5) S. 439 ff.; Isler (Fn. 16), 1 ff.; https://www.cio.de/a/blockchain-ein-dilemma-fuer-den-datenschutz,3545513 (Abruf 6. Februar 2019).

halten. Der öffentliche Schlüssel hingegen muss notwendigerweise veröffentlicht oder zumindest bestimmten Dritten bekannt gemacht werden. Dabei ist zu beachten, dass keine Möglichkeit besteht, den privaten aus dem öffentlichen Schlüssel herzuleiten.[26]

[Rz 33] Das Schlüsselpaar Private und Public Key soll somit den Aussteller der Dokumente oder der jeweiligen Transaktion mit einer gewissen Sicherheit ausweisen. Durch diese Zurechenbarkeiten kann mithin eine gewisse Sicherheit im Geschäftsverkehr geschaffen werden.

b. Einordnung des Public Keys

[Rz 34] Bei dieser gesamthaften Betrachtungsweise könnte man beim Schlüsselpaar als solches von personenbezogenen Daten ausgehen. Betrachtet man die asymmetrische Verschlüsselung differenzierter, kommt man nicht umhin zu fragen, ob der tatsächliche Bezug nicht lediglich durch den Private Key gegeben ist und der Public Key demgegenüber nur das Werkzeug darstellt, um die Funktion des Private Keys zu ermöglichen. Gerade mit Blick auf Bitcoin ist erkennbar, inwiefern diese Frage berechtigt ist: Mittels Private Key kann eine digitale Signatur erstellt werden, die die Bitcoins weiter transferiert. Der damit verbundene Public Key kann von jedermann zur Überprüfung der Transaktion genutzt werden. Durch diesen können keine Rückschlüsse auf den Private Key gemacht werden und somit auch nicht auf die Person (oder das Unternehmen), wenn nicht die Umstände dazu führen, dass eine Identifikation möglich wird. Im Falle von Bitcoin hat die Forschung jedoch gezeigt, dass öffentliche Schlüssel oft über Zusatzinformationen mit natürlichen Personen verbunden werden können. In diesen Fällen wird somit vertreten, dass von einem personenbezogenen Datum gesprochen werden muss.[27] Dies zeigt auf, dass für eine korrekte Einordnung eine Einzelfallbetrachtung notwendig und jeweils darauf abzustellen ist, ob aufgrund der Umstände der Public Key einer bestimmten Person zugeordnet werden kann.

c. Zum vorliegenden Use Case

[Rz 35] Vorliegend wird sowohl der Public Key der Einzelperson im Rahmen der SSI auf einer Blockchain gespeichert als auch jener der anerkannten Zertifizierungsstelle.

[Rz 36] Wenn der öffentliche Schlüssel nur mit einem Unternehmen verbunden werden kann, hat dieser nicht als personenbezogene Daten nach DSGVO zu gelten.[28] Im Rahmen der kommenden Revision des DSG sollen im Sinne der Harmonisierung mit der DSGVO juristische Personen vom Schutzbereich ausgeschlossen werden. Bis zur allfälligen Gesetzesänderung ist jedoch von der juristischen Person als Subjekt des Datenschutzes auszugehen.

[Rz 37] Der Key wird – auf den vorliegenden Fall reduziert – lediglich auf der Blockchain abgespeichert. Es finden demnach in diesem Zusammenhang keine weiteren Transaktionen statt. Folglich ist fraglich, ob von dem Public Key auf das Zertifizierungsunternehmen geschlossen werden kann. Gemäss dem heutigen Stand der Technik ist dies nicht möglich und auch künf-

---

26 Kryptowissen.de, Asymmetrische Verschlüsselung, https://www.kryptowissen.de/asymmetrische-verschluesselung.html (Abruf 11. April 2019), m.w.H.

27 Vgl. Stengel/Aus der Au (Fn. 5), 438 f.; Jaccard/Tharin, (Fn. 22), Rz. 15 ff.

28 Die DSGVO hat den Datenschutz für juristische Personen ausgeschlossen; die Schweiz versucht mit der Revision des DSG gleichzuziehen. Siehe hierzu Botschaft vom 15. September 2017 zur Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941 ff.

tig wäre dies ein grösserer technischer Aufwand. Bei dieser Betrachtung ist somit nicht von einem Personendatum auszugehen. Es ist jedoch durchaus möglich, dass eine Zertifizierungsstelle sein Schlüsselpaar nicht nur für diesen Case einsetzt, sondern es sich auch noch weiter zu Nutze macht. Ebenfalls muss eingeräumt werden, dass bei einem kleinen Kreis von Zertifizierungsunternehmen nicht ausgeschlossen werden kann, dass in Verbindung mit weiteren Informationen der Public Key schlussendlich doch einem Unternehmen zugeordnet werden könnte. Der Personenbezug bleibt jedoch nach wie vor sehr schwach. Selbst bei öffentlicher Bekanntgabe ist wohl kaum von einer Persönlichkeitsverletzung auszugehen.

[Rz 38] Darüber hinaus wird im vorliegenden Use Case das Zertifizierungsunternehmen ein Interesse daran haben, dass der Public Key öffentlich ist und gespeichert wird, da ansonsten das System und die vereinfachte Handhabung der Prüfung nicht funktionieren würde. Dennoch ist darauf hinzuweisen, dass der Inhaber des Public Keys entscheidet, ob und wenn ja, wo er diesen veröffentlicht. Daher ist auch bei diesem Use Case die Zertifizierungsstelle vorgängig über Art und Ort der Speicherung in Kenntnis zu setzen. Um allfälligen Streitigkeiten entgegen zu wirken, wird im Zuge der Informierung der einzubindenden Unternehmen direkt eine Einwilligung im Sinne von Art. 13 DSG eingeholt.

[Rz 39] Hinsichtlich dem Recht auf Löschung kann Folgendes festgehalten werden: Einerseits besteht die Möglichkeit, dass der Private Key vernichtet wird und so auch der Public Key keine Verwendung mehr findet, bzw. seines Sinnes und Zweckes entleert ist. Auf der anderen Seite wäre ein Löschungsbegehren, nachdem die Funktionsweise der Blockchain bekannt ist und auch welche Gesetze diesem inhärent sind, als Verletzung gegen den Grundsatz von Treu und Glauben gemäss Art. 2 ZGB zu werten.

[Rz 40] Das Gesagte hat ebenfalls für die öffentlichen Schlüssel der Privatperson, in casu den Mitarbeiter, zu gelten. Die Ablage der Public Keys dient lediglich der Erfassung und es können keine Rückschlüsse auf die Person gemacht werden. Aufgrund dessen liegt keine datenschutzrechtliche Problematik vor.[29] Im Rahmen der Identifizierung der Mitarbeitenden ist, aus den oben genannten Gründen, über die Speicherung des Public Keys zu informieren und allenfalls das Einverständnis nach Art. 13 DSG und Art. 6 DSGVO zu verlangen. Auch hier kann dies im Zuge der Einbindung in das System erfolgen.

7. Hash auf der Blockchain

a. Einleitende Bemerkungen

[Rz 41] Hashes (sog. Verschlüsselungswerte) werden mittels Hash-Algorithmen erstellt. Ein Hashwert kann als Prüfsumme bezeichnet werden, die aus dem zu prüfenden Inhalt selbst errechnet werden kann. Der Hash ist mit dem Fingerabdruck vergleichbar, der die ursprünglichen Daten charakterisiert. Aus dem Hashwert kann nicht auf das ursprüngliche Objekt geschlossen werden, es könnte höchstens durch Ausprobieren gefunden werden (sog. Nichtreproduzierbarkeit).[30] Zu erwähnen ist jedoch, dass je mehr Informationen über die Generierung des Hashes

29 Selbstredend könnte auch eine andere technische Möglichkeit für Erfassung des Public Keys dienen. Im Rahmen dieses Use Cases wurde jedoch zur Klärung jedweder Fragestellung in Zusammenhang mit Blockchain diese wo möglich integriert und als Variante geprüft.

30 Vgl. Ziff. 14 DSGVO: «Der durch diese Verordnung gewährte Schutz sollte für die Verarbeitung der personenbezogenen Daten natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gelten. Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als

vorliegen, desto eher kann der Lösungsraum einer Brute-Force-Attacke[31] eingeschränkt werden, was die Herleitbarkeit des Hashes erhöht.

b. Einordnung des Hashwertes gemäss bestehender Literatur

[Rz 42] Sind neben den Hashwerten keine weiteren Merkmale oder Transaktionen auf der Blockchain, werden lediglich die ausserhalb des Systems abgelegten Daten nachgewiesen. Erst wenn der Hashwert als ID fungiert und mit weiteren Daten oder mit Transaktionen verknüpft wird, kann ein Personenbezug hergeleitet werden. Dies nicht aufgrund des Hashwertes selbst, sondern vielmehr aus dem Netz von Informationen, welche die Vorgänge erzeugen.

[Rz 43] Stengel/Aus der Au wollen gehashte Daten immer als Personendaten nach DSGVO gelten lassen. Sie berufen sich dabei auf die Artikel-29-Datenschutzgruppe, gemäss welcher Hashfunktionen als Technik zur Pseudonymisierung – statt Anonymisierung – gelten sollen.[32]

[Rz 44] Die Artikel-29-Datenschutzgruppe hat sich in ihrer Stellungnahme 0829/14/EN, WP216 wie folgt geäussert: « [. . .] Wenn jedoch der Bereich der Eingabewerte der Hash-Funktion bekannt ist, können diese über die Hash-Funktion wiedergegeben werden, um den richtigen Wert für einen bestimmten Datensatz abzuleiten. Wurde beispielsweise ein Datensatz durch Hashing der nationalen Identifikationsnummer pseudonymisiert, so kann dies einfach durch Hashing aller möglichen Eingabewerte und Vergleich des Ergebnisses mit den Werten im Datensatz abgeleitet werden. Hash-Funktionen sind in der Regel so konzipiert, dass sie relativ schnell zu berechnen sind und Brute-Force-Angriffen ausgesetzt sind. Die Verwendung einer salted-hash-Funktion (bei der ein Zufallswert, das so genannte Salz zu dem zu hashenden Attribut hinzugefügt wird) kann die Wahrscheinlichkeit der Ableitung des Eingabewerts verringern, aber dennoch kann die Berechnung des ursprünglichen Attributwerts, der sich hinter dem Ergebnis einer salted Hash-Funktion verbirgt, mit angemessenen Mitteln noch möglich sein.»

[Rz 45] Andere Autoren wählen für die Einordnung eine differenzierte Betrachtungsweise. So beispielsweise Erbguth: «Werden kryptografische Hashwerte auf einer öffentlichen Blockchain abgelegt, so beweist der Hashwert selbst zunächst nur, dass das digitale Objekt zum Zeitpunkt des Erstellens des Blocks existierte. Sind auf der Blockchain keine weiteren Merkmale oder Transaktionen neben dem Hashwert aufgeführt, so validiert der Hashwert damit lediglich ausserhalb der Blockchain befindliche Daten. Werden diese ausserhalb der Blockchain abgelegten Daten gelöscht, ist damit auch der Hashwert auf der Blockchain ohne jede Aussagekraft. Anders sieht es aus, wenn der Hashwert als eine Art pseudonyme ID mit weiteren Daten, wie z.B. Transaktionen, verknüpft wird. Dann allerdings ergibt sich der Personenbezug nicht aus dem Hashwert selbst, sondern aus dem Netz der darüber verknüpften weiteren Informationen.»[33] Mittlerweile hat ebenfalls EU Blockchain Observatory festgehalten, dass die Einordnung des Hashes an-

---

juristische Person gegründeter Unternehmen, einschliesslich Name, Rechtsform oder Kontaktdaten der juristischen Person.»

31 Eine Burteforce-Attacke ist der Angriff auf einen kryptografischen Algorithmus, wobei systematisch alle möglichen Kombinationen (Ziffern, Buchstaben und Leerzeichen) durchexerziert werden. Das Ziel dabei ist, verschlüsselte Passwörter, Dateien, Nachrichten und Informationen zu eruieren.

32 Die Autoren beziehen sich in der Folge jedoch auch eher auf die Umstände, statt der im Paper erwähnten Möglichkeit der Ableitung. Stengel/Aus der Au (Fn. 5), 445.

33 Erbguth (Fn. 15), Ziff. 3.1.; Jörn Erbguth, Blockchain und DSGVO in: Jusletter IT 21. Februar 2019, Rz. 9 ff.

spruchsvoll sei und nicht ohne Weiteres erfolgen könne, da es sich hierbei um eine Grauzone handle.[34]

c. Einordnung des Hashes anhand des vorliegenden Use Cases

[Rz 46] Im vorliegenden Use Case wird aus den Protokollen periodisch ein Hash generiert, der zu Zwecken des Nachweises und zur Sicherstellung der Unveränderbarkeit auf der Blockchain gespeichert wird. Diese Hashes basieren auf den Informationen betreffend Ein- und Austritt der zertifizierten Personen. Aufgrund des oben Erwähnten stellt sich die Frage, ob ein Personenbezug gegeben ist, da nicht nur hinsichtlich einzelner Personen, sondern auch bei Personengruppen ein Schutz besteht.

[Rz 47] Der Hash wäre als Personendatum zu qualifizieren, wenn im Sinne von Art. 4 DSG und Art. 5 DGVO aufgrund der Umstände auf den Inhalt bzw. die Personen geschlossen werden könnte (indirekte Bestimmbarkeit). Da in casu weder Transaktionen noch andere Handlungen vorgenommen werden, die zu weiteren Informationen führen könnten, ist dahingehend ein Rückschluss nicht möglich. Dem steht die obige Stellungnahme der Artikel-29-Datenschutzgruppe gegenüber, wonach ein Hash allgemein als pseudonymisiertes Personendatum zu betrachten ist, da es möglich sein könnte dieses zu erraten, wenn man gewisse Parameter weiss. Diesen Ausführungen ist entgegenzuhalten, dass mit Blick auf den technischen Aspekt des Hashings je nach Grösse des Bereiches der Eingabewerte zu differenzieren ist. Hierzu folgende Erklärung anhand des Beispiels von Passwörtern, die gehasht werden: Wenn der Bereich der Eingabewerte aus einem 8-stelligen Passwort besteht, dessen Stellen die Zahlen 0–9 enthalten können, ergibt sich eine mögliche Kombination von 8^10 Werten (= 1'073'741'824). Diese zu hashen dauert aufgrund ihrer Einfachheit entsprechend kurz. In der Folge gestaltet sich der Vergleich und somit die Ableitung des ursprünglichen Eingabewertes ebenfalls einfach, sofern die Struktur des Wertes (8-stellig und Zahlen von 0–9) bekannt ist. Wenn nun die Kombination 24 Stellen hat und neben den Zahlen auch Buchstaben möglich sind, dann ergibt dies bereits 24^36 = 4.87e+49 mögliche Werte. In diesem Falle dauert die Ermittlung, selbst wenn man pro Sekunde zwei Millionen Hashes berechnen könnte, 7.5e+35 Jahre. Die Bitcoin Hashrate[35] beträgt aktuell 70'000'000 Terra Hashes/s – selbst wenn man diese Leistung für die Eruierung verwenden würde, bedürfte es 22'064'803'018'079'654'732'689.4 Jahre, um eine Entschlüsselung vorzunehmen. Im Übrigen besteht zur Verhinderung der Ermittlung die Möglichkeit, ausser dem Hash selbst noch einen geheimen Schlüssel einzufügen, der lediglich zwischen den Knoten der Blockchain geteilt wird. Dies kann selbst bei «einfachen» Hashes (insbesondere Daten mit geringer Entropie[36]) verhindern, dass die Ermittlung möglich ist, wodurch eine höhere Sicherheit gewährleistet wird.

[Rz 48] Mit Blick auf die obigen Ausführungen, wonach ein Bezug gemäss Datenschutz nur solange als gegeben erachtet wird, als die Identifizierung ohne unverhältnismässigen Aufwand mög-

34 The EU Blockchain Observatory and Forum, Blockchain and the GDPR, 16. Oktober 2018, https://www.eublockchainforum.eu/reports, S. 21 ff.

35 Die Fähigkeit der gesamten Rechenkapazität im Bitcoin-Netzwerk Hashes zu berechnen.

36 «Unter Entropie verstehen Physiker ein Mass für die möglichen Zustände, die ein System einnehmen kann. Je höher die Entropie, desto höher die Unordnung eines Systems. Weil Informationen im Prinzip geordnete Daten sind, ist die Entropie in der Informationstechnik auch ein Mass für den Informationsgehalt einer Datenmenge. Im Zusammenhang mit kryptographischen Systemen lässt sich mit ihr daher auch die Zufälligkeit einer Datenmenge beschreiben.» https://www.heise.de/glossar/entry/Entropie-397939.html (Abruf 6. Februar 2019).

lich ist, wird ersichtlich, dass je nach Entropie nicht mehr von Personendaten gesprochen werden kann. Ebenfalls kann nicht per se auf eine Pseudonymisierung geschlossen werden. Bei jener besteht – wie unter III, A. 2 dargestellt – ein Schlüssel, der es dem Inhaber erlaubt, die Pseudonymisierung aufzuheben. Da der Hash wie oben dargestellt nicht reversibel ist, somit kein Schlüssel besteht, um die verhashten Informationen festzustellen, hat er auch nicht als Pseudonym zu gelten. Die Sachlage ist eher mit jener der anonymisierten öffentlichen Urteile zu vergleichen. Das Gericht und die beteiligten Personen kennen die Identitäten der Parteien, die in der öffentlichen Version als Person A, Unternehmen X oder ähnlich bezeichnet werden. Nichtsdestotrotz wird von einer Anonymisierung gesprochen, da kein Schlüssel existiert, der aus dem Terminus «Person Y» die darunter liegende tatsächliche Identität eruieren kann. Es ist jedoch aufgrund des heutigen umfassenden Informationsflusses immer möglich mit genügend Recherche die jeweiligen Beteiligten ausfindig zu machen. Gemäss dem Entscheid der Eidgenössischen Rekurskommission für Staatshaftung vom 15. Februar 2006, ist die Anonymisierung genügend, wenn der Aufwand zur Feststellung der Identität des Beschwerdeführers so gross erscheint, dass ihn ein Dritter, der an den Angaben interessiert ist, vernünftigerweise nicht auf sich nehmen wird (E. 5b, c). Es liegt überdies keine Verletzung des Anonymisierungsgrundsatzes vor, wenn Personen, welche mit den Einzelheiten des Falles vertraut sind, gegebenenfalls erkennen können, um wen es sich handelt.[37] Folglich ist die generelle Annahme, dass ein Hash per se nicht als Anonymisierung, sondern als Pseudonymisierung und als Personendatum zu qualifizieren sei, verfehlt. Vielmehr sollte im Einzelfall geprüft werden, ob ein Rückbezug mit verhältnismässigem Aufwand möglich ist.

[Rz 49] Im vorliegenden Use Case stellt sich daher die Hauptfrage, wie gross der Bereich der Eingabewerte ist. Das Log erfasst Ein- und Ausgänge im Bereich von Millisekunden, welche ebenfalls zu den verhashten Daten gehört. Dies mit allen anderen Eingaben zu erraten bzw. zu berechnen, ist vergleichbar mit dem oben aufgeführten Beispiel zu 24-stelligen Passwörtern. Folglich kann kein Rückbezug angenommen werden und der Hash gilt nicht als personenbezogenes Datum.

[Rz 50] Selbst wenn bei den Hashes von einem Personenbezug ausgegangen werden müsste, würde dies den vorliegenden Use Case nicht verunmöglichen. Die Erfassung der Daten wäre über die Notwendigkeit im sicherheitsrelevanten Bereich meist über eine gesetzliche Grundlage gerechtfertigt. Das gilt etwa für die Protokollierung, welche im Interesse der Sicherheit und somit ebenfalls in jenem der Allgemeinheit erfolgt. Die Speicherung dient in diesen Fällen somit einem übergeordneten Interesse und ist aufgrund dessen nach Art. 13 DSG sowie Art. 6 DSGVO gerechtfertigt. Zudem darf Folgendes nicht vergessen werden: werden die externen Daten gelöscht, aufgrund deren der Hash entstanden ist, so ist Letzterer seines Inhaltes entleert und dadurch ohne jede Aussagekraft. Folglich könnte dem im DSG und insbesondere in der DSGVO geforderten Recht auf Berichtigung und Löschung gerecht werden.

d. Exkurs: Vergleich zur AHV- bzw. Sozialversicherungsnummer

[Rz 51] Die aktuelle AHV-Nummer der Schweiz hat 13 Stellen und enthält im Gegensatz zu den früheren Nummern keinerlei Personenkennzeichen mehr.[38] Aufgrund dessen wird diese Sozi-

37 Eidgenössische Rekurskommission für die Staatshaftung, Entscheid vom 15. Februar 2006 http://vpb.admin.ch/rohtexte/R/2006/HRK2005-004.pdf (Abruf 10. April 2019); siehe ebenfalls zur gleichen Thematik Urteil des Bundesgerichts 1A.228/2003 vom 10. März 2004.

38 Proxena GmbH, Sozialversicherungsnummer, https://www.sozialversicherungsnummer.ch/, mit weiteren Hinweisen (Abruf 6. Februar 2019).

alversicherungsnummer als sog. Nichtsprechende Nummer ausgewiesen und ist im Sinne von Art. 3 lit. a DSG 1. Teilsatz betreffend Bezug auf eine bestimmte Person nicht als geschütztes Personendatum zu qualifizieren. Wie erwähnt, hängt die Qualifikation im Sinne des zweiten Teilsatzes von Art. 3 lit. a DSG betreffend die bestimmbare Person davon ab, ob mit vernünftigem Aufwand mit zusätzlichen Informationen eine Individualisierung möglich ist.[39] Aufgrund des oftmals kontrovers diskutierten[40] exzessiven Gebrauchs der AHV-Nummer und der jeweiligen Verknüpfung und Ablage mit weiteren Angaben zur Person, hat die Nummer – trotz der Unmöglichkeit des Rückschlusses und der eigentlichen völligen Anonymität – nunmehr in weiten Bereichen grundsätzlich als Personendatum zu gelten.[41]

[Rz 52] Mit Blick auf die obigen Ausführungen fällt somit Folgendes auf: Einerseits hat dieses Praxisbeispiel gezeigt, dass eine absolut nicht rückverfolgbare Nummer in Verbindung mit weiteren Informationen doch verhältnismässig leicht zu einem Personendatum werden kann, wobei auch hier wieder eine Einzelfallbetrachtung gemacht werden muss. Dabei darf nicht vergessen werden, dass jede Person Inhaber nur einer einzelnen Nummer sein kann, wodurch bei entsprechender Nutzung eine grössere Möglichkeit der Informationssammlung besteht. Dies ist bei Public/Private Keys oder auch generierten Hashes nicht der Fall. Jede Person kann so viele Keys besitzen wie er will und sie auch nach seinem Willen einsetzen. Dies zeigt, dass hier umso mehr eine Betrachtung des Einzelfalls notwendig ist, da ansonsten nicht adäquate Einordnungen und Rechtsfolgen entstehen.

B. Verantwortlichkeit des Systems

[Rz 53] Bestehende Regelungen zur Haftung wie OR 41, das Produktehaftpflichtgesetz, die Kodifizierungen zur Haftung des Gemeinwesens usw. stellen ausreichende Rechtsgrundlagen dar. Im vorliegenden dezentralen System ist vielmehr fraglich, wie und wo die Verantwortlichkeit zu liegen kommt und wer schlussendlich für was und gestützt auf welche Rechtsgrundlage haftet.[42] Bei der Bitcoin-Blockchain wurde dafür plädiert, dass die Entwickler die Verantwortlichen sind. Dabei müsste mit Blick auf die Produktehaftpflicht die Frage gestellt werden, ob ein Defekt oder ein unerwünschtes Resultat aufgrund der Nutzung entstand oder so gar nicht hätte existieren dürfen. Nur Nutzung, die vernünftigerweise hätte erwartet werden müssen, wäre somit bei Defekten der Technologie selbst zu beachten. Wäre somit erstellt, dass eine fehlerhafte Architektur vorliegt, so könnte man allenfalls eine Verantwortlichkeit der Entwickler annehmen. Jedoch ist eine Durchsetzung der Haftung nur bei den privaten Blockchains möglich, da bei diesen bekannt ist, wer sie aufgebaut hat und betreibt. Bei den öffentlichen Blockchains haben die jeweiligen

39 Thomas Probst, Die unbestimmte «Bestimmbarkeit» der von Daten betroffenen Person im Datenschutzrecht, AJP 2013, S. 1423 ff.

40 An dieser Stelle wird auf die Ausführungen zur Diskussion nicht weiter eingegangen und lediglich auf die Literatur verwiesen: https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/externe/2017-09-27.html, (Abruf 6. Februar 2019); egovernment, Einsatz der AHV-Nummer als einheitlicher Personenidentifikator https://www.egovernment.ch/de/dokumentation/rechtliche-fragen/register/einsatz-der-ahv-nummer-als-identifikator/, (Abruf 6. Februar 2019); https://www.bfh.ch/de/forschung/forschungsprojekte/9d3ecaab-d58e-4236-aeb9-ddee9a93962e/ (Abruf 6. Februar 2019); Konverenz der schweizerischen Datenschutzbeauftragten, Verwendung der AHV-Nummer mit hohen Risiken verbunden, http://www.privatim.ch/de/verwendung-der-ahv-nummer-mit-hohen-risiken-verbunden/ (Abruf 6. Februar 2019).

41 Vgl. SHK-Rudin, Art. 3 N 27.

42 Erbguth (Fn. 33), Rz. 29 ff. m.w.H.; ebenso Jaccard/Tharin (Fn. 16), Rz. 38 ff.

Entwickler meist unter Pseudonymen gearbeitet, wodurch ihre Identitäten unbekannt geblieben sind.[43]

[Rz 54] Auch hinsichtlich der Netzwerkbetreiber ist es schwierig, einen Anknüpfungspunkt für eine Verantwortlichkeit zu erhalten. Lediglich bei einer permissioned Blockchain ist klar, wer genau die Blockchain betreibt bzw. Bewilligungen vergibt etc. und somit für die Nutzung bzw. für die Datenproduktion/-erstellung verantwortlich ist. Bei einer öffentlichen Blockchain ist die Eruierung unmöglich, da das Kollektiv[44], das bekannt ist, bereits viel zu gross ist, um eine Zurechnung zu machen. Darüber hinaus besteht in Ermangelung einer Meldepflicht betreffend die Betreiber ebenfalls eine grosse Dunkelziffer.

[Rz 55] Hinsichtlich der Transaktionen wurde dafür plädiert, dass derjenige, der eine Transaktion erstellt, signiert und in das Bitcoin-Netzwerk gibt, der Verantwortliche i.S.v. Art. 4 Nr. 7 DSGVO ist. Eine Transaktion unter die Verantwortlichkeit im Rahmen des DSG/DSGVO zu subsumieren erscheint etwas fragwürdig. Dies nicht zuletzt, weil gemäss Definition von Art. 4 Nr. 7 DSGVO «Verantwortlicher» die Person oder Stelle ist, die über die Zwecke und Mittel der Verarbeitung der Personendaten entscheidet. Diesen Versuch der Subsumtion ist nicht zuletzt die Folge der extensiven Zuordnung von Informationen als Personendaten.

[Rz 56] In Fällen, bei welchen man nicht umhinkommt, von Personendaten in Zusammenhang mit Blockchain zu sprechen, hat folgendes zu gelten: Jeder hat sich an die Bearbeitungsgrundsätze gemäss Art. 4 DSG zu halten bzw. dafür besorgt zu sein, dass die Personendaten korrekt und genügend gesichert sind. Demgegenüber wurden im Rahmen der DSGVO die Verantwortung auf vier verschiedene beteiligte Instanzen aufgeteilt: Die betroffene Person (Art. 4 Nr. 1 DSGVO), den Verantwortlichen (Art. 4 Nr. 7 DSGVO), den Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) und Dritte (Art. 4 Nr. 10 DSGVO). Dieser Aufteilung liegt die Konzeption zu Grunde, dass jeweils einer dieser Akteure festlegt, zu welchem Zweck mittels welcher Instrumentarien die Personendaten bearbeitet werden sollen und immer auch jener somit – und nie nur der Verarbeiter – die Verantwortung tragen soll. Dass dieses System mit einer klaren Zuordnung im Rahmen der öffentlichen Blockchain nicht greifen kann, ist augenfällig. Aber auch hinsichtlich der Konzeption des DSG dürfte sich, je nach Ausgestaltung der Blockchain (public/privat oder permissioned/permissionless), die Suche und schlussendlich Inpflichtnahme des Verantwortungsträgers als schwierig gestalten.

[Rz 57] Für den vorliegenden Fall gilt somit, dass sofern es sich entgegen der obigen Ausführungen um Personendaten handeln sollte, einerseits die Akteure selbst, welche die Blockchain als Ablage nutzen, entsprechend verantwortlich sind.

[Rz 58] Da allenfalls ein Interesse daran besteht, dass nur bestimmte Informationen, z.B. die anerkannten Ausbildungsstätten, auf der Blockchain gespeichert sind, könnte dahingehend eine permissioned Blockchain geschaffen werden. Insofern hätte man hier auch eine verantwortliche Instanz, namentlich die Stelle, welche die permission vergibt. In diesem Fall würde sich somit auch die Suche nach einem Verantwortlichen erübrigen.

[Rz 59] Im Rahmen der Ablage des Hashes hat man dafür besorgt zu sein, dass dieser so konzipiert ist, dass tatsächlich kein Rückbezug stattfinden kann. Sei es, dass die Informationen eine so hohe

43 GitHub, Ethereum > Contributers https://github.com/ethereum/go-ethereum/graphs/contributors (Abruf 29. November 2018).

44 Vgl. hierzu am Beispiel von Ethereum: Aktuell sind es 15'000 Personen, die öffentlich bekannt geben, dass sie Ethereum-Nodes betreiben; https://www.ethernodes.org/network/1 (Abruf 29. November 2018).

Entropie aufweisen, dass sie in absehbarer Zeit nicht zurückbezogen werden können oder aber, dass ein geheimer Key eingefügt wird, der nur den entsprechenden Parteien bekannt ist.

IV. Fazit

[Rz 60] Wie oben dargestellt, kann die Blockchain mehr als eine Transaktionsplattform für Bitcoin und Co. darstellen. Jedoch ist die Handhabung und Ausgestaltung noch immer mit vielen Unklarheiten verbunden. In diesem Ökosystem der Trustlessness und gleichzeitigen teilweisen Anonymität stellen sich auf rechtlicher Seite etliche Herausforderungen. Dies nicht zuletzt, da sich die technische Seite sehr komplex präsentiert und diese bereits auch nur zu erfassen und zu verstehen eine Sache für sich ist. Eine juristisch korrekte Lösung zu finden, die angemessen ist und die Technologie nicht verunmöglicht, stellt eine nicht unerhebliche Herausforderung dar.

[Rz 61] Vielerorts wird ebenfalls aufgrund der Fortentwicklung der Technik und der allfälligen Möglichkeit künftig mittels Quantencomputern davor gewarnt, mittels Kryptographie etc. zu arbeiten, da man irgendwann in der Lage sein könnte, jedwede Information zu entschlüsseln. Dazu sei Folgendes erwähnt: die Entwicklung der Technologien wird voranschreiten, ob man diese nun einsetzt oder nicht. Sobald Quantencomputer und die dazugehörenden Möglichkeiten Realität sein werden, muss ohnehin der Umgang mit Daten neu überdacht werden und der Datenschutz anders als bisher stattfinden. Man sollte sich somit nicht bereits vorgängig vor den Technologien verschliessen, sondern durch sie lernen, um auf die Änderungen vorbereitet zu sein oder zumindest schnellstmöglich auf sie reagieren zu können.

[Rz 62] Die Technologie bietet, wie aufgezeigt, viele Möglichkeiten für Lösungen von bislang aufwändigen Prozessen, es wäre daher verfehlt, aufgrund von Ängsten und Unsicherheiten das Potenzial nicht auszuschöpfen und den Einsatz der Blockchain im nicht finanziellen Sektor frühzeitig zu verwerfen.

Barbara A. Möri, MLaw Rechtsanwältin, SBB AG, Bern.