Zeitschrift für Informationsrecht 7, 382–393 (2019)
https://doi.org/10.33196/ziir201904038201
ZIIR 2019, 382

AUFSÄTZE

Die Blockchain-Technologie im Lichte der DSGVO

Die unmittelbare Anwendbarkeit der 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 („DSGVO") in allen Mitgliedstaaten der EU seit 25. Mai 2018, hat im Zusammenhang mit der Blockchain-Technologie maßgebliche, grundsätzliche Fragen aufgeworfen. Das enorme Innovationspotenzial und die unzähligen Anwendungsbereiche der Blockchain gebieten es freilich, die Kompatibilität und das allfällige Spannungsverhältnis zwischen DSGVO und der Blockchain-Technologie neu zu beurteilen. Aus diesem Grund ist es entscheidend, sich schon bei der Entwicklung einer neuen Technologie und der Anwendbarkeit für Use Cases in der Praxis mit der datenschutzrechtlichen Vereinbarkeit zu beschäftigen (Stichwort: privacy by design). Dieser Artikel untersucht die Anwendbarkeit der DSGVO auf die Blockchain-Technologie, konkretisiert die datenschutzrechtlichen Akteure und analysiert Schwierigkeiten, Inkompatibilitäten und deren Auswirkungen auf die gegenwärtige Praxis.[1]

Deskriptoren: Blockchain; personenbezogene Daten; räumlicher/sachlicher Anwendungsbereich; Recht auf Löschung; Bitcoin-Transaktion.
Normen: Art 2 DSGVO; Art 4–7 DSGVO; Art 16, 17 DSGVO; Art 26 DSGVO.

Von Arthur Stadler und Jaqueline Bichler

I. Die Blockchain-Technologie: Neue Herausforderungen für den Datenschutz

Der Grundanwendungsfall der Blockchain-Technologie (etwa in Bezug auf die Kryptowährung Bitcoin) zeichnet sich durch eine dezentrale und gleichzeitig unveränderliche Datenspeicherung aus.[2] Einer der Hauptvorteile ist die Eliminierung von Intermediären, was jedoch die Beantwortung der Frage der datenschutzrechtlichen Verantwortlichkeit nicht ersetzt, sondern erschwert. Ein weiteres Charakteristikum ist, dass jeder Teilnehmer einer Blockchain Einsicht in die gespeicherten Daten nehmen kann, wodurch „*die uneingeschränkte Richtigkeit und unmittelbare Überprüfbarkeit der Daten durch jeden Teilnehmer sichergestellt werden*"[3] kann. Auf den ersten Blick scheint es daher so, als sei der Einsatz der Blockchain-Technologie zur Speicherung personenbezogener Daten grundsätzlich mit der DSGVO unvereinbar. Datenschutzrechtliche Vorgaben sind für die Blockchain-Technologie allerdings erst dann (umso mehr!) relevant, wenn auf der Blockchain personenbezogene Daten verarbeitet bzw gespeichert werden.

II. Fällt die Blockchain-Technologie in den Anwendungsbereich der DSGVO?

Vom sachlichen Anwendungsbereich der DSGVO sind gemäß Artikel 2 Abs 1 DSGVO die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht-automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, umfasst. Keine Anwendung findet die Verordnung allerdings auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (Artikel 2 Abs 2 lit c DSGVO). Somit ist bereits an dieser Stelle vorwegzunehmen, dass die DSGVO hinsichtlich rein privater Zwecke nicht anwendbar ist. Während die französische Datenschutzbehörde CNIL (Commission Nationale de l'Informatique et des Libertés) bspw die Anwendbarkeit der DSGVO für private Bitcoin-Transaktionen ausschließt[4], ist dies uE diffe-

1 Großer Dank gebührt RAA Mag. Tamino Chochola für ausgiebige juristische Diskussionen und Anregungen zu diesem Thema.
2 Vgl *Knoll*, ZIIR 2016, 406 (407).
3 *Gorzala/Hanzl*, RdW 2018, 485 (486).
4 *CNIL*, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data (Stand 6.11.2018).

renzierter zu betrachten. Denn sofern eine natürliche Person zur Ausübung **ausschließlich** persönlicher oder familiärer Tätigkeiten personenbezogene Daten verarbeitet, werden diese vom Geltungsbereich der DSGVO zwar nicht umfasst. Doch auch wenn die Reichweite dieser sogenannten „Haushaltsausnahme" nicht umschrieben ist, kristallisiert sich aus der Rechtsprechung des Europäischen Gerichtshofes („**EuGH**") heraus, dass eine Verarbeitungstätigkeit freilich nicht mehr unter die Haushaltsausnahme fällt, wenn zumindest ein Teil der erhobenen Daten einem potenziell unbegrenzten Personenkreis durch Weitergabe zugänglich gemacht wird.[5] Gerade eine derartige Veröffentlichung gegenüber einer unbestimmten Anzahl an Personen erfolgt zumindest in öffentlichen Blockchains, wodurch uE die Anwendbarkeit von Artikel 2 Abs 2 lit c DSGVO ausscheidet. Der sehr breit gefächerte Verarbeitungsbegriff umfasst freilich beinahe jeglichen Umgang mit persönlichen Daten.[6]

Unter einem **Dateisystem** versteht die Verordnung Artikel 4 Z 6 DSGVO zufolge *"jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird"*[7]. Dieser Definition entsprechend kann die Blockchain, die umgangssprachlich oft als eine Art Kontobuch bezeichnet wird, problemlos unter den Begriff ‚Dateisystem' subsumiert werden. Trotz der zahlreichen Unterschiede, die im Lichte des Einsatzes verschieden ausgestalteter Blockchains denkbar sind, bleibt das Wesen der Technologie als Aneinanderreihung von Datensätzen in jedem Fall bestehen. Die Sammlung der Daten mittels Blockchain folgt grundsätzlich einem einheitlichen System, das technisch vorgegeben wird. Die Blockchain weist demnach eine ausreichende Struktur auf, die entweder (im Normalfall) von jedem eingesehen werden kann oder die – wie verlangt – nach bestimmten Kriterien zugänglich ist. Im Hinblick auf das Erheben und Ordnen von Daten im Zuge von Transaktionen auf einer Blockchain und die damit verbundene dezentrale Speicherung dieser Daten ist folglich festzuhalten, dass diese Verarbeitungstätigkeiten zweifelsfrei dem Verarbeitungsbegriff der DSGVO entsprechen.[8]

Nach der Definition der DSGVO sind „**personenbezogene Daten**" gemäß Artikel 4 Z 1 alle *"Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann"*. Die DSGVO findet freilich keine Anwendung auf anonyme Informationen. Damit meint die Verordnung *"Informationen, die sich nicht auf eine identifizierte oder identifizierbare Person beziehen, oder personenbezogene Daten, die derart anonymisiert sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann."*[9] Davon zu unterscheiden ist die Pseudonymisierung, wonach bei pseudonymisierten Daten ein Personenbezug der Daten wiederhergestellt werden kann, da die Verarbeitung personenbezogener Daten „nur" so erfolgt, dass die Daten ohne Zusatzinformationen keiner spezifischen Person mehr zugeordnet werden können.[10] Ob nun auf einer Blockchain personenbezogene Daten verarbeitet werden, kommt ua auf die jeweilige Ausgestaltung der Blockchain an. Dabei wird zwischen privaten und öffentlichen Blockchains unterschieden: Während bei der privaten Blockchain von einer zentralen Stelle der private Schlüssel einer bestimmten Person zugeordnet und somit auch eindeutig ein Personenbezug hergestellt werden kann, ist es bei der öffentlichen Blockchain, auf der jeder Teilnehmer Daten speichern, überprüfen und ergänzen kann, grundsätzlich nicht möglich, vom öffentlichen auf den privaten Schlüssel zu schließen.[11] In der Blockchain verwendet man Hashfunktionen, um die Informationen in den Datenblöcken zu verschlüsseln.[12] Auch wenn die Hashfunktionen immer komplexer werden, ist eine Rückrechnung – vor allem in Zeiten von Cloudcomputing und Supercomputern – theoretisch (bzw in der Zukunft) nicht ausgeschlossen.[13] Auch mit Hilfe von Big-Data-Analysen oder der Ermittlung der IP-Adresse könnte ein Personenbezug hergestellt werden.[14]

Die Klarnamen von Blockchain-Teilnehmern werden im Normalfall durch Pseudonyme ersetzt, weswegen ihre Identität daraus zumindest nicht direkt hervorgeht; von einer identifizierbaren natürlichen Person ließe sich folg-

5 EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551; vgl auch *Jahnel/Pallwein-Prettner/Marzi*, Datenschutzrecht[2] 64.
6 Vgl *Hladjk* in Knyrim, Datenschutz-Grundverordnung 39.
7 Artikel 4 Z 6 DSGVO.
8 Vgl *Gorzala/Hanzl*, RdW 2018, 485 (486).
9 ErwGr 26 DSGVO.
10 Vgl *Jahnel/Pallwein-Prettner/Marzi*, Datenschutzrecht[2] 53.
11 Vgl *Gorzala/Hanzl*, RdW 2018, 485 (487).
12 Vgl *Knoll*, ZIIR 2016, 406 (407).
13 Vgl auch *Dobrauz-Saldapenna/Rosenauer*, in Pachinger [Hrsg], Datenschutz. Recht und Praxis, 2019, 133–152.
14 Vgl *Gorzala/Hanzl*, RdW 2018, 485 (488).

lich nur dann sprechen, wenn ihre Identität mithilfe zusätzlicher Informationen ermittelt werden kann.[15] Zur Einordnung, ob es für die Ermittlung des Personenbezugs auf eine entsprechende Möglichkeit des Verantwortlichen – dessen datenschutzrechtliche Stellung im Kontext der Blockchain an späterer Stelle ausgeführt wird – ankommt, oder ob auch auf andere Personen abzustellen ist, existieren unterschiedliche theoretische Konzepte. Nach der „relativen Theorie" muss der Verantwortliche selbst einen Personenbezug herstellen können, wobei in jedem Fall eine Verhältnismäßigkeitsprüfung hinsichtlich Identifizierungsmöglichkeit und dem damit verbundenen Arbeitsaufwand vonnöten wäre; folgt man der „absoluten Theorie", so soll schon eine Identifizierungs*möglichkeit* irgendeines Dritten genügen, obwohl man in ErwGr 26 durch die verwendeten Begrifflichkeiten eine gewisse Abschwächung ausmachen könnte:[16] „*Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. 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.*"[17] Darin lässt sich zwar eine Nähe zur absoluten Theorie erkennen, *Hein/Wellbrock/Hein* etwa vertreten jedoch die Ansicht, dass grundsätzlich der relativen Theorie zu folgen ist, als andernfalls eine wirksame Anonymisierung von Daten nahezu ausgeschlossen und eine Pseudonymisierung generell immer rückverfolgbar wäre; im Hinblick auf die Blockchain solle jedoch aufgrund der nicht eindeutig bestimmbaren Verantwortlichkeit die absolute Theorie gelten.[18]

Gerade bei privaten Blockchains, und zwar dann, wenn die Identifikation der beteiligten Akteure einer Transaktion auf der Blockchain einen wesentlichen Bestandteil darstellt – dies ist etwa bei einem Register gewerblicher Schutzrechte der Fall – ist eine Verarbeitung personenbezogener Daten impliziert.[19] Der EuGH hat in diesem Kontext ausgesprochen, dass auch eine dynamische IP-Adresse ein personenbezogenes Datum darstellt, da der Verantwortliche mithilfe von Zusatzinformationen des Internetproviders im Grunde die Daten der IP-Adresse zu einem bestimmten Zeitpunkt mit den Kontaktdaten der natürlichen Person verknüpfen kann, wodurch die Person identifizier*bar* wird.[20] *Hein/Wellbrock/Hein* folgern daraus: „*In diesem Fall ist der EuGH der relativen Theorie gefolgt, die darum erweitert wurde, dass Informationen Dritter einzubeziehen sind, falls der Verarbeiter einen Rechtsanspruch hat, auf diese Informationen zuzugreifen*".[21] Aufgrund der strengen EuGH-Rsp ist daher davon auszugehen, dass auch öffentliche Blockchains in den Anwendungsbereich der DSGVO fallen.[22] Im Fall von Kryptowährungen etwa besteht die grundsätzliche Möglichkeit, Informationen derart zusammenzuführen, dass die IP-Adresse von Nutzern ausgelesen werden kann; ggf ist die dadurch bestehende Identifizierungsmöglichkeit – wie schon angeschnitten – durch eine Pseudonymisierung abgeschwächt, soweit alle dazu benötigten Informationen mit ausreichenden Sicherheitsvorkehrungen getrennt von den anderen Daten aufbewahrt werden.[23]

Fraglich ist in diesem Zusammenhang auch, ob ein Hash als personenbezogenes Datum zu qualifizieren ist. Ganz allgemein lässt sich dazu feststellen, dass es sich bei einem Hashwert um ein personenbezogenes Datum handelt, wenn durch Heranziehung zusätzlicher Informationen der Hashwert einer natürlichen Person zugeordnet werden kann.[24] Während der Erzeuger des Hashwertes relativ einfach einen Personenbezug herstellen kann, stellt der Hashwert für den Empfänger, der ausschließlich den Hashwert erhält, dann kein personenbezogenes Datum dar, wenn er keine Rückschlüsse auf die jeweilige Person ziehen kann.[25] In diesem Zusammenhang hat auch das Verwaltungsgericht Bayreuth in einem Beschluss ausgesprochen, dass gehashte E-Mail-Adressen personenbezogene Daten sind, da das Hashen per se keine Anonymisierung darstellt.[26]

15 *Hein/Wellbrock/Hein*, Blockchain-Anwendungen 22.
16 *Hein/Wellbrock/Hein*, Blockchain-Anwendungen 23–24.
17 ErwGr 26 DSGVO.
18 *Hein/Wellbrock/Hein*, Blockchain-Anwendungen 24.
19 *Schreiber*, Was Blockchain mit Datenschutz zu tun hat, https://www.haerting.de/neuigkeit/was-blockchain-mit-datenschutz-zu-tun-hat (Stand 7.3.2018).
20 Vgl EuGH C-582/14, *Breyer/Bundesrepublik Deutschland*, ECLI:EU:C:2016:779; vgl auch *Jahnel/Pallwein-Prettner/Marzi*, Datenschutzrecht² 50.
21 *Hein/Wellbrock/Hein*, Blockchain-Anwendungen 23.
22 Vgl *Gorzala/Hanzl*, RdW 2018, 485 (488).
23 *Piska/Wagner*, ZTR 2018, 195 (198).
24 *Kuss/Bader/Preikschat*, Blockchain DSGVO-konform betreiben, https://www.cio.de/a/blockchain-dsgvo-konform-betreiben,3591845,5 (Stand 28.11.2018).
25 *Kuss/Bader/Preikschat*, Blockchain DSGVO-konform betreiben, https://www.cio.de/a/blockchain-dsgvo-konform-betreiben,3591845,5 (Stand 28.11.2018).
26 VG Bayreuth, Beschluss v 8.5.2018 – B 1 S 18.105, http://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-9586?AspxAutoDetectCookieSupport=1 (abgefragt 1.4.2019).

III. Rechtmäßigkeit der Datenverarbeitung

Eine Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn eine Rechtsgrundlage gemäß Artikel 6 Abs 1 DSGVO vorliegt. Eine rechtmäßige Verarbeitung kann sich auf (i) eine freiwillige Einwilligung der betroffenen Person, (ii) die Erfüllung eines Vertrages oder die Durchführung vorvertraglicher Maßnahmen, (iii) die Erfüllung einer rechtlichen Verpflichtung, (iv) lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person, (v) die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder auf (vi) die überwiegend berechtigten Interessen des Verantwortlichen oder eines Dritten stützen.

Durch die Wahl der Nutzung eines dezentralen Netzwerkes (wie zB das Bitcoin-Netzwerk) durch die betroffene Person kann eine de facto Zustimmung der jeweiligen Person angedacht werden.[27] Vorausgesetzt, eine erteilte Einwilligung wird als Rechtmäßigkeitsgrundlage herangezogen, muss die betroffene Person jedoch freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich eine Erklärung abgeben, dass sie mit einer bestimmten Datenverarbeitung einverstanden ist.[28] Dass die betroffene Person ihre Einwilligung in Kenntnis der Sachlage abgeben muss, umfasst sowohl den Umfang und den Zweck der Datenverarbeitung als auch die Kenntnis der Identität des Verantwortlichen.[29] Doch gerade bei einer öffentlichen Blockchain ist es im Zeitpunkt der Einwilligung für die betroffene Person unmöglich, sich des Verantwortlichen und des Umfangs der Datenverarbeitung ausreichend bewusst zu sein.

"Bei einer öffentlichen Blockchain ist eine Einwilligung schon deshalb nicht denkbar, weil ein Verantwortlicher nicht eindeutig festgestellt werden kann. Bei einer privaten Blockchain allerdings wird jeder Nutzer von einer zentralen Stelle eingeladen. Diese zentrale Stelle kann grundsätzlich als Verantwortlicher im Sinne der DSGVO angesehen werden."[30] Beispielhafte Konstellationen einer solchen zentralen Stelle wären Anbieter von elektronischen Geldbörsen (wallets) oder Dienstleister, welche die Blockchain als öffentliche Datenbank nutzen.[31] Somit kann festgehalten werden, dass die Frage der Rechtmäßigkeit der Datenverarbeitung im Rahmen einer privaten, genehmigten Blockchain einfacher zu beantworten ist, da von jedem Teilnehmer eine Einwilligung in die Geschäftsbedingungen und Datenschutzerklärung eingeholt werden kann, bevor sie bzw er Zugang zum Netzwerk erhält.

Da die betroffene Person jedoch gemäß Artikel 7 Abs 3 DSGVO das Recht hat, ihre Einwilligung jederzeit zu widerrufen, ist es ratsam, die Datenverarbeitung auf die Rechtsgrundlage der Vertragserfüllung gemäß Artikel 6 Abs 1 lit b DSGVO zu stützen. Auf Basis der Initiierung einer Transaktion durch den Nutzer selbst, kann argumentiert werden, dass die betroffene Person eine vertragliche Verpflichtung – immanent – mit der Plattform eingeht und sich die Rechtmäßigkeit der Datenverarbeitung somit auf diese Grundlage stützt.[32]

Sofern die Verarbeitung personenbezogener Daten nicht für einen bestehenden Vertrag erforderlich ist und die betroffene Person der Verarbeitung auch nicht explizit zugestimmt hat, könnte unter Umständen mit der Rechtsgrundlage des überwiegenden berechtigten Interesses gemäß Artikel 6 Abs 1 lit f DSGVO argumentiert werden. Dies trifft insofern zu, als in den meisten Fällen weder die Interessen noch die Grundrechte oder Grundfreiheiten der betroffenen Person überwiegen und somit ein stärkeres wirtschaftliches Interesse des Verantwortlichen an einer funktionieren Blockchain besteht, welches folglich eine rechtmäßige Verarbeitung personenbezogener Daten ermöglicht.

IV. Teilnehmer der Blockchain und ihre datenschutzrechtliche Stellung

Das dezentrale System der Blockchain und die Vielzahl der involvierten Akteure werfen die Frage auf, wer Verantwortlicher oder Auftragsverarbeiter im Sinne der DSGVO ist bzw welche datenschutzrechtliche Rolle die einzelnen Teilnehmer einer Blockchain einnehmen. Diese Einordnung ist insbesondere deshalb relevant, da, sobald personenbezogene Daten verarbeitet werden, der jeweilige Verantwortliche für die Einhaltung der geltenden Datenschutzregeln zu sorgen und diese Einhaltung auch nachzuweisen hat (Artikel 5 Abs 2 DSGVO).

A. Verantwortlicher im Sinne der DSGVO

Gemäß Artikel 4 Z 7 DSGVO ist Verantwortlicher jene natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Verantwortliche ist für die Einhaltung der Datenschutzbestimmungen verantwortlich, fungiert zugleich als Anlaufstelle für

27 *The European Union Blockchain Observatory and Forum*, Blockchain and the GDPR, https://www.eublockchainforum.eu/reports (S 24, Stand 16.10.2018).
28 Artikel 7 Abs 4 DSGVO; vgl *Feiler/Horn*, DSGVO 188.
29 Vgl *Jahnel/Pallwein-Prettner/Marzi*, Datenschutzrecht² 74.
30 *Piska/Wagner*, ZTR 2018, 195 (198).
31 *Jakúbek/Panic*, MR 2018, 255 (259–260).
32 *The European Union Blockchain Observatory and Forum*, Blockchain and the GDPR, https://www.eublockchainforum.eu/reports (S 25, Stand 16.10.2018).

betroffene Personen bei der Geltendmachung ihrer Rechte und ist allfälligen Haftungsansprüchen betroffener Personen ausgesetzt.[33] Die Artikel-29-Datenschutzgruppe – ein Beratungsorgan auf EU-Ebene, welches mittlerweile durch den Europäischen Datenschutzausschuss („**EDSA**") ersetzt wurde – hat veranschaulicht, in welchen Fällen über Mittel und Zwecke entschieden wird: Einerseits kann die Verantwortung aufgrund einer ausdrücklichen rechtlichen Zuständigkeit oder die Verantwortung aufgrund einer implizierten Zuständigkeit (zB Arbeitgeber in Bezug auf Daten über seine/ihre Mitarbeiter), andererseits die Verantwortung aufgrund eines tatsächlichen Einflusses (zB Bewertung vertraglicher Beziehungen) die Fähigkeit, über Zwecke und Mittel zu entscheiden, begründen.[34]

B. Auftragsverarbeiter im Sinne der DSGVO

Nach dem Begriffsverständnis der DSGVO ist Auftragsverarbeiter *"eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet"*[35]. Maßgeblich ist, dass die Datenverarbeitungen des Auftragsverarbeiters im Auftrag und nur auf ausdrückliche Weisung des Verantwortlichen durchgeführt werden und der Auftragsverarbeiter selbst nicht über die Mittel und Zwecke der Verarbeitung entscheidet.[36] Ist dies der Fall, so ist gemäß Artikel 28 Abs 3 DSGVO zwingend eine schriftliche Auftragsverarbeitervereinbarung abzuschließen.

C. Teilnehmer

Nach der Definition der französischen Datenschutzbehörde CNIL ist Teilnehmer derjenige, der das Recht hat, einen Eintrag zu machen – zB eine Transaktion vorzunehmen, für welche eine Authentifizierung verlangt wird.[37]

Sowohl die wohl überwiegende Mehrheit der Literatur[38] als auch einige Datenschutzbehörden qualifizieren die einzelnen Teilnehmer als Verantwortliche im Sinne der DSGVO. Der ungarischen Datenschutzbehörde zufolge ist der für die Datenverarbeitung Verantwortliche in erster Linie jene juristische oder natürliche Person, die den Zweck der Datenverarbeitung bestimmt, Entscheidungen darüber trifft und durchführt. Da es sich bei der Blockchain um ein dezentrales System handelt, in dem es keine zentrale Stelle gibt, welche Aufsichtsrechte über den Systembetrieb und die Datentransaktionen ausübt, sind es die einzelnen Benutzer, welche die Datenverarbeitung faktisch durchführen.[39] Probleme ergeben sich gerade bei der öffentlichen Blockchain jedoch dahingehend, dass (üblicherweise) keiner der einzelnen Teilnehmer Einfluss auf das gesamte System hat. Bei einer privaten Blockchain hingegen ist derjenige Verantwortlicher im Sinne der DSGVO, der den Zugang zur Blockchain festlegt, da er über Mittel und Zwecke der Datenverarbeitung entscheiden kann.

Die französische Datenschutzbehörde ist der Ansicht, dass sowohl natürliche Personen, wenn die Verarbeitung personenbezogener Daten mit einer beruflichen oder kommerziellen Tätigkeit in Verbindung steht, als auch juristische Personen, die personenbezogene Daten in einer Blockchain verarbeiten, als Verantwortliche im Sinne des Artikel 4 Z 7 DSGVO zu qualifizieren sind.[40] Wie bereits unter Punkt 2 erläutert, ist die DSGVO zumindest nicht auf Transaktionen, die für rein private Zwecke erfolgen, anwendbar.

Diese Auffassung mag zwar in der Theorie logisch und nachvollziehbar klingen, praktisch würde eine Einordnung nach diesen Kriterien allerdings teilweise auf Probleme hinsichtlich der Überprüfbarkeit stoßen. Eine Differenzierung muss wiederum insbesondere im Lichte der denkbaren Unterschiede in der Ausgestaltung verschiedenartiger Blockchains vorgenommen werden. Wie bereits ausgeführt, könnten bei privaten Blockchains mit wenigen Teilnehmern nach den Kriterien der französischen Datenschutzbehörde relativ einfach Verantwortliche ausfindig gemacht werden. Bei öffentlichen Blockchains (zB der Bitcoin-Blockchain) mit unbegrenzter

33 Vgl *Jahnel/Pallwein-Prettner/Marzi*, Datenschutzrecht² 56.

34 Vgl *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", http://www.privacy-regulation.eu/privazyplan/article29/files/wp169%20DE%20Verantwortlicher%20vs.%20Auftragsverarbeiter%202010%2002%2016.pdf (Stand 16.2.2010).

35 Artikel 4 Z 8 DSGVO.

36 Vgl *Bogendorfer* in Knyrim, Datenschutz-Grundverordnung 170.

37 *CNIL*, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data (Stand 6.11.2018); vgl auch *Jakúbek/Panic*, MR 2018, 255 (256).

38 Vgl *Erbguth/Fasching*, ZD 2017, 560 (565) mwN; vgl *Jakúbek/Panic*, MR 2018, 255 (258).

39 *Hungarian National Authority for Data Protection and Freedom of Information*, The Opinion of the Hungarian National Authority for Data Protection and Freedom of Information on Blockchain Technology in the Context of Data Protection, https://www.naih.hu/files/Blockchain-Opinion-2018-01-29.pdf (S 4, Stand 18.7.2017).

40 *CNIL*, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf (S 1, Stand 6.11.2018).

Teilnehmeranzahl ist eine konkrete Rollenverteilung hingegen nahezu unmöglich. Die fehlende Beherrschbarkeit durch einzelne Personen führt zu einem Ergebnis, mit dem die – eigentlich dem Anspruch der Technologieneutralität folgende – DSGVO nicht umgehen kann: Der Ansatz, alle involvierten Teilnehmer gemäß Artikel 26 DSGVO gemeinsam zu Verantwortlichen – sogenannte „joint controller" – zu erklären (was grundsätzlich naheliegend wäre), kann schon im Hinblick auf konkrete Sanktionen für Datenschutzverletzungen nicht vollständig überzeugen. Ggf könnte man die Programmierer der Blockchain – soweit überhaupt bekannt, soweit sie am Netzwerk auch wirklich teilnehmen bzw soweit sie nicht lediglich im Werkvertragsverhältnis technische Implementierungen geliefert haben – als Verantwortliche ansehen, da spezifische technische Vorgaben bzgl der Art und Weise der Datenerhebung auf der Blockchain zumindest denkbar sind und einer Entscheidung über Zwecke und Mittel nahekommen.[41] Dabei ergeben sich allerdings zahlreiche Folgeprobleme, unter anderem hinsichtlich bereits bestehender Blockchains (freigegebener Quellcode) sowie einer technischen Anpassung an Änderungen der Rechtslage. Zwischen dem einfachsten Fall einer privaten Blockchain mit klarer Aufgabenverteilung und den schwer beherrschbaren Fällen von öffentlichen Blockchains mit extremer Speicherkapazität und einer Unmenge von Daten liegen Zwischenfälle, die eine Einordnung im Einzelfall verlangen. Außerdem wäre es über die Lokalisierung von potentiellen Verantwortlichen hinaus notwendig, ihnen eine Verbindung mit ihrer beruflichen oder kommerziellen Tätigkeit nachzuweisen. Ohne hier einen klaren Standpunkt zu beziehen, muss festgehalten werden, dass die DSGVO, die zugegeben einer anderen gesetzgeberischen Generation entstammt, im Moment selbst keine zufriedenstellende Lösung für jeden erdenklichen Fall zu bieten scheint.

D. Miner

Zunächst ist anzumerken, dass der Begriff „Miner" an dieser Stelle nicht zu eng verstanden werden und generell „Nodes" erfassen soll, die für die Validierung von Blöcken zuständig sind (vgl etwa die Bezeichnung „Validator" beim proof of stake Algorithmus). Auch im Hinblick auf die Tätigkeit der Miner wird in der Literatur die Ansicht vertreten, dass der einzelne Miner mangels eines rechtlichen oder tatsächlichen Einflusses auf die Transaktionen nicht als Verantwortlicher im Sinne der DSGVO zu qualifizieren ist.[42]

Nach der Auffassung der französischen Datenschutzbehörde CNIL sind Miner nicht Verantwortliche, sondern Auftragsverarbeiter, da sie nicht über die Mittel und Zwecke der Datenverarbeitung entscheiden, sondern „nur" Transaktionen validieren, die von Teilnehmern eingereicht wurden.[43] *Stadler/Völkel* sprechen in Vorträgen oft von der „Bienen-Theorie": Miner seien vergleichbar mit Bienen, die einen „Reward" für das „Bestäuben" und – geradezu nebenbei – für das Validieren von Transaktionen erhalten. Sie entscheiden nicht über die Menge des Nektars oder die Anzahl der Blumen/Transaktionen, daher nicht über Mittel und Zweck, im Übrigen auch nicht über die Höhe des „Rewards". Diesbezüglich ist sich die CNIL der praktischen Schwierigkeiten der Qualifikation der Miner als Auftragsverarbeiter v.a. im Hinblick darauf bewusst, dass bei einer öffentlichen Blockchain zwischen den Verantwortlichen und Auftragsverarbeitern Vereinbarungen gemäß Artikel 28 DSGVO geschlossen werden müssten. Die CNIL erachtet zudem den Datentransfer außerhalb der Europäischen Union besonders im Rahmen einer öffentlichen Blockchain als problematisch, da der Verantwortliche nur schwer die Kontrolle über den Standort der Miner hat. Bei der zulassungsbeschränkten Blockchain kann laut CNIL der Transfer durch Standardvertragsklauseln, verbindliche Unternehmensregeln, Verhaltenskodices oder Zertifizierungsmechanismen reguliert werden. Aus diesem Grund rät die französische Datenschutzbehörde zum Einsatz einer zulassungsbeschränkten Blockchain.[44]

Die ungarische Datenschutzbehörde ist hingegen der Ansicht, dass Miner Verantwortliche sind.[45] Dadurch wird der Kreis der Verantwortlichen einer Blockchain sehr weit gezogen.[46]

41 Zurecht ist darauf hinzuweisen, dass freilich bloße Hersteller von Systemen (Programmierer, Entwickler) keine Datenverarbeiter sind, wenn sie sich nicht am Konsensmechanismus beteiligen, vgl *Dobrauz-Saldapenna/Rosenauer*, in Pachinger [Hrsg], Datenschutz. Recht und Praxis, 2019 (133–152), mwN.

42 *Jakúbek/Panic*, MR 2018, 255 (257).

43 *CNIL*, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf (S 2, Stand 6.11.2018).

44 *CNIL*, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf (S 5, Stand 6.11.2018).

45 The Opinion of the Hungarian National Authority for Data Protection and Freedom of Information on Blockchain Technology in the Context of Data Protection, https://www.naih.hu/files/Blockchain-Opinion-2018-01-29.pdf (S 4, Stand 18.7.2017).

46 Vgl *Dobrauz-Saldapenna/Rosenauer*, in Pachinger [Hrsg], Datenschutz. Recht und Praxis, 2019 (133–152).

Da Miner jedoch auf die Transaktionen innerhalb der Blöcke und somit auf den Inhalt der Datensätze selbst keinen Einfluss haben – und somit keine wesentlichen Entscheidungen im Blockchain-System treffen[47] –, mangelt es ihnen an der Entscheidung über die Mittel und Zwecke der Datenverarbeitung, weshalb sie uE nicht als Verantwortliche im Sinne der DSGVO zu qualifizieren sind.

Ein anderer Zugang wäre, mehrere Miner als gemeinsame Verantwortliche im Sinne des Artikel 26 DSGVO zu qualifizieren. Durch einen Zusammenschluss mehrerer Miner zu mindestens 51 % der Rechenleistung des Netzwerkes könnte die Möglichkeit einer Entscheidung über die Mittel und Zwecke der Verarbeitung personenbezogener Daten gegeben sein. Bei dieser Konstellation ist es geboten, gemäß Artikel 26 Abs 1 DSGVO zwischen den Verantwortlichen eine schriftliche Vereinbarung darüber abzuschließen, wer welche Verpflichtungen gemäß der DSGVO erfüllt. Unseres Erachtens ist eine Einordnung von Minern als gemeinsame Verantwortliche allerdings verfehlt, da diese lediglich Transaktionen zusammenfassen und Hashwerte errechnen, eine Veränderung der personenbezogenen Daten ist ihnen allerdings verwehrt,[48] weshalb Minern keine datenschutzrechtliche Verantwortlichkeit im Sinne des Artikel 4 Z 7 DSGVO auferlegt werden kann.

E. Non mining full nodes

„Non mining full nodes" sind Full Nodes, die keine neuen Blöcke erzeugen und dementsprechend keine Miner sind; sie verifizieren die Richtigkeit einzelner unbestätigter Transaktionen unabhängig von sowie vor der Übermittlung an andere(n) Nodes nach fest vorgegebenen Regeln.[49]

In der Literatur gibt es kaum Ansätze hinsichtlich der Frage, welche Stellung den „non mining full nodes" zukommt. Dies ist nicht zuletzt darauf zurückzuführen, dass begrifflich nur selten zwischen verschiedenen Arten von Nodes differenziert wird, obwohl eine solche Unterscheidung rechtlich an manchen Stellen durchaus geboten wäre. *Jakúbek/Panic* vertreten die Ansicht, „*ihre Stellung ähnelt* [...] *jener eines Telekommunikationsbetreibers, der in Bezug auf die von seinen Kunden über das Netzwerk übermittelten Daten* [...] *nicht Verantwortlicher ist.*"[50] Die Einordnung, dass Telekommunikationsbetreiber nicht als Verantwortliche im Sinne der DSGVO anzusehen sind, basiert auf einer Stellungnahme der Artikel-29-Datenschutzgruppe aus 2010.[51]

Da die einzelnen „non mining full nodes" bei Transaktionen ausschließlich die Einhaltung fixierter Regeln überprüfen und ein entsprechendes Ergebnis übermitteln, allerdings keinerlei faktischen Einfluss auf den Inhalt neuer Blöcke ausüben, kommt eine Qualifizierung als Verantwortliche im Sinne der DSGVO unseres Erachtens von vornherein nicht in Betracht, da sie weder über die Mittel noch über die Zwecke der Verarbeitung personenbezogener Daten entscheiden.

Die Verarbeitung von Transaktionsdaten zur Verifizierung und nachfolgenden Übermittlung durch „non mining full nodes" – ohne Interesse oder Bedarf an einer inhaltlichen Verarbeitung personenbezogener Daten – fällt dessen ungeachtet aufgrund des weiten Verarbeitungsbegriffs freilich in den Anwendungsbereich der DSGVO.[52] Ggf wäre eine Klassifizierung als Auftragsverarbeiter gemäß Artikel 28 DSGVO denkbar. Dabei müsste allerdings ein Weisungszusammenhang zu einem als Verantwortlicher zu qualifizierendem Teilnehmer der Blockchain hergestellt werden können, wobei – wie bereits aufgezeigt – schon die Einordnung von Teilnehmern als Verantwortliche generell in vielen Fällen Schwierigkeiten bereitet.

V. Vollständige Wahrnehmung der Betroffenenrechte?

Sofern personenbezogene Daten in zulässiger Weise verarbeitet werden, müssen die gesetzlichen Informationspflichten sowie die Betroffenenrechte gewahrt werden. Im Hinblick auf die rechtmäßige Wahrnehmung der in der DSGVO vorgesehenen Betroffenenrechte, ist zwischen den einzelnen Rechten der betroffenen Person zu differenzieren. Während das Recht auf Information (Artikel 13, 14 DSGVO), das Recht auf Auskunft (Artikel 15 DSGVO) und das Recht auf Datenübertragbarkeit (Artikel 20 DSGVO) mit den technischen Eigenschaften der Blockchain kompatibel erscheinen, ergeben sich beim Recht auf Löschung (Artikel 17 DSGVO) technische Umsetzungsschwierigkeiten.[53] Entgegen der Ansicht der CNIL sind *Dobrauz-Saldapenna/Rosenauer* der Ansicht, dass dem Recht auf Auskunft im Zusammenhang mit der Blockchain-Technologie nur unzureichend entsprochen

47 *Hein/Wellbrock/Hein*, Blockchain-Anwendungen 28.
48 *Hein/Wellbrock/Hein*, Blockchain-Anwendungen 30.
49 Vgl *Jakúbek/Panic*, MR 2018, 255 (256).
50 *Jakúbek/Panic*, MR 2018, 255 (257).
51 Vgl *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", http://www.privacy-regulation.eu/privazyplan/article29/files/wp169%20DE%20Verantwortlicher%20vs.%20Auftragsverarbeiter%202010%2002%2016.pdf (Stand 16.2.2010).
52 Vgl *Jakúbek/Panic*, MR 2018, 255 (257).
53 So auch *CNIL*, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf (S 8, Stand 6.11.2018).

werden kann. Denn „*innerhalb der Blockchain werden schließlich Informationen und Daten über alle Nodes verteilt, unabhängig von geografischen Grenzen. Darüber hinaus ist es nicht möglich über einen Node in Erfahrung zu bringen, welche personenbezogenen Daten verarbeitet werden, da diese verschlüsselt sind.*“[54]

A. Recht auf Löschung

Artikel 17 Abs 1 DSGVO normiert das Recht der betroffenen Person, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, wenn (i) die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden nicht mehr notwendig sind, (ii) die betroffene Person ihre Einwilligung widerruft, (iii) die betroffene Person Widerspruch gegen die Datenverarbeitung einlegt, (iv) die personenbezogenen Daten unrechtmäßig verarbeitet wurden, (v) die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist oder (vi) die personenbezogenen Daten eines Kindes bzgl angebotener Dienste der Informationsgesellschaft gemäß Artikel 8 Abs 1 DSGVO erhoben wurden.

Das Recht auf Löschung berührt jedoch nicht die Pflicht des Verantwortlichen, auch ohne Antrag einer betroffenen Person in regelmäßigen Abständen zu überprüfen, ob verarbeitete Daten zu löschen sind.[55] Unter Löschung per se wird die technische Löschung elektronischer Daten verstanden, sodass kein Zugriff auf die Daten mehr erfolgen kann.[56] Die DSGVO selbst definiert nicht, was genau unter „Löschen“ zu verstehen ist. Grundsätzlich kann jedoch gesagt werden, dass es dem Verantwortlichen obliegt, dass die Daten unter Anwendung üblicher Verfahren nicht mehr ausgelesen werden können („physische Löschung“), sie müssen unkenntlich gemacht werden.[57]

Für den Fall, dass der Verantwortliche die personenbezogenen Daten öffentlich gemacht hat und zur Löschung derselben verpflichtet ist, hat er gemäß Artikel 17 Abs 2 DSGVO, unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten, angemessene Maßnahmen – auch technischer Art – zu treffen, um für die Datenverarbeitung Verantwortliche, welche die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien dieser verlangt hat. Dieses sogenannte „Recht auf Vergessenwerden“ besteht allerdings selbstständig und kann sohin etwa auch mit einem Berichtigungsantrag kombiniert werden.[58] Die spiegelbildliche Pflicht des Verantwortlichen beschränkt sich auf die Information Dritter, denn eine Löschung muss vom Verantwortlichen bei den Dritten nicht erwirkt werden. Ein weitergehendes „Recht auf Vergessenwerden“ besteht im Zusammenhang mit dem Auffinden von personenbezogenen Informationen in Suchmaschinen. In der Rechtssache *Google Spain und Google* sprach der EuGH die Möglichkeit einer Verpflichtung von Suchmaschinen aus, Daten aus ihren Suchergebnissen zu entfernen, soweit diese auf Informationen über das betroffene Individuum verweisen, an deren Auffindbarkeit kein besonderes öffentliches Interesse (mehr) besteht.[59] Gerade dieses „Recht auf Vergessenwerden“ könnte mit der Transparenz und Unlöschbarkeit von Informationen auf der Blockchain kollidieren, sofern Suchmaschinen mithilfe dieser Technologie betrieben werden.

Wenn Daten nun auf der Blockchain gespeichert werden, kann der Verantwortliche diese Daten bei der Eingabe in die Blockchain durch Verschlüsselung oder Hashfunktionen fast unzugänglich machen. Allerdings ist es technisch unmöglich, dem Recht auf Löschung im Sinne des Art 17 DSGVO nachzukommen, da die Daten weiterhin auf der Blockchain existieren und nicht endgültig gelöscht werden. Es können zwar in einem neuen Block ältere Informationen (personenbezogene Daten) für ungültig erklärt werden, vollständig gelöscht werden die Daten dennoch nicht, da sie für alle Teilnehmer weiterhin lesbar bleiben.

Eine Möglichkeit, dieser Problematik zu begegnen, wäre, editierbare – sogenannte „redactable“ – Blockchains zu schaffen, die ex-ante derart konzipiert sind, dass es einer autorisierten Stelle ermöglicht wird, Blöcke nachträglich zu ändern bzw zu löschen und gleichzeitig die Unversehrtheit der Blockchain zu erhalten. Dies kann etwa mittels sogenannter „Chamäleon-Hashes“ erreicht werden, die anstelle von gewöhnlichen kryptografischen Hashwerten an jenen Stellen eingesetzt werden, die einer späteren Veränderung durch Berechtigte zugänglich sein sollen; dabei können auch Änderungsbedingungen (zB Fristen) definiert werden.[60] Ein solches Konzept, das es zulässt, den selben Hash für den selben Block mittels privatem Schlüssel öfter zu vergeben, wurde für private Blockchains vom Unternehmen Accenture entwickelt.[61] Veränderungen bleiben durch „digitale

54 *Dobrauz-Saldapenna/Rosenauer*, in Pachinger [Hrsg], Datenschutz. Recht und Praxis, 2019 (133–152).
55 Vgl *Jahnel/Pallwein-Prettner/Marzi*, Datenschutzrecht² 113.
56 Vgl *Jahnel/Pallwein-Prettner/Marzi*, Datenschutzrecht² 114.
57 *Haidinger* in Knyrim, DatKomm Art 17 Rz 63 (Stand 1.10.2018, rdb.at); OGH 11.10.2010, 6 Ob 112/10d.
58 *Haidinger* in Knyrim, DatKomm Art 17 Rz 4.
59 EuGH C-131/12, *Google Spain und Google*, ECLI:EU:C:2014:317.
60 Vgl *Erbguth*, DATENSCHUTZ AUF ÖFFENTLICHEN BLOCKCHAINS, https://erbguth.ch/Erbguth_DatenschutzBlockchains.pdf (S 3, abgefragt 30.4.2019).
61 *Piska/Wagner*, ZTR 2018, 195 (201).

Narben" sichtbar, weswegen zumindest die Tatsache, dass eine Änderung vorgenommen wurde, jederzeit transparent nachvollziehbar ist.[62] Auch wenn dies insgesamt ein guter Ansatz ist, um dem Recht auf Löschung nach der DSGVO zu entsprechen, eignet sich diese Lösung vorrangig für private, geschlossene Blockchains, da wiederum eine zentrale Instanz, der vertraut werden soll, die Änderungen genehmigen muss.[63] Im Bereich der öffentlichen Blockchains müsste (i) ein zu solchen Änderungen Berechtigter ausfindig gemacht werden; außerdem wären die Daten (ii) zunächst öffentlich einsehbar, was vielfach nicht gewollt sein wird.[64] *Piska/Wagner* stehen einem Einsatz in öffentlichen Blockchains schon aus Gründen der Glaub- und Vertrauenswürdigkeit der Blockchain abneigend gegenüber.[65] In jedem Fall muss uE bereits im Vorhinein festgelegt werden, dass „Chamäleon-Hashes" eingesetzt werden, was Teilnehmern schon beim Beitritt zu einem Blockchain-Netzwerk wissen lässt, dass eine nachträgliche Änderungsmöglichkeit besteht.[66]

Ein weiterer interessanter Ansatz, welcher das Potential hat, die Vorzüge der Blockchain-Technologie mit den Anforderungen der DSGVO zu vereinen, bestünde darin, personenbezogene Daten von vornherein nicht direkt auf der Blockchain zu speichern oder auf eine Art zu speichern, die es niemandem ermöglicht, persönliche Informationen zu gewinnen. Sogenannte „Zero Knowledge Proofs" erlauben es etwa, Transaktionen derart in der Blockchain abzulegen, dass alleine die rechnerische Korrektheit, allerdings kein Inhalt, ausgelesen werden kann (vgl etwa die Kryptowährung Zcash).[67] Das Speicherverfahren „Content Addressed Storage" ermöglicht es mithilfe eines Smart Contracts, außerhalb der Blockchain gespeicherte Daten über Referenzen in der Blockchain aufzufinden. Daneben kann die generelle Möglichkeit der Verschlüsselung, welche die DSGVO an einigen Stellen erwähnt, auch im Zusammenhang mit der Blockchain – allerdings auf Kosten ihrer Transparenz – fruchtbar gemacht werden. Soweit Daten ausschließlich verschlüsselt auf der Blockchain gespeichert werden, haben nur jene Personen Zugriff auf persönliche Informationen, die den Schlüssel kennen. Nicht eine Löschung der verschlüsselten Daten selbst, aber eine unwiderrufliche Löschung des Schlüssels ist möglich und geeignet, um den Personenbezug der Daten endgültig zu entfernen. Dabei ist zu beachten, dass auch ein Smart Contract keinen Zugriff auf die verschlüsselten Daten haben darf.[68] Eine Möglichkeit, um dem Recht auf Löschung vollständig nachzukommen, wäre, personenbezogene Daten in einem „off-chain"-Datenspeicher aufzubewahren, da somit bei Bedarf personenbezogene Daten ohne weitere Auswirkungen gelöscht werden können.[69] Wie gut sich diese Lösungsmodelle für öffentliche Blockchains eignen, muss im Einzelfall beurteilt werden.

Eine entsprechende Ausgestaltung der Blockchain könnte es auch ermöglichen, personenbezogene Daten aus älteren Blöcken zu entfernen, wenn sie nicht mehr benötigt werden.[70] Durch das sogenannte „Pruning" werden Hashbäume verkürzt, wobei die Verkürzung bei allen teilnehmenden Nodes zwangsweise durchgesetzt werden kann.[71] Daten, die dabei gelöscht werden sollen, müssen bereits in einer neuen Transaktion enthalten sein, weswegen Informationen entfernt werden können, ohne, dass der jeweilige Legitimationsnachweis und die Funktionsfähigkeit der Blockchain verloren geht (der Hashwert des Blocks bleibt eben unverändert).[72] Da die Idee dahinter eine Verbesserung der Leistung durch Reduzierung der Größe der Blockchain ist, eignet sich „Pruning" grundsätzlich zur Speicherbegrenzung im Sinne von Artikel 5 Abs 1 lit e DSGVO.[73] Dieser Ansatz zeigt ebenfalls Potential, eine Wahrung des Rechts auf Löschung nach Artikel 17 DSGVO zu ermöglichen; allerdings führt „Pruning" im Gegenzug sehr wahrscheinlich zu einem Verlust von Nachvollziehbarkeit sowie Fälschungssicherheit der Blockchain.[74] Außerdem zieht die Notwendigkeit einer zentralen (vertrauenswürdi-

62 *Hein/Wellbrock/Hein*, Blockchain-Anwendungen 41.
63 Vgl *Dobrauz-Saldapenna/Rosenauer*, in Pachinger [Hrsg.], Datenschutz. Recht und Praxis, 2019, 13 (133–152).
64 Vgl *Erbguth*, DATENSCHUTZ AUF ÖFFENTLICHEN BLOCKCHAINS, https://erbguth.ch/Erbguth_DatenschutzBlockchains.pdf (S 3, abgefragt 30.4.2019).
65 *Piska/Wagner*, ZTR 2018, 195 (200).
66 *Hein/Wellbrock/Hein*, Blockchain-Anwendungen 41.
67 Vgl *Erbguth*, DATENSCHUTZ AUF ÖFFENTLICHEN BLOCKCHAINS, https://erbguth.ch/Erbguth_DatenschutzBlockchains.pdf (S 4, abgefragt 30.4.2019).
68 Vgl *Erbguth*, DATENSCHUTZ AUF ÖFFENTLICHEN BLOCKCHAINS, https://erbguth.ch/Erbguth_DatenschutzBlockchains.pdf (S 4, abgefragt 30.4.2019).
69 *IBM Security*, Blockchain and the GDPR – How blockchain could address five areas associated with GDPR compliance, https://www.ibm.com/downloads/cas/2EXR2XYP (abgefragt 2.5.2019).
70 *The European Union Blockchain Observatory and Forum*, Blockchain and the GDPR, https://www.eublockchainforum.eu/reports (S 31, Stand 16.10.2018).
71 Vgl *Wagner/Groß*, Blockchain und Smart Contracts – Moderne IT-Konzepte aus (datenschutz-)rechtlicher Sicht, https://www.psp.eu/media/allgemein/white_paper_blockchain.pdf (abgefragt 2.5.2019).
72 *Hein/Wellbrock/Hein*, Blockchain-Anwendungen 40.
73 *The European Union Blockchain Observatory and Forum*, Blockchain and the GDPR, https://www.eublockchainforum.eu/reports (S 31, Stand 16.10.2018).
74 *Hein/Wellbrock/Hein*, Blockchain-Anwendungen 40.

gen) Instanz, welche Löschungen vornimmt, wiederum eine stark eingeschränkte Eignung für bestimmte Arten von Blockchains nach sich, die sich gerade die Veränderungsresistenz auf ihre Fahnen geheftet haben.

In diesem Zusammenhang ist auch anzumerken, dass die betroffene Person die unverzügliche Löschung ihrer Daten nur verlangen kann, wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (Artikel 17 Abs 1 lit a DSGVO). In diesem Kontext stellt sich allerdings auch die Frage, ob die Daten für den erhobenen Zweck im Hinblick auf die technischen Besonderheiten der Blockchain nicht doch notwendig sind und auch bleiben. Denn gerade die Unveränderlichkeit der einzelnen Blöcke und die konstante Nachvollziehbarkeit aller Vorgänge auf einer Blockchain sind ihre elementaren Bestandteile und in vielen Fällen jene Eigenschaften, aufgrund derer eine Blockchain überhaupt eingesetzt werden soll.

Die Tatsache, dass Daten in einem Block, der von der Mehrheit der Teilnehmer akzeptiert worden ist, im Normalfall technisch nicht mehr verändert oder gelöscht werden können, spielt auch für den Grundsatz der Datenminimierung gemäß Artikel 5 Abs 1 lit c DSGVO eine Rolle. Demnach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Problematisch in diesem Zusammenhang ist auch, dass der Blockchain permanent neue Blöcke hinzugefügt werden, wodurch dem Grundsatz der Datenminimierung nur schwer entsprochen werden kann. Des Weiteren müsste eine Aufbewahrungsfrist für die Speicherung der personenbezogenen Daten festgelegt werden, was de facto aufgrund der technischen Gegebenheiten der Blockchain jedoch nicht möglich ist. Ein möglicher Ansatz in diesem Zusammenhang wäre es, die Datenspeicherung über die Erreichung des mit der Blockchain verbundenen Zweckes zu rechtfertigen. „*Bei der Datenspeicherung in der Blockchain erfolgt die Validierung einer neuen Transaktion immer unter Berücksichtigung der bereits verbuchten Transaktionen. Da die gesamte Transaktionshistorie erforderlich ist, um neue Daten zu validieren bzw. um eine mehrseitige Überprüfbarkeit herzustellen, kann ins Treffen geführt werden, dass genau das für die Zweckerreichung erforderlich ist. Somit wäre dieses Vorgehen mit dem Prinzip der Datenminimierung vereinbar.*“[75]

Generell kann gesagt werden, dass eine Blockchain, auf der die Speicherung personenbezogener Daten vorgesehen ist, schon in der Entwicklungsphase auf diese Aufgabe vorbereitet werden sollte. Die DSGVO bezeichnet dies in Art 25 als „Datenschutz durch Technikgestaltung“ (geläufiger als privacy by design) und sieht vor, dass die Befolgung datenschutzrechtlicher Grundsätze schon durch eine frühzeitige technische Implementierung sichergestellt werden soll. In solchen Fällen wird gerade bei privaten Blockchains ein DSGVO-konformer Einsatz relativ einfach realisierbar sein. Bei durchdachter und gezielter technischer Umsetzung kann eine Blockchain darüber hinaus sogar förderlich für den Datenschutz sein und eine Überwachung der Einhaltung der DSGVO begünstigen bzw mittels Smart Contracts selbst durchführen.

B. Recht auf Berichtigung

Gemäß Artikel 16 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen unverzüglich die Berichtigung oder die Vervollständigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unseres Erachtens ist es technisch unmöglich, das Recht auf Berichtigung verordnungskonform zu gewährleisten, wenn unverschlüsselte Daten auf der Blockchain gespeichert werden. Denn ebenso wie beim Recht auf Löschung können die Daten auf den einzelnen Blöcken einer Blockchain nicht mehr geändert und somit weder berichtigt noch vervollständigt werden, weshalb auch diesem Recht der betroffenen Person nicht im Sinne der DSGVO entsprochen werden kann. *Dobrauz-Saldapenna/Rosenauer* zufolge wäre ein Lösungsansatz, „*die unrichtigen Daten auf der Blockchain zu belassen und mittels einer ergänzenden Erklärung richtig zu stellen. Durch diese Vorgehensweise würde der ursprünglich falsche Eintrag nicht gelöscht oder direkt verändert (was auch nicht möglich wäre). Allerdings ist eine solche ergänzende Erklärung nur zulässig, wenn sie das Prinzip der Zweckbindung gleichermaßen berücksichtigt und erfüllt.*“[76]

C. Informations- und Auskunftspflichten

Sobald personenbezogene Daten verarbeitet werden, sind nicht nur gewisse Betroffenenrechte zu wahren, sondern auch die Informationspflichten gemäß Artikel 13 bzw Artikel 14 DSGVO zu erfüllen. Daraus resultiert für den Verantwortlichen unter anderem die Pflicht, der betroffenen Person den Namen und die Kontaktdaten des Verantwortlichen mitzuteilen. Wie dies im Rahmen einer Blockchain-Transaktion zu erfolgen hat, ist allerdings fraglich.

75 *Dobrauz-Saldapenna/Rosenauer*, in Pachinger [Hrsg], Datenschutz. Recht und Praxis, 2019, (133–152).

76 *Dobrauz-Saldapenna/Rosenauer*, in Pachinger [Hrsg], Datenschutz. Recht und Praxis, 2019, (133–152).

Im Hinblick auf das Recht auf Auskunft gemäß Artikel 15 DSGVO, wonach die betroffene Person das Recht hat, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden, ist anzumerken, dass die mangelnde Feststellung eines Verantwortlichen der betroffenen Person die vollständige Ausübung dieses Rechts verwehren kann. Folglich stellen sich diese Probleme immer dann nicht, wenn entsprechend den bisherigen Ausführungen ein Verantwortlicher – insbesondere bei privaten Blockchains – bestimmt werden kann. Er wäre dann zuständig, Betroffenen die von der DSGVO geforderten Informationen zu erteilen. Auskunft über Verarbeitungen kann gerade durch die lückenlose Dokumentation von Daten auf der Blockchain leicht gewährt sowie die Richtigkeit der Angaben einfach bewiesen werden. Soweit allerdings kein Verantwortlicher auszumachen ist bzw unklar ist, wer tatsächlich als Verantwortlicher in Frage kommt, ergeben sich verschiedenartige und skurrile Probleme, die im Moment wohl noch nicht abschließend aufgelöst werden können. Folgt man etwa der Ansicht, dass die Teilnehmer einer öffentlichen Blockchain entsprechend Artikel 26 DSGVO gemeinsam verantwortlich sind, könnte zB Person A, die eine Transaktion auf der Bitcoin-Blockchain tätigt und im Weiteren über die Auslesung ihrer (dynamischen) IP-Adresse mit nachfolgender Verknüpfung von Daten identifizierbar wäre, gemeinsam mit Person B – die ebenfalls am Netzwerk teilnimmt – für die Datenverarbeitung verantwortlich sein (die Zahl der Teilnehmer wird hierbei natürlich stark vereinfacht). Gleichzeitig ist sie aber eine betroffene Person, da es sich um ihr personenbezogenes Datum IP-Adresse handelt. Für Person B könnte dies in gleicher Weise zutreffen. Person A und Person B müssten sich nun abstimmen, wer den Informationspflichten und Betroffenenrechten im Sinne der DSGVO nachkommt. Gemäß Artikel 12 Abs 4 DSGVO finden die Informationspflichten keine Anwendung, wenn die betroffene Person bereits über die Informationen verfügt. Weiß Person A nun im konkreten Beispiel, dass durch eine einfache Bitcoin-Transaktion eine Verarbeitung personenbezogener Daten mittels Blockchain in Gang gesetzt wurde sowie, dass sie selbst gemeinsam mit Person B verantwortlich dafür ist?

VI. Fazit

Die einfachste Lösung, datenschutzkonform mit der Blockchain-Technologie zu interagieren, ist es, alle personenbezogenen Daten von öffentlichen oder privaten Blockchain-Transaktionen off-chain, zum Beispiel in einer Datenbank oder in einem Filesystem, zu speichern. In weiterer Folge könnte ein Link zu den Daten führen, der aber ins Leere läuft, sobald die Daten gelöscht werden. In diesem Kontext empfiehlt bereits das „EU Blockchain Observatory and Forum" Unternehmen sogenannte „business-to-business"-Anwendungen. Demnach sollte jedes Unternehmen die personenbezogenen Daten ihrer Nutzer separat von der Blockchain, off-chain, speichern und die Blockchain-Technologie stattdessen nutzen, um mit anderen Unternehmen schneller und kostengünstiger Geschäfte abzuschließen, ohne die Details einer Benutzertransaktionen in der Blockchain zu veröffentlichen.[77]
Im Ergebnis kann keine einheitliche datenschutzrechtliche Beurteilung von Verarbeitungsvorgängen auf der Blockchain vorgenommen werden. Die zahlreichen Möglichkeiten der technischen Ausgestaltung von Blockchain-Lösungen führen zu ebenso unterschiedlichen rechtlichen Implikationen. Im Standardfall einer öffentlich einsehbaren Blockchain müsste man zu dem Schluss kommen, dass personenbezogene Daten nicht verarbeitet werden dürfen, da es unmöglich scheint, allen Anforderungen der DSGVO gerecht zu werden. Auf der anderen Seite folgt die DSGVO einem technologieneutralen Ansatz und hat nicht die Zielsetzung, Innovation und technologischem Fortschritt im Weg zu stehen. Wie so oft konnte augenscheinlich im Rahmen des Gesetzgebungsprozesses nicht jede erdenkliche Entwicklung vorausgesehen werden. Auch dann, wenn sich Innovation schon innerhalb dieses Zeitraums abzuzeichnen beginnt, ist die Reaktion des Gesetzgebers meist träge, was nicht völlig unverständlich ist. Praktische Entwicklungen können bekanntermaßen in verschiedene Richtungen verlaufen. Wünschenswert wäre demnach eine Klarstellung der EDSA oder eine *lex specialis* für Blockchain-Anwendungen. Grundsätzlich sind auch die Vertragserfüllung und die berechtigten Interessen des Verantwortlichen als zulässige Rechtsgrundlage solcher Datenverarbeitungen durchaus denkbar. Lediglich im Rahmen der Betroffenenrechte müsste eine leichte Modifikation vonstattengehen oder müssten die Anforderungen etwas abgeschwächt werden. Der Blockchain Bundesverband in Deutschland vertritt etwa die Forderung, bestimmte Formen der Kryptografie als sichere Verschlüsselungsmethoden mit Anonymisierungsfunktion anzuerkennen, was datenschutzrechtliche Probleme in diesem Zusammenhang (zumindest auf den ersten Blick) gänzlich beseitigen würde.[78]

77 *The European Union Blockchain Observatory and Forum*, Blockchain and the GDPR, https://www.eublockchainforum.eu/reports (S 29, Stand 16.10.2018).

78 *Hein/Wellbrock/Hein*, Blockchain-Anwendungen 32.

Ist die Blockchain von Beginn an dazu gedacht, personenbezogene Daten zu speichern, kann die Problematik durch entsprechende Vorkehrungen in der Entwicklungsphase entschärft und eine DSGVO-konforme Datenverarbeitung durch aufgezeigte Lösungsmodelle verwirklicht werden. Alleine durch eine einfache Veranschaulichung wie „Die Blockchain tut nur das, was ihr aufgetragen wurde", kann leicht das Potential derselben begreiflich gemacht werden, nicht nur datenschutzrechtlich zulässig eingesetzt zu werden, sondern auch zur Verbesserung und transparenteren Ausgestaltung des Datenschutzes selbst beizutragen.

Angesichts der Empfehlungen einiger Datenschutzbehörden und der derzeitigen Unmöglichkeit, beim Einsatz der Blockchain-Technologie allen Rechten und vor allem Pflichten der DSGVO vollinhaltlich nachzukommen, gilt es, Entscheidungen der EDSA, der nationalen Datenschutzbehörden sowie weitere Judikatur abzuwarten, um die Kompatibilität der Blockchain mit der DSGVO weiter zu konkretisieren.

Korrespondenz: Dr. Arthur Stadler,
arthur.stadler@svlaw.at; Mag. Jacqueline Bichler,
jacqueline.bichler@svlaw.at.