www.jusletter.ch

Michael Isler

Datenschutz auf der Blockchain

Datenschutz auf der Blockchain ist rechtlich bislang kaum erforschtes Terrain. Während sich bei geschlossenen Systemen diesbezüglich keine besonderen Herausforderungen stellen, versagen bei offenen Architekturen wie Bitcoin die datenschutzrechtlichen Instrumente. Umso bedeutsamer erweisen sich systemimmanente Datenschutzfunktionen (Privacy by Design), deren Implementierung jedoch auf der Vorstufe der Entwicklung der Technologie und nicht erst im Bearbeitungsstadium zu erfolgen hätte. Zielkonform umgesetzt, hat die Blockchain gar das Potential, die Kontrolle über Personendaten und damit die Einhaltung der Zweckbindung technisch zu unterstützen.

Beitragsarten: Beiträge
Rechtsgebiete: Informatik und Recht

Zitiervorschlag: Michael Isler, Datenschutz auf der Blockchain, in: Jusletter 4. Dezember 2017

Inhaltsübersicht

1. Datenschutz und Blockchain – ein Thema?

1.1. Zwiespältiges Verhältnis

[Rz 1] Das Verhältnis der Blockchain[1] zum Datenschutz ist ein ambivalentes. Öffentliche Blockchain-Anwendungen wie Bitcoin sind gleichsam die Antipode des Datenschutzes: Alle Transaktionen sind jederzeit – wenn auch in verschlüsselter Form – öffentlich einsehbar.[2] Die der virtuellen Währung Bitcoin zugrunde liegende Technologie einer verteilten webbasierten Datenbank (*distributed ledger technology*) zeichnet sich weiter dadurch aus, dass lediglich Einträge hinzugefügt, nicht aber nachträglich entfernt werden können. Schliesslich validiert ein Konsensmechanismus die neuen Einträge unwiderruflich. Daraus ergeben sich u.a. die folgenden Eigenschaften:[3]

- Die nachträgliche Unabänderbarkeit der Daten (*immutabability*);

---

1 Auf eine ausführliche Erläuterung der Funktionsweise der Blockchain-Technologie wird hier verzichtet. Einen guten und aktuellen Überblick aus rechtlicher Sicht bietet statt vieler Markus Kaulartz, Die Blockchain-Technologie, CR 2016, 474–480; vgl. auch Luzius Meisser, Kryptowährungen: Geschichte, Funktionsweise, Potential, in: Rolf H. Weber / Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, 73–92, 81 ff.

2 Joachim Galileo Fasching, Anwendungsbereiche und ausgewählte Rechtsfragen der Blockchain-Technologie, Masterthesis, Wien 2017, 9, abrufbar unter http://www.it-law.at/publikation/anwendungsbereiche-und-ausgewaehlte-rechtsfragen-der-blockchain-technologie/ (Alle Websites zuletzt besucht am 26. Oktober 2017); Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 6, abrufbar unter https://bitcoin.org/bitcoin.pdf.

3 Rainer Böhme / Paulina Pesch, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, in: Datenschutz und Datensicherheit 2017, 473–481, 473.

- die unwiderlegbare Vermutung der Richtigkeit der Daten (*irrefutability*).

[Rz 2] Allein diese zwei Besonderheiten der Blockchain lassen aus datenschutzrechtlicher Sicht aufhorchen, stehen sie doch im Widerspruch zum Berichtigungsrecht, welches sowohl gemäss schweizerischem Datenschutzgesetz (Art. 5 Abs. 2 des Bundesgesetzes über den Datenschutz; DSG[4]) als auch nach der EU Datenschutz-Grundverordnung (Art. 16 DSGVO[5]) einem Datensubjekt in Bezug auf seine Personendaten zusteht. Die datenschutzrechtlichen Betroffenenrechte sind ebenso unverjährbar und unverzichtbar[6] wie die Einträge auf der Blockchain unveränderbar und unwiderlegbar. Unweigerlich muss man auch an das durch den Europäischen Gerichtshof (EuGH) statuierte Recht auf «Vergessenwerden»[7] denken, das in Art. 17 DSGVO als weitreichendes Löschungsrecht kodifiziert wurde. Dieses Recht scheint mit den beschriebenen Grundeigenschaften einer öffentlichen Blockchain ebenfalls inkompatibel zu sein.

[Rz 3] Nun wird man einwenden, dies sei alles irrelevant, denn die Einträge auf einer Blockchain seien zwar öffentlich einsehbar, könnten aber keiner Person zugeordnet werden. Bitcoin wird u.a. mit dem Ziel eingesetzt, anonyme Zahlungstransaktionen abwickeln zu können.[8] Die Identität der Berechtigten ist nicht offengelegt.[9] Bei Anonymität liegen keine Informationen zu einer bestimmten oder bestimmbaren Person und damit keine personenbezogenen Daten im Sinne von Art. 3 lit. a DSG bzw. Art. 4 Nr. 1 DSGVO vor. Aufgrund dieser Verschleierung der Identität ist die Blockchain, trotz oder gerade wegen ihrer umfassenden Transparenz, eigentlich eine datenschutzfreundliche Technologie.

[Rz 4] Bitcoin-Transaktionen sind jedoch nur vermeintlich anonym.[10] Die Identität der Nutzer verbirgt sich hinter einer kryptografischen Identität, einem Pseudonym, dem sog. öffentlichen Schlüssel bzw. der daraus abgeleiteten Bitcoin-Adresse.[11] Eine Untersuchung hat gezeigt, dass es möglich ist, Bitcoin-Adressen von Zahlungsauslösern und Zahlungsempfängern mit der IP-Adresse zu verknüpfen, von welcher die Transaktion ausgelöst wurde.[12] Folgt man der Praxis des Bundesgerichts und des EuGH zum Personenbezug von IP-Adressen,[13] ist mit dieser Zusatzinformation der Weg zur Bestimmbarkeit der betroffenen Person nicht mehr weit. Soweit der öffentliche Schlüssel nicht laufend geändert wird, lassen sich auch Transaktionshistorien zurück-

4 Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1).

5 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).

6 Vgl. Beat Rudin, in: Bruno Baeriswyl / Kurt Pärli (Hrsg.), Stämpflis Handkommentar Datenschutzgesetz (DSG), Bern 2015, Art. 8, N 30.

7 Urteil des EuGH vom 13. Mai 2014 C-131/12 *Google Spain und Google*.

8 Arthur Gervais, Vorteile und Probleme von Blockchains, in: digma 2017, 128–131, 129 f.; Jean-Daniel Schmid / Alexander Schmid, Bitcoin – eine Einführung in die Funktionsweise sowie eine Auslegeordnung und erste Analyse möglicher rechtlicher Fragestellungen, in: Jusletter 4. Juni 2012, Rz. 9.

9 Satoshi Nakamoto (Fn. 2), 6: «*[…] privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone*».

10 Ebenso Schmid / Schmid (Fn. 8), Rz. 10; Gervais (Fn. 8), 129 m.H. auf datenschutzfreundlichere Kryptowährungen.

11 Böhme / Pesch (Fn. 3), 478.

12 Alex Biryukov / Dmitry Khovratovich / Ivan Pustogarov, Deanonymisation of Clients in Bitcoin P2P Network, 5. Juli 2014, https://arxiv.org/abs/1405.7418; vgl. auch Fergal Reid / Martin Harrigan, An Analysis of Anonymity in the Bitcoin System, 7. Mai 2012, https://arxiv.org/abs/1107.4524.

13 BGE 136 II 508, E. 3.2 – *Logistep*; Urteil des EuGH vom 19. Oktober 2016 C-582/14 *Patrick Breyer*, E. 45 ff.

verfolgen und auf diese Weise Profile erstellen.[14] Darüber hinaus bewegen sich in Blockchain-Systemen auch zahlreiche Intermediäre wie Wallet-Provider, denen die Identität ihrer Kunden bekannt ist oder zumindest sein kann.[15] Es wäre daher verfehlt, im Blockchain-Kontext pauschal von Anonymität zu sprechen.

1.2. Offene und geschlossene Systeme

[Rz 5] Das obige Streiflicht hat gezeigt, dass die datenschutzrechtlichen Implikationen der Blockchain-Technologie eine vertiefte Auseinandersetzung verdienen. Dabei ist jedoch im Auge zu behalten, dass es *die* Blockchain nicht gibt. Bitcoin ist zwar die Wiege der Blockchain, aber digitale Währungen sind längst nicht das einzige Anwendungsfeld dieser neuen Technologie. Vielmehr existieren zahlreiche Adaptionen, die in unterschiedlicher Ausprägung die Vorteile eines auf Netzwerkknoten verteilten Registers nutzen.[16]

[Rz 6] Bei der Kategorisierung von Blockchain-Anwendungen sind zwei Ebenen zu unterscheiden, nämlich diejenige der an einer *Blockchain-Transaktion* und diejenige der am *Konsensmechanismus* einer Blockchain beteiligten Akteure:

1.2.1. Die Ebene der an einer Blockchain-Transaktion Beteiligten

[Rz 7] Wenn eine Blockchain jedermann offensteht, um auf ihr Transaktionen zu initiieren, spricht man von einer *public blockchain*. Dies ist bspw. bei Bitcoin und Ethereum der Fall. Es gibt dort keine Wächter, die über den Zutritt zum Blockchain-Universum entscheiden. Das Gegenstück zu diesen offenen Systemen ist die *private blockchain*. Der Lesezugriff und die Berechtigung, Transaktionen ausführen zu lassen, sind dort auf einen bestimmten und bekannten Kreis von Personen beschränkt. Beispiele hierfür sind diverse Konsortialprojekte von Banken oder Versicherungen, die auf Blockchain basieren und in der Regel eine effizientere Geschäftsabwicklung unter den beteiligten Instituten ermöglichen wollen, aber ansonsten wenig mit einer öffentlichen und verteilten Datenbank wie der Bitcoin-Blockchain gemein haben.[17] Auch im geschlossenen Kontext werden aber die erschwerte Abänderbarkeit (zur Verhinderung von Compliance-Verstössen) oder die Elimination von Fehlerquellen (Unmöglichkeit der doppelten Verbuchung einer Transaktion) als Vorteile der Technologie erkannt.[18]

---

14 Vgl. Nakamoto (Fn. 2), 6.

15 Vgl. Böhme / Pesch (Fn. 3), 479.

16 Die nachstehenden Ausführungen stützen sich weitgehend auf Fasching (Fn. 2), 4 f. sowie BitFury Group, Public versus Private Blockchains, Part 1: Permissioned Blockchains, White Paper, 20. Oktober 2015, 10, abrufbar unter http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf.

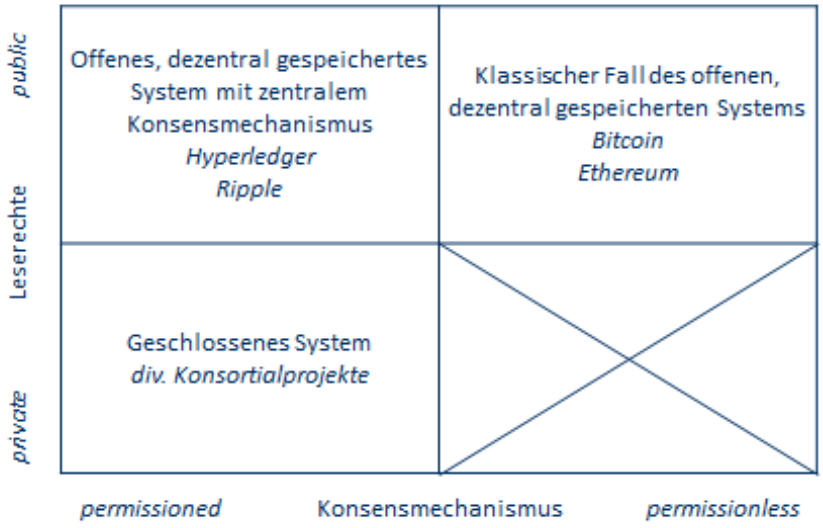
17 Shermin Voshmgir, Blockchains, Smart Contracts und das Dezentrale Web, Technologiestiftung Berlin 2016, 16, abrufbar unter https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf. Beispiele für *permissioned blockchains* sind das Bankenkonsortium 3R (vgl. den Eintrag «R3» in Wikipedia, abrufbar unter https://en.wikipedia.org/wiki/R3_(company)) oder das Versicherungskonsortium 3Bi (vgl. Reuters, Blockchain Consortium Grows to 15 Members, 6. Februar 2017, abrufbar unter https://www.reuters.com/article/blockchain-insurance/blockchain-insurance-consortium-grows-to-15-members-idUSL1N1FR0OG,).

18 Vgl. Peter Rossbach, Blockchain-Technologien und ihre Implikationen, Teil 2: Anwendungsbereiche der Blockchain-Technologie, 2016, 2, abrufbar unter http://blog.frankfurt-school.de/wp-content/uploads/2016/02/Blockchain_FSBlog_part2.pdf.

1.2.2. Die Ebene der am Konsensmechanismus einer Blockchain Beteiligten

[Rz 8] Die verteilte Architektur der öffentlichen Blockchain ohne zentrale Kontrollinstanz verlangt nach einem Konsensmechanismus, der dafür sorgt, dass eine in Auftrag gegebene Transaktion validiert und demgemäss ein neuer Transaktionsblock an die Kette gehängt werden kann, der anschliessend von allen Teilnehmern des Netzwerks als richtig anerkannt wird. Mit diesem Konsensmechanismus lässt sich verhindern, dass Transaktionen doppelt ausgeführt werden (Problem des «*double spending*»).[19] Die angesprochene Validierung sorgt dafür, dass eine auf der Blockchain initiierte Transaktion vollzogen, d.h. ein neuer Block hinzugefügt werden kann, und kompensiert die Abwesenheit der zentralen unabhängigen Vertrauensinstanz, welche in herkömmlichen Systemen die Verantwortung für die Abwicklung der Transaktion übernimmt.[20] In die Rolle der zentralen Vertrauensinstanz schlüpft somit das Prinzip der «*trustlessness*»:[21] Auf der öffentlichen Blockchain übt die Mitwirkung der am Konsensmechanismus beteiligten Akteure die Kontrollfunktion aus.

[Rz 9]



Die gängigsten Konsensmechanismen sind der *Proof of Work* (PoW) und der *Proof of Stake* (PoS). Danach bestimmt entweder die investierte Rechenleistung oder die Teilhabe am Netzwerk darüber, ob eine Transaktion bestätigt wird oder nicht.[22] Bei einer *permissionless blockchain* ist jeder Nutzer berechtigt, Transaktionen zu validieren. Dies ist wiederum bei Bitcoin oder Ethereum der Fall. In der *permissioned blockchain* werden Transaktionen demgegenüber von einer begrenzten Anzahl vertrauenswürdiger Personen validiert, deren Identität bekannt ist.[23] Diese können

19 Fasching (Fn. 2), 9.

20 Vgl. Fasching (Fn. 2), 8; Schmid / Schmid (Fn. 8), Rz. 5.

21 Böhme / Pesch (Fn. 3), 473.

22 Vgl. Meisser (Fn. 1), 82 f.

23 Mirjam Eggen, Chain of Contracts, in: AJP 2017, 3–15, 5; Gervais (Fn. 8), 128; European Union Agency for Network and Information Security (ENISA), Distributed Ledger Technology & Cybersecuirty, 18. Januar 2017, 12, abrufbar unter https://www.enisa.europa.eu/publications/blockchain-security.

Transaktionsblöcke auch rückgängig machen, wenn Konsens besteht.[24] Die in Konsortien organisierten Blockchain-Projekte können diesbezüglich erneut als Beispiel genannt werden.

[Rz 10] Somit stehen sich zwei Systeme gegenüber: Die *public permissionless blockchain* als offenes System auf der einen Seite, die *private permissioned blockchain* als geschlossenes System auf der anderen Seite. Dazwischen liegt die *public permissioned blockchain*. Diese ist zwar dezentral gespeichert, so dass die «Passagiere» frei in die Blockchain einsteigen dürfen, doch wird der Verkehr durch eine oder mehrere bekannte Kontrollinstanzen geregelt.[25] Logisch nicht abbildbar ist eine *private permissionless blockchain*. Dies führt zu folgender Typologie:

1.3. Relevanz der Erscheinungsformen der Blockchain für den Datenschutz

[Rz 11] Für den Datenschutz ergeben sich aus der gezeigten Typologie zwischen offenen und geschlossenen Blockchain-Systemen unterschiedliche Ansätze, was anhand der Kriterien in der nachstehenden Übersichtstabelle illustriert werden kann:

[Rz 12]

Kriterium	***Public permissionless blockchain***	***Public permissioned blockchain***	***Private permissioned blockchain***
System	Offen	Offen	Geschlossen
Konsensmechanismus	Verteilt, anonym	Gebündelt, identifiziert	Gebündelt, identifiziert
Publizität	Öffentliche Lese- und Initiationsrechte; Verschleierung der Identifikationsparameter durch Kryptografie	Öffentliche Lese- und Initiationsrechte; Verschleierung der Identifikationsparameter durch Kryptografie	Beschränkte Lese- und Initiationsrechte; Teilnehmer bekannt
Manipulationsresistenz	Faktische Irreversibilität, sofern keine Konzentration der am Konsensmechanismus Beteiligten vorliegt	Mutier- und Löschbarkeit bei Konsens unter Kontrollinstanzen	Mutier- und Löschbarkeit bei Konsens unter Kontrollinstanzen

[Rz 13] Zentral verwaltete Blockchain-Systeme unterscheiden sich kaum von der Struktur einer herkömmlichen Datenbank. Es gibt Instanzen, welche die datenschutzrechtliche Verantwortung übernehmen können und müssen. Die Systeme sind gegen aussen abgeschottet, die Teilnehmer bekannt. Im Rahmen des Zulassungsverfahrens zum System können auch datenschutzrechtlich

24 ENISA (Fn. 23), 12.

25 Vgl. Gervais (Fn. 8), 128, mit Nennung der Beispiele Hyperledger (https://hyperledger.org/) und Ripple (https://ripple.com/).

notwendige Mitteilungen erfolgen oder Einwilligungen eingeholt werden. Anliegen der betroffenen Personen wie Auskunfts-, Berichtigungs- oder Löschungsrechte können an die Kontrollinstanzen gerichtet und von diesen bedient werden.

[Rz 14] Demgegenüber stossen die datenschutzrechtlichen Instrumente bei offenen Systemen an Grenzen. Die bekannten datenschutzrechtlichen Konzepte gehen regelmässig davon aus, dass eine oder mehrere Personen die Herrschaft über die Zwecke und Mittel der Bearbeitung von Personendaten innehaben. Besonders konsequent geht hierbei die DSGVO vor, indem sie die Verantwortung für die Einhaltung des Datenschutzes strikte dem «Verantwortlichen» gemäss Art. 4 Nr. 7 zuweist.[26] Das schweizerische Datenschutzrecht ist diesbezüglich weniger rigide. Jeder, der Personendaten bearbeitet, ist Adressat der datenschutzrechtlichen Bearbeitungsgrundsätze. Daneben existiert der «Inhaber einer Datensammlung» gemäss Art. 3 lit. i DSG als qualifizierter Datenbearbeiter, bei dem für gewisse Aufgaben die Verantwortung gebündelt wird.[27] Im gegenwärtigen Entwurf des zu revidierenden Datenschutzgesetzes[28] wird dieses Konzept grundsätzlich beibehalten, die Rolle des Inhabers der Datensammlung aber durch den Verantwortlichen abgelöst und ausgebaut.[29]

1.4. Fokus auf offene Systeme

[Rz 15] Um die Eingangsfrage zu beantworten: Datenschutz auf der Blockchain ist ein Thema, kann aber je nach Ausgestaltung der Datenbank ganz unterschiedliche Richtungen einschlagen. Solange wir uns in den vertrauten Gewässern der geschlossenen Systeme bewegen, liegen die Lösungen auf der Hand. Anspruchsvolle und bisher auch kaum untersuchte Rechtsfragen stellen sich hingegen bei der öffentlichen Blockchain, deren Akteure in einer verteilten Konsensstruktur ohne zentralen Kontrollmechanismus wirken. Aus diesem Grund wird der vorliegende Beitrag auf diese offenen Architekturen fokussieren. Wenn im Folgenden etwas unpräzise von öffentlicher Blockchain die Rede ist, ist mithin die *public permissionless blockchain* gemeint.

2. Anwendbarkeit des Datenschutzrechts

2.1. Kollisionsrecht

[Rz 16] Bevor geprüft werden kann, ob und inwiefern Datenschutz auf der Blockchain greift, ist das anwendbare Recht zu bestimmen. Als global verteiltes Netzwerk, bei dem eine Vielzahl von Knoten den gesamten Inhalt der Datenbank parallel verarbeitet, bietet die Blockchain reihenwei-

---

26 Vgl. Jürgen Hartung, in: Jürgen Kühling / Benedikt Buchner (Hrsg.), DS-GVO Kommentar, München 2017, Art. 4 Nr. 7, N 6.

27 Z.B. Auskunftserteilung (Art. 8 DSG), Anmeldung von Datensammlungen (Art. 11a Abs. 5 DSG), Einhaltung der Informationspflichten bei der Beschaffung von besonders schützenswerten Daten oder Persönlichkeitsprofilen (Art. 14 DSG).

28 Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (Entwurf), BBl 2017 7193, Sonderdruck; Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941, Sonderdruck.

29 Art. 4 lit. i E-DSG; Botschaft E-DSG (Fn. 28), 85.

se Anknüpfungspunkte für die Bestimmung der gerichtlichen und behördlichen Zuständigkeit wie auch des anwendbaren Datenschutzrahmens.

2.1.1. Internationale Zuständigkeit

[Rz 17] Eine internationale Zuständigkeit in der Schweiz dürfte regelmässig gegeben sein, wenn eine betroffene Person mit Wohnsitz oder gewöhnlichem Aufenthalt in der Schweiz gegenüber einem Datenbearbeiter eine Persönlichkeitsverletzung geltend macht. Persönlichkeitsverletzungen sind im Hinblick auf die Prüfung der gerichtlichen Zuständigkeit als unerlaubte Handlung zu qualifizieren. Wirkt sich die schädigende Handlung in der Schweiz aus, kann die gerichtliche Zuständigkeit an den Erfolgsort gemäss Art. 129 des Bundesgesetzes über das Internationale Privatrecht (IPRG; SR 291) bzw. Art. 5 Nr. 3 des Lugano-Übereinkommen (LugÜ)[30] angeknüpft werden.[31]

2.1.2. Anwendbares Recht

[Rz 18] Liegt eine internationale Zuständigkeit in der Schweiz vor, kann die betroffene Person zwischen mehreren Rechtsordnungen wählen (Art. 139 Abs. 1 i.V.m. Art. 139 Abs. 3 IPRG): Sie kann sich u.a. auf das Recht an ihrem eigenen Wohnsitz bzw. gewöhnlichen Aufenthalt wie auch am Erfolgsort berufen, sofern der Schädiger mit dem Erfolgseintritt in einem dieser Staaten rechnen musste. Da eine öffentliche Blockchain bezüglich des Wohnsitzes der Transaktionsteilnehmer agnostisch ist, muss jeder Bearbeiter von Personendaten damit rechnen, dass dadurch ein Teilnehmer in der Schweiz in seiner Persönlichkeit verletzt werden kann. Somit dürften die zivilrechtlichen Normen des schweizerischen Datenschutzrechts regelmässig Anwendung finden, selbst wenn die Datenbearbeitung nicht in der Schweiz stattfindet.

[Rz 19] Die Anwendung der öffentlich-rechtlichen Normen des Datenschutzgesetzes, allen voran die Prüfungszuständigkeit des EDÖB gemäss Art. 29 DSG, beurteilt sich demgegenüber nach dem Territorialitätsprinzip,[32] wobei die Erhebung von Personendaten oder der Eintritt einer Persönlichkeitsverletzung in der Schweiz als Anknüpfungspunkt selbst dann genügen, wenn die Daten ins Ausland übermittelt und überwiegend dort bearbeitet werden.[33]

[Rz 20] Der extraterritoriale Geltungsanspruch von Datenschutzvorschriften ist nichts Aussergewöhnliches. Die DSGVO will in bestimmten Fällen ebenfalls extraterritorial angewendet sein. Anders als das IPRG knüpft die DSGVO aber an die Niederlassung des Verantwortlichen oder Auftragsverarbeiters in der Union an (Art. 3 Abs. 1 DSGVO).[34] Sie findet jedoch auch auf Verantwortliche oder Auftragsverarbeiter ausserhalb der EU Anwendung, z.B. auf Personen mit Sitz in der Schweiz, sofern und soweit diese Personendaten bearbeiten im Zusammenhang mit (i)

---

30 Übereinkommen über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen abgeschlossen am 30. Oktober 2007, für die Schweiz in Kraft getreten am 1. Januar 2011 (Lugano-Übereinkommen, LugÜ; SR 0.275.12).

31 Lukas Bühlmann / Michael Reinle, Extraterritoriale Wirkung der DSGVO, in: digma 2017, 8–12, 12 Fn. 19; Nicolas Passadelis, in: Nicolas Passadelis / David Rosenthal / Hans-Peter Thür (Hrsg.), Datenschutzrecht, Basel 2015, Rn. 6.23.

32 Bühlmann / Reinle (Fn. 31), 12.

33 BGE 138 II 346, E. 3.2 m.w.H. – *Google Street View*.

34 Vgl. Bühlmann / Reinle (Fn. 31), 9.

gezielten Vertragsangeboten an Personen in der EU (Art. 3 Abs. 2 lit. a DSGVO) oder (ii) der Beobachtung des Verhaltens von Personen in der EU, insbesondere durch Online-Tracking (Art. 3 Abs. 2 lit. b DSGVO).

[Rz 21] Während also im schweizerischen Kollisionsrecht für die Anknüpfung an schweizerisches Recht die Lokalisierung der betroffenen Person den Ausschlag geben kann, stellt die DSGVO immer auf die Tätigkeit eines Verantwortlichen oder eines Auftragsverarbeiters ab. Um das anwendbare Recht bestimmen zu können, muss also nach der DSGVO im Rahmen einer Vorprüfung eruiert werden, wer der Verantwortliche bzw. Auftragsverarbeiter sein könnte.[35] Wie noch zu zeigen sein wird, ist dies bei der öffentlichen Blockchain ein schwieriges Unterfangen.

2.2. Personenbezug

2.2.1. Begriff der Personendaten

[Rz 22] Das Datenschutzgesetz greift immer dann, wenn Personendaten bearbeitet werden (Art. 2 DSG). Personendaten sind gemäss Art. 3 lit. a DSG alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Die Legaldefinition der personenbezogenen Daten in Art. 4 Nr. 1 DSGVO ist bis auf die verwendete Terminologie identisch, konkretisiert aber das Kriterium der Bestimmbarkeit. Eine Person ist demgemäss identifizierbar, wenn sie direkt oder indirekt mittels Zuordnung zu einem persönlichen Identifikationsmerkmal bestimmt werden kann.

2.2.2. Kriterien der Bestimmbarkeit

[Rz 23] Im Kontext der Blockchain steht regelmässig die Frage im Zentrum, ob sich die in der Datenbank hinterlegten verschlüsselten Daten auf eine *bestimmbare* Person beziehen. Bestimmbar ist eine Person dann, wenn aufgrund zusätzlicher Informationen auf deren Identität geschlossen werden kann. Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Vielmehr ist die Frage der Bestimmbarkeit nach einem objektiven und einem subjektiven Kriterium zu beantworten:[36]

- Aus *objektiver Sicht* ist der Aufwand zu berücksichtigen, den eine Identifizierung einer Person aus dem vorhandenen Datenschatz mit sich bringt. Ist der Aufwand dafür derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor.[37]
- In *subjektiver Hinsicht* ist relevant, welches Interesse der Datenbearbeiter selbst oder ein Empfänger der Daten an der Identifizierung hat.[38]

---

35 So auch Böhme / Pesch (Fn. 3), 478.

36 BGE 136 II 508, E. 3.2 – *Logistep*; ähnlich der Urteil des EuGH vom 19. Oktober 2016 C-582/14 *Patrick Breyer ./. Bundesrepublik Deutschland*, E. 45 ff.; vgl. auch Philippe Meier / Nicolas Tschumy, L'adresse IP : une donnée personnelle ? Ou quand la CJUE rejoint le TF !, in: Jusletter 23. Januar 2017, Rz. 12 ff.; im Unionsrecht ist allerdings umstritten, ob dem beschriebenen relativen Ansatz zu folgen ist oder nicht vielmehr ein absoluter Personenbezug für die Identifizierbarkeit bereits genügt: Manuel Klar / Jürgen Kühling, in: Jürgen Kühling / Benedikt Buchner (Hrsg.), DS-GVO Kommentar, München 2017, Art. 4 Nr. 1, N 25.

37 Botschaft DSG, BBl 1988 II 443, 444 f., Ziff. 221.1.; vgl. auch Botschaft E-DSG (Fn. 28), 81.

38 Rudin (Fn. 6), Art. 3, N 11.

[Rz 24] Die Bestimmbarkeit einer Person hängt m.a.W. von den konkreten Umständen ab, wobei die Möglichkeiten und Interessen sämtlicher Bearbeiter im Datenerhebungs- und Verarbeitungsprozess zu berücksichtigen sind. Stellt für einen bestimmten Datenbearbeiter in der Verarbeitungskette eine Information ein Personendatum dar, gilt diese Qualifikation grundsätzlich auch für die ihm vorgelagerten Datenbearbeiter.[39]

[Rz 25] Bei diesem Punkt kommt der Praxis zur Qualifikation von dynamischen IP-Adressen entscheidende Bedeutung zu, denn die Ausgangslage ist vergleichbar.[40] Demnach sind dynamische IP-Adressen für Webseiten-Betreiber dann als Personendaten zu qualifizieren, wenn im konkreten Fall eine tatsächliche oder rechtliche Zugriffsmöglichkeit auf die damit verbundenen Zusatzinformationen besteht, welche eine Identifizierung des Anschlussinhabers ermöglichen, wobei die Schwelle nach der Gerichtspraxis sehr tief angesetzt wird.[41] Auf der Blockchain fehlt bei den hinterlegten alphanumerischen Codes auf den ersten Blick jeder Personenbezug. Für die meisten Akteure bleiben die auf der Blockchain sichtbaren pseudonymen Profile daher Sachdaten.[42] Sobald jedoch ein Interesse an der Herstellung eines Personenbezugs besteht, ist der Verknüpfungsaufwand je nach Informationslage nicht besonders gross.[43]

2.2.3. Singularisierung

[Rz 26] Im Sog der DSGVO geht die Diskussion sogar noch einen Schritt weiter. Man fragt sich, ob zumindest im Online-Bereich auch Angaben als personenbezogen gelten, die sich auf eine von allen anderen Personen unterscheidbare, aber nicht namentlich bekannte Person beziehen («Singularisierung» statt «Identifizierung»).[44] Die Legaldefinition in Art. 4 Nr. 1 DSGVO könnte in diesem Sinne interpretiert werden, denn laut Erwägungsgrund 26 soll bereits das «Aussondern» ein Mittel sein, um eine Person wenigstens indirekt identifizieren zu können. Nach der vorliegenden Auffassung ist die Singularisierung indessen nur ein Indiz für den Personenbezug, ersetzt diesen aber nicht. Infolgedessen sollten Angaben wie eine Bitcoin-Adresse nicht als personenbezogen gelten, soweit der Personenbezug nicht durch Verknüpfung mit weiteren Angaben hergestellt werden kann. Andernfalls wären sämtliche verschlüsselten Identifikatoren, die auf einer öffentlichen Blockchain hinterlegt und einer Person zugeordnet sind, *per se* als Personendaten zu qualifizieren. Dies würde zu einem exorbitanten Geltungsanspruch des Datenschutzes führen, der in keinem vernünftigen Verhältnis mehr zu dessen Hauptzweck, dem Schutz der informationellen Selbstbestimmung, stehen würde.

---

39 BGE 136 II 508, E. 3.5 – *Logistep*; ähnlich Klar/Kühling (Fn. 36), Art. 4 Nr. 1, N 24; vgl. auch DSGVO, Erwägungsgrund 26: «*Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind*».

40 Vgl. auch Fasching (Fn. 2), 18.

41 Barbara Widmer, Bei IP-Adressen kommt es darauf an…, in: digma 2017, 76–77, 77, mit Hinweisen auf BGE 136 II 508, – *Logistep* und Urteil des EuGH vom 19. Oktober 2016 C-582/14 *Patrick Breyer ./. Bundesrepublik Deutschland*.

42 Vgl. auch Kaulartz (Fn. 1), 479 f. («*selbst generierte Pseudonyme*»).

43 Vgl. Gervais (Fn. 8), 129.

44 Hierzu eingehend David Rosenthal, Zauberwort Singularisierung: Personendaten ohne Identifizierbarkeit? in: digma 4/2017 (noch nicht publiziert).

[Rz 27] Die Gesetzgebungsmaschine in der EU ist freilich auf dem Weg, die vermeintliche Schutzlücke zu schliessen: Der Vorschlag der EU-Kommission für eine ePrivacy-Verordnung,[45] welche die ePrivacy-Richtlinie[46] ersetzen soll, ist auf dem Tisch. Die ePrivacy-RL (Richtlinie 2002/58/EG) ist am 31. Juli 2002 in Kraft getreten und verpflichtet die Mitgliedstaaten, spezifische Regelungen zum Datenschutz in der Telekommunikation zu erlassen, z.B. über das Mithören von Telefongesprächen und das Abfangen von E-Mails. 2009 wurde die ePrivacy-RL sodann durch die Richtlinie 2009/136/EG[47] ergänzt (Cookie-Richtlinie), die für das Setzen von Cookies[48] eine ausdrückliche Einwilligung verlangt. Die ePrivacy-Verordnung will die Regulierungsschraube weiter anziehen und insbesondere die gesamte elektronische Kommunikation, einschliesslich der Datenübermittlung von Maschine zu Maschine (sog. Internet der Dinge), dem Grundsatz der Vertraulichkeit unterstellen.[49] Eine Personenbeziehbarkeit ist nicht erforderlich. Die ePrivacy-Verordnung würde somit auf vollkommener Transparenz basierende automatisierte Abwicklungssysteme vor erhebliche Probleme stellen, wenn nicht gar verunmöglichen.

2.3. Rollenverteilung

2.3.1. Begriff des Bearbeitens

[Rz 28] Das zweite Aufgreifkriterium des Datenschutzrechts – nebst dem Vorliegen von Personendaten – ist deren Bearbeitung. Damit ist jeder Umgang mit Personendaten gemeint, und zwar unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten, ja selbst das Anonymisieren von Personendaten (vgl. Art. 3 lit. e DSG). Die DSGVO beschreibt unter dem Begriff des «Verarbeitens» denselben Vorgang (Art. 4 Nr. 2 DSGVO).

[Rz 29] Dass auf der Blockchain Daten bearbeitet werden, dürfte unbestritten sein. Die Blockchain wird laufend fortgeschrieben; kommt ein neuer Knoten dazu, werden die Datenblöcke dupliziert und erneut abgelegt. Dabei kommen der Initiator einer Transaktion (soweit er nicht in seiner Eigenschaft als betroffene Person eigene Daten in das System einspeist),[50] der mögliche Empfänger und die am Konsensmechanismus beteiligten Personen als Bearbeiter in Frage.

---

45 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 10 final.

46 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

47 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

48 Ein Cookie ist eine Textdatei auf einem Computer. Sie enthält typischerweise Daten über besuchte Webseiten, die der Webbrowser beim Surfen im Internet speichert; vgl. EDÖB, Erläuterungen zu Webtracking, Dezember 2014, abrufbar unter https://www.edoeb.admin.ch/datenschutz/00683/01103/01104/index.html?lang=de.

49 Erwägungsgrund 12 des Entwurfs der ePrivacy-Verordnung. Art. 5 des Entwurfs lautet: «*Elektronische Kommunikationsdaten sind vertraulich. Eingriffe in elektronische Kommunikationsdaten wie Mithören, Abhören, Speichern, Beobachten, Scannen oder andere Arten des Abfangens oder Überwachens oder Verarbeitens elektronischer Kommunikationsdaten durch andere Personen als die Endnutzer sind untersagt, sofern sie nicht durch diese Verordnung erlaubt werden*».

50 Böhme / Pesch (Fn. 3), 478.

2.3.2. Zuordnung der Verantwortung für die Datenbearbeitung

[Rz 30] Nach schweizerischem Datenschutzrecht sind die Adressaten des datenschutzrechtlichen Pflichtenprogramms damit identifiziert: Jeder Bearbeiter hat sich an die Bearbeitungsgrundsätze gemäss Art. 4 DSG zu halten, sich über die Richtigkeit der Personendaten zu vergewissern (Art. 5 DSG) und für eine ausreichende Datensicherheit zu sorgen (Art. 7 DSG). Eine Bündelung dieser Pflichten bei einer einzigen oder mehreren verantwortlichen Stellen sah der schweizerische Gesetzgeber nicht vor.[51] Alle, die an der Blockchain teilnehmen, sind damit Bearbeiter im Sinne des Datenschutzgesetzes.

[Rz 31] Anders die DSGVO: Diese nimmt nicht jeden «Verarbeiter» in die Pflicht, sondern bezeichnet vier Hauptakteure mit je eigenem Schutz- bzw. Verantwortungsspektrum: 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). Diesem Quartett liegt die Vorstellung zugrunde, dass Datenbearbeitungen immer in einer hierarchischen Ordnung stattfinden.[52] Der Verantwortliche legt fest, zu welchen Zwecken und mit welchen Mitteln Personendaten bearbeitet werden sollen. Er bearbeitet die Daten entweder selbst oder delegiert diese Aufgabe an Auftragsverarbeiter. *Tertium non datur*. Dies zeigt sich darin, dass sämtliche Pflichten der DSGVO entweder an den Verantwortlichen alleine oder den Auftragsverarbeiter gerichtet sind, nie jedoch an einen «Verarbeiter».[53]

[Rz 32] Zwar rechnet auch die DSGVO in Art. 26 mit der Möglichkeit, dass mehrere Personen gemeinsam für die Verarbeitung verantwortlich sind, doch zielt die Regelung auf Situationen ab, in denen sich verschiedene Verarbeiter in kollektiver Abstimmung für die Zwecke einer gemeinsamen Datenverarbeitung organisieren. Die Regelung will die Akteure komplexer Ökosysteme, in denen mehrere Personen in intransparenter Weise zusammenwirken, in das Schema der organisierten und kontrollierten Verantwortung mit klar definierten Kompetenzen einordnen.[54] Dieser Regulierungsansatz versagt bei der öffentlichen Blockchain von Vornherein.[55] Sie basiert auf dem Prinzip der *Trustlessness* und verkörpert das Gegenteil dessen, was dem EU-Gesetzgeber vorschwebt.

2.3.3. Versagen des datenschutzrechtlichen Rollenkonzepts der DSGVO

[Rz 33] Weil nicht sein kann, was nicht sein darf, wird in der Literatur allenthalben verzweifelt nach einem Verantwortlichen i.S.v. Art. 4 Nr. 7 DSGVO für die Datenbearbeitung auf der Blockchain gesucht. Das Spektrum der Ideen ist breit, überzeugt aber nicht:

---

51 David Rosenthal, in: David Rosenthal / Yvonne Jöhri (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 3 Bst. j DSG, N 116.

52 Vgl. Erwägungsgrund 79 der DSGVO: «*Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter bedarf es auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden einer klaren Zuteilung der Verantwortlichkeiten durch diese Verordnung [...]*».

53 Vgl. nur Art. 5 Abs. 2 DSGVO, wonach für die Einhaltung der Datenbearbeitungsgrundsätze gemäss Art. 5 Abs. 1 der Verantwortliche verantwortlich und nachweispflichtig ist.

54 Vgl. Jürgen Hartung, in: Jürgen Kühling / Benedikt Buchner (Hrsg.), DS-GVO Kommentar, München 2017, Art. 26, N 10.

55 Vgl. Böhme / Pesch (Fn. 3), 479.

- Fasching ordnet die Rolle der Verantwortlichen bei der Bitcoin-Blockchain der Gruppe von Entwicklern zu, die laufend Änderungen testen und implementieren.[56] Dieser Ansatz lässt sich allerdings nicht mit dem Regelungskonzept der DSGVO (wie auch des DSG) vereinbaren. Der sachliche Anwendungsbereich der DSGVO ist auf Datenverarbeitungen beschränkt. Die DSGVO kann somit Personen, die keine Personendaten verarbeiten, nicht in die Pflicht nehmen. Hersteller von Systemen sind keine Datenverarbeiter,[57] sie werden in Erwägungsgrund 78 der DSGVO einzig (unverbindlich) aufgerufen, ihre Produkte datenschutzfreundlich auszugestalten. Die Zertifizierung von Produkten nach Art. 40 ff. DSGVO bietet dazu immerhin ein – wenn auch kaum genutztes – Mittel. Die Entwickler einer Blockchain betreiben das System nicht, sie beteiligen sich auch nicht mit einer Kontrollmehrheit am Konsensmechanismus und haben daher keine Möglichkeit, Zwecke und Mittel der Datenverarbeitungen auf einer öffentlichen Blockchain festzulegen.
- Ein anderer Ansatz will die am Konsensmechanismus Beteiligten (*bitcoin miners*) als Verantwortliche qualifizieren,[58] was bei *permissioned blockchains* ein gangbarer Weg ist,[59] bei öffentlichen Blockchains hingegen nicht nur an der faktischen Durchsetzbarkeit scheitern wird, sondern auch konzeptionell verfehlt ist, weil ein einzelner Knoten im dezentralen Netzwerk gar nicht die technischen Mittel zur Verfügung hat, um die datenschutzrechtlichen Vorgaben gegenüber den weiteren Netzwerkteilnehmern zu erfüllen.[60]
- Schliesslich hat sich offenbar auch die ungarische Datenschutzaufsichtsbehörde zur Anwendbarkeit der DSGVO auf die Blockchain geäussert und qualifiziert dabei jeden teilnehmenden Datenempfänger als Verantwortlichen.[61] Diese Ansicht zieht den Kreis der Verantwortlichen noch weiter als die vorangehende Theorie und ist daher mit gleicher Begründung abzulehnen.

[Rz 34] Die öffentliche Blockchain ist ein verteiltes Register ohne zentrale Kontrollinstanzen. Dies ist durchaus ernst gemeint. Daher ist es auch müssig, nach einem Verantwortlichen zu suchen; es gibt ihn nicht. Die öffentliche Blockchain ist nach dem Regelungskonzept der DSGVO datenschutzrechtliches Niemandsland, ein datenschutzfreier Raum.[62]

[Rz 35] Diese pauschale These ist insoweit zu relativieren, als sie nur für das System der Blockchain an sich gilt. Sobald Daten aus der Blockchain herausfiltriert und in eigenen Systemen weiterbearbeitet werden, z.B. durch Wallet-Provider, können die datenschutzrechtlichen Rollen wieder zugeordnet werden. Weiter unterstreicht die These auch die Wichtigkeit eines Systemdatenschutzes (Privacy by Design und Privacy by Default), der in Art. 25 DSGVO verankert ist. Gerade

56 Fasching (Fn. 2), 20.

57 Jürgen Hartung, in: Jürgen Kühling / Benedikt Buchner (Hrsg.), DS-GVO Kommentar, München 2017, Art. 24, N 12 a.E.

58 Jacek Czarnecki, Blockchains and Personal Data Protection Regulations Explained, in: Coindesk, 26. April 2017, abrufbar unter https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained/.

59 Böhme / Pesch (Fn. 3), 479, Fn. 44; demgegenüber will Fasching, (Fn. 2), 20, die am Konsensmechanismus Beteiligten als Auftragsverarbeiter qualifizieren.

60 Vgl. Böhme / Pesch (Fn. 3), 478 f.

61 Dóra Petrányi / Marton Domokos, Hungary: Data Protection Aspects of Blockchain, 17. August 2017, http://www.cms-lawnow.com/ealerts/2017/08/hungary-data-protection-aspects-of-blockchain; ähnlich auch Carmen Tang, EU Regime: When Blockchain meets GDPR, in: Asian Legal Business, 1. November 2017, abrufbar unter http://www.legalbusinessonline.com/news/sponsored-eu-regime-when-blockchain-meets-gdpr/75053.

62 Im Ergebnis wohl ebenso Böhme / Pesch (Fn. 3), 479.

weil im Kontext der öffentlichen Blockchain der Datenschutz auf der Bearbeitungsebene versagt, liegt in systemimmanenten Datenschutzlösungen viel Potenzial.[63]

3. Bearbeitungsgrundsätze

[Rz 36] Das schweizerische Datenschutzrecht kennt – im Gegensatz zum europäischen Pendant[64] – kein Bearbeitungsverbot mit Erlaubnisvorbehalt, solange die Bearbeitung rechtmässig und in Übereinstimmung mit den Datenbearbeitungsgrundsätzen von Art. 4, 5 und 7 DSG erfolgt (vgl. Art. 12 Abs. 2 lit. a DSG).[65] Der Entwurf des zu revidierenden Datenschutzgesetzes[66] ändert an dieser Grundkonzeption nichts.[67]Weiter ist bei grenzüberschreitender Datenbekanntgabe, die auf der Blockchain systemimmanent ist, ein Datenexport in Länder ohne angemessenes Datenschutzniveau untersagt (Art. 6 Abs. 1 DSG), wenn keine hinreichenden vertraglichen Garantien vorliegen oder die betroffene Person im Einzelfall eingewilligt hat (Art. 6 Abs. 2 lit. a und b DSG). Nach schweizerischer Rechtsauffassung hat jeder Bearbeiter von Personendaten innerhalb der Blockchain die genannten Grundsätze zu beherzigen. Verstösst er dagegen, liegt eine Persönlichkeitsverletzung vor (Art. 12 Abs. 2 lit. a DSG). Die Datenbearbeitung ist in diesem Fall nur rechtmässig, wenn ein Rechtfertigungsgrund vorliegt, z.B. die Einwilligung der betroffenen Person (Art. 13 Abs. 1 DSG).

[Rz 37] Es liegt auf der Hand, dass Datenbearbeitungen auf der Blockchain in mancher Hinsicht mit den genannten Datenbearbeitungsgrundsätzen inkompatibel sind. Die betroffene Person hat auf die Erweiterung des Netzwerks und dessen geografische Verbreitung keinerlei Einfluss, sie kann nicht verhindern, dass bestimmte Personen Einblick in ihre Daten erhalten. Auf der anderen Seite darf von jeder Person, die ihre Daten der Blockchain anvertraut, erwartet werden, dass sie sich der wesentlichen Eigenschaften der Blockchain bewusst ist. In diesem Zusammenhang kommt Art. 13. Abs. 3 DSG erhebliche Bedeutung zu. Die Bestimmung besagt, dass in der Regel keine Persönlichkeitsverletzung vorliegt, wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. In der DSGVO fehlt eine die Eigenverantwortung des Datensubjekts betonende äquivalente Bestimmung. Art. 9 Abs. 2 Bst. e DSGVO hält einzig fest, dass die enge Zweckbindung für besonders sensible Daten gemäss Art. 9

---

63 Vgl. hierzu die Beispiele bei Böhme / Pesch (Fn. 3), 479 sowie Stephan Wiefling / Luigi La Iacono / Frederik Sandbrink, Anwendung der Blockchain ausserhalb von Geldwährungen, in: Datenschutz und Datensicherheit 2017, 482–486, 483 f.

64 Vgl. Art. 6 Abs. 1 und 9 Abs. 1 DSGVO.

65 Es sind dies u.a.:

– *Grundsatz der Transparenz:* Die Beschaffung der Personendaten und insbesondere der Zweck ihrer Bearbeitung muss für die betroffene Person erkennbar sein (Art. 4 Abs. 4 DSG);

– *Grundsatz der Zweckbindung:* Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG);

– *Grundsatz der Verhältnismässigkeit:* Die Bearbeitung der Personendaten muss verhältnismässig sein, d.h. darf nicht weiter gehen, als es der Zweck der Bearbeitung erforderlich macht (Art. 4 Abs. 2 DSG);

– *Grundsatz der Datenintegrität:* Der Bearbeiter hat sich über die Richtigkeit der Personendaten zu vergewissern und unvollständige oder unrichtige Personendaten zu vernichten (Art. 5 Abs. 1 DSG);

– *Grundsatz der Datensicherheit:* Personendaten sind durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten zu schützen (Art. 7 Abs. 1 DSG).

66 Fn. 28.

67 Vgl. Art. 5 Abs. 6, Art. 13 und Art. 26 E-DSG.

Abs. 1 DSGVO nicht gilt, wenn die betroffene Person die Daten offensichtlich öffentlich gemacht hat. Die allgemeinen Schutzvorschriften nach Art. 6 DSGVO bleiben aber weiterhin wirksam.[68]

[Rz 38] Art. 13 Abs. 3 DSG ist zwar kein Freipass für jede erdenkliche Bearbeitung freiwillig publik gemachter Personendaten, er genügt jedoch, um deren perpetuierte Transparenz, Mobilität und Persistenz innerhalb der Blockchain zu rechtfertigen. Datenschutzrechtlich unzulässig kann aber eine weitergehende systematische Erhebung und Bearbeitung von Daten aus der Blockchain und deren Verknüpfung mit zusätzlichen Informationen durch Dritte sein, denn eine solche Tätigkeit ist für die betroffene Person weder erkennbar noch durch den ursprünglichen Zweck gedeckt, die Daten für die Teilnahme am Blockchain-System zugänglich zu machen.[69]

4. Betroffenenrechte

4.1. Übersicht

[Rz 39] Die Ausübung der Rechte der betroffenen Personen ist im Blockchain-Umfeld noch schwieriger zu bewältigen als die Einhaltung der Bearbeitungsgrundsätze. Die wichtigsten Betroffenenrechte sind das Auskunfts-, Berichtigungs-, Widerrufs- und Löschungsrecht.[70] Inskünftig werden auch die Rechte, bei automatisierten Einzelfallentscheidungen eine Überprüfung durch eine natürliche Person zu verlangen,[71] und das Recht auf Datenportabilität[72] zu beachten sein.

[Rz 40] Im Rahmen der DSGVO wird die Rechtsausübung regelmässig an der Abwesenheit eines Verantwortlichen scheitern. Auch im schweizerischen Recht richten sich die Rechtsbehelfe mitunter einzig gegen den Inhaber der Datensammlung, so namentlich das Auskunftsrecht (Art. 8 Abs. 1 DSG). Innerhalb des Blockchain-Netzwerks ist das Auskunftsrecht somit mangels Passivlegitimation der dezentral und autonom agierenden Bearbeiter nicht durchsetzbar. Bei den anderen Rechten, die alle auf eine Korrektur oder Entfernung der Einträge auf der Blockchain abzielen, ist die Durchsetzung systembedingt nicht möglich.[73] Der in Anspruch genommene Bearbeiter hat gar nicht die Möglichkeit, die Blockchain zu manipulieren. In dieser Integritätssicherung liegt die Stärke, gleichzeitig aber auch die augenfälligste offene Datenschutzflanke der Blockchain.

4.2. Überprüfungsrecht bei automatisierter Einzelfallentscheidung

[Rz 41] Besondere Brisanz kommt der obigen Schlussfolgerung bei denjenigen Betroffenenrechten zu, die gerade deshalb geschaffen wurden, um die Abhängigkeit der Datensubjekte von digitalen Technologien und den durch Algorithmen getroffenen Entscheidungen zu mildern. Paradebeispiel für ein solches Recht ist das partielle Verbot der sog. automatisierten Einzelfallentscheidung

---

68 Thilo Weichert, in: Jürgen Kühling / Benedikt Buchner (Hrsg.), DS-GVO Kommentar, München 2017, Art. 9, N 77.

69 Corrado Rampini, in: Urs Maurer-Lambrou / Gabor Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, 3. Aufl., Basel 2014, Art. 13 DSG, N 18; vgl. auch für das deutsche Recht auch Böhme / Pesch (Fn. 3), 479.

70 Art. 5 Abs. 2, Art. 8, Art. 12 Abs. 2 lit. b und Art. 15 Abs. 1 DSG; Art. 7 Abs. 3, Art. 15–17 und Art. 21 DSGVO.

71 Art. 19 Abs. 2 E-DSG; Art. 22 DSGVO.

72 Art. 20 DSGVO; der E-DSG sieht ein Recht auf Datenportabilität nicht vor.

73 Fasching (Fn. 2), 20.

(Art. 22 DSGVO). Auf der Blockchain abgewickelte *Smart Contracts* produzieren beispielsweise laufend ohne menschliche Unterstützung automatisierte Rechtsfolgen.[74] Gemäss Art. 22 DSGVO hat die betroffene Person nun aber das Recht, keiner ausschliesslich auf automatisierter Verarbeitung beruhenden Entscheidung unterworfen zu werden, sofern diese ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Zwar ist eine solche automatisierte Entscheidung zulässig, wenn sie für den Abschluss oder die Erfüllung eines Vertrages erforderlich ist (Art. 22 Abs. 2 Bst. a und c DSGVO) oder mit ausdrücklicher Einwilligung der betroffenen Person erfolgt, aber nur dann, wenn der Verantwortliche der betroffenen Person das Recht einräumt, die Überprüfung der Entscheidung durch eine Person zu erwirken (Art. 22 Abs. 3 DSGVO).

[Rz 42] Dieses Konzept der menschlichen Einwirkung auf einen vordefinierten Algorithmus läuft der Grundidee des selbstausführenden und selbstdurchsetzenden *Smart Contracts* zuwider, indem eben bei einem Protest der betroffenen Person nicht vollständig auf den Code abgestellt werden darf, sondern die Zweitmeinung eines echten Menschen eingeholt werden muss. Stehen sich in einem *Smart Contract* zwei einander bekannte Parteien gegenüber, kann dieses Recht auf menschliches Eingreifen eine Überprüfung von automatisierten Transaktionen dennoch ermöglichen. Der Verantwortliche definiert sich dann allerdings nicht über seine Rolle als Teilnehmer auf der Blockchain, sondern auf Grund seiner Parteistellung im bilateralen Vertragsverhältnis zur betroffenen Person.

[Rz 43] Dies lässt sich anhand eines Beispiels illustrieren. Ein Ferienresort bietet seinen Gästen einen Gutschein für einen Drink an der Poolbar an, wenn diese auf einer hauseigenen Bewertungs-App ihre Laune mehr als dreimal täglich als schlecht einstufen. Die Ausstellung des Gutscheins wird in einem *Smart Contract* einprogrammiert. Verweigert der *Smart Contract* den Gutschein, kann der Gast zwar nichts gegen die Dokumentierung des Vertrages und der ausgebliebenen Transaktion auf der Blockchain unternehmen. Er kann aber dennoch vom Hotel eine Überprüfung der automatisierten Entscheidung durch eine Person verlangen. Dieses datenschutzrechtlich verankerte Überprüfungsrecht birgt also durchaus das Potential, die Ausbreitung und Wirkungsweise von *Smart Contracts* je nach Sichtweise entweder zu bremsen oder in geordnete Bahnen zu lenken. Jedenfalls bleibt es nicht ohne korrigierende Wirkung auf zwei Haupteigenschaften der Blockchain, nämlich die Unabänderbarkeit und vermutete Richtigkeit der auf ihr dokumentierten Informationen.

[Rz 44] Das Überprüfungsrecht scheitert allerdings dann wieder an der Abwesenheit eines Verantwortlichen,[75] wenn die betroffene Person an einem autonomen *Smart Contract* partizipiert, der auf der Blockchain abläuft, ohne dass sich eine Gegenpartei konstituiert. Hierbei kann es sich bspw. um ein *Smart Casino* handeln.[76] Bei derartigen Konstrukten hat man sich damit abzufinden, dass keine Vertragspartei haftbar gemacht werden kann.[77] Die Abwesenheit einer verantwortlichen Gegenpartei ist auch der Grund dafür, dass es an einer datenschutzrechtlichen Anlaufstelle fehlt, um das Recht auf Überprüfung der automatisierten Entscheidung geltend zu machen.

---

74 Vgl. Eggen (Fn. 23), 6; Stephan D. Meyer / Benedikt Schuppli, «Smart Contracts» und deren Einordnung in das schweizerische Vertragsrecht, in: recht 2017, 204–224, 207 f.

75 Dies gilt sowohl nach Art. 22 DSGVO wie auch Art. 19 E-DSG.

76 Vgl. dazu Andreas Glarner/Stephan D. Meyer, Smart Contracts in Escrow-Verhältnissen, in: Jusletter 4. Dezember 2017, Ziff. III.3.a.

77 Ein Vertragsverhältnis besteht weder zu den Entwicklern der Blockchain noch zu den am Konsensmechanismus beteiligten *Miners*, *v*gl. Meyer / Schuppli (Fn. 74), 212 ff.

4.3. Recht auf Datenportabilität

[Rz 45] Vollkommen unwirksam dürfte demgegenüber das Recht auf Datenübertragbarkeit sein (Art. 20 DSGVO). Dieses räumt einer betroffenen Person das Recht ein, dass der Verantwortliche die ihm überlassenen Personendaten in einem strukturierten, gängigen und maschinenlesbaren Format herausgeben muss, sofern die Verarbeitung auf der Basis einer Einwilligung oder der Abwicklung eines Vertrages und mithilfe automatisierter Verfahren erfolgt. Hauptbeispiel sind Daten, die auf einer Social Media-Plattform gespeichert sind. Die Blockchain kann nicht mit einer derartigen Konstellation verglichen werden; es fehlt nicht nur an einem Verantwortlichen, sondern – wie bereits mehrfach angedeutet – auch an einer Einwilligung bzw. einem Vertragsverhältnis der betroffenen Person mit der Vielzahl der Datenbearbeiter, die den Betrieb einer öffentlichen Blockchain aufrechterhalten. Ausserhalb des Blockchain-Universums kann das Recht auf Datenübertragbarkeit aber sehr wohl greifen, bspw. gegenüber einem Wallet-Provider.

5. Fazit

[Rz 46] Die Berührungspunkte zwischen der Blockchain und dem Datenschutz sind mannigfach. Obwohl die auf einer öffentlichen Blockchain abgelegten Daten in der Regel verschlüsselt sind, können dennoch Personendaten anfallen, da mittels Verknüpfung weiterer Informationen eine Zuordnung zu einer natürlichen Person möglich wird. Ist dies der Fall, vertragen sich die Transparenz und die Unabänderbarkeit der auf der Blockchain dokumentierten Informationen schlecht mit den Grundprinzipien des Datenschutzes.

[Rz 47] Die dezentrale Architektur der öffentlichen Blockchain schlägt dem Datenschutz allerdings in mancherlei Hinsicht ein Schnippchen. Die wichtigste Erkenntnis aus der vorstehenden Analyse ist, dass sich bei einer auf unzählige Knoten verteilten Datenbank keine für die Datenbearbeitung verantwortliche Person finden lässt. Damit zielt zumindest unter dem Regime der DSGVO, die von der Prämisse einer hierarchisch organisierten Datenverarbeitungsstruktur ausgeht, jeder datenschutzrechtliche Rechtsbehelf ins Leere. Das schweizerische Recht ist demgegenüber weniger zentralistisch konzipiert und nimmt – von wenigen Ausnahmen abgesehen – jeden Datenbearbeiter in die Pflicht. Es betont aber auch die Eigenverantwortung der betroffenen Person, indem die Bearbeitung öffentlich zugänglich gemachter Daten grundsätzlich gerechtfertigt ist. Die Beteiligung an einem Blockchain-System dürfte somit bis zu einem gewissen Grad einer Aufgabe der informationellen Selbstbestimmung über die freiwillig in das System eingegebenen Daten gleichkommen.

[Rz 48] Bei aller Kritik und allen Zweifeln darf jedoch nicht ausser Acht gelassen werden, dass die Blockchain gerade im Bereich des Datenschutzes Stärken aufweist, welche die Technologie zu einem vielgenutzten Werkzeug zur Verbesserung des Datenschutzes machen könnten. Dabei geht es nicht nur um die Sicherstellung der Datenintegrität aufgrund der durch die verteilte Struktur bewirkten Reduktion des Risikos, das in der Abhängigkeit von Einzelkomponenten («*single point of failure*») liegt.[78] In Zukunft könnte die Blockchain-Technologie beispielsweise eine technische Kontrolle des Zugriffs auf und der Weiterbearbeitung von Personendaten durch Dritte ermöglichen. Jede betroffene Person hätte einen privaten Schlüssel, um Dritten Zugang zu ihren Daten

78 Vgl. Böhme / Pesch (Fn. 3), 473.

zu gewähren und einen bestimmten Bearbeitungsumfang freizugeben. Ausserhalb dieser autorisierten Zone wäre eine Datenbearbeitung technisch nicht möglich. Die Daten selbst würden nicht auf dem öffentlichen Blockchain-Register selbst, sondern in einem separaten Raum gespeichert. Auf der Blockchain wäre einzig sichtbar, zu welcher Adresse Daten vorhanden sind.[79] Dieses Beispiel zeigt, dass mit technischen Lösungen (Privacy by Design) transparenzbedingte Nachteile öffentlicher Blockchains gemildert werden können.

Dr. Michael Isler, Rechtsanwalt, Walder Wyss AG, Zürich.

79 Vgl. zum Ganzen Stephan Wiefling / Luigi Lo Iacono / Frederik Sandbrink, Anwendung der Blockchain ausserhalb von Geldwährungen, in: Datenschutz und Datensicherheit 2017, 482–486, 483.