Blockchain und Datenschutz

von Erik Tröber

Open Peer Review
Dieser Beitrag wurde lektoriert von: Michelle Duda, Isabel Lihotzky und Hendrik Scheja

Erik studiert Jura an der Universität zu Köln und ist studentische Hilfskraft im Bereich des Datenschutzrechts bei Loschelder Rechtsanwälte.

A. Einleitung

Die Blockchain-Technologie wird immer mehr integraler Bestandteil der Digitalisierung.[1] So werden heute bereits die Supply Chains der Lebensmittelindustrie durch Blockchain-Technologie überwacht. Auch DAX-Konzerne kommen nicht mehr um den Einsatz dieser Technologie herum:[2] Vonovia, der größte Wohnungsverwalter Deutschlands, hat vor kurzem das erste Mal eine vollständige Schuldverschreibung auf der Blockchain ausgegeben.[3] Doch was passiert mit den Daten, die sich auf der Blockchain befinden? Wer schützt sie und welche Probleme treten dabei in Bezug auf personenbezogene Daten auf?

Dieser Artikel befasst sich mit der Anwendung des Datenschutzrechts, insbesondere der DSGVO, auf die Blockchain-Technologie und den damit einhergehenden Herausforderungen sowie zu erwartenden Fragen.

1 *Frink*, CTRL 1/2021, 15 f.; *Dischinger*, CTRL 1/2021, 18 f.
2 *Kamath*, Food Traceability on Blockchain: Walmart's and Mango Pilots with IBM, hier abrufbar (Stand: 25.05.21).
3 Heinz, Vonovia emittiert digitale Schuldverschreibung durch Security Token, hier abrufbar (Stand: 25.05.21).

B. Anwendbarkeit des Datenschutzrechts

Die Vorschriften des Datenschutzrechts finden nur auf Daten Anwendung, welche einen Personenbezug aufweisen. Nach der Legaldefinition aus Art. 4 Nr.1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Es stellt sich zunächst die Frage, welche Art von Daten bei der Nutzung von Blockchain-Technologien verarbeitet werden und ob deswegen die Vorschriften des Datenschutzes Anwendung finden.
Als Beispiel werden in der Bitcoin-Blockchain transparent in digitalen Transaktionslisten sämtliche Transaktionen, die im System der Blockchain durchgeführt werden, gespeichert.[4] Es werden dabei zwar keine Daten wie Vor- und Nachname oder sonstige direkt identifizierbaren Daten übertragen. Jedoch werden bei jeder Transaktion, welche nur von einem Wallet zu einem anderen Wallet funktioniert, die Identifikationsnummern der Wallets abgespeichert. Unter einem Wallet versteht man eine elektronische Brieftasche, vergleichbar mit einem Bankkonto. Nur durch diese Speicherung dieser Nummern kann die Richtigkeit der getätigten Transaktion validiert werden.
Ob durch solche Identifikationsnummern eine Person identifizierbar, also bestimmbar ist, ist sowohl auf nationaler als auch auf europäischer Ebene umstritten.
Auf nationaler Ebene werden zwei Ansätze zur Bestimmbarkeit von personenbezogenen Daten vertreten. Der objektive Ansatz sieht einen Personenbezug schon dann, wenn die hypothetische Möglichkeit besteht, dass eine beliebige Stelle, die hinter den Daten stehende Person mit verhältnismäßigen Mitteln bestimmen kann.[5] Hiernach wären alle Wallet-Adressen personenbeziehbar, denn zumindest der Inhaber kennt seine Identität.[6] Demgegenüber liegt nach dem relativen Ansatz ein Personenbezug vor, wenn die jeweils konkret verantwortliche Stelle mit den ihr tatsächlich zur Verfügung stehenden Möglichkeiten ohne unverhältnismäßigen Aufwand den Bezug selbst herstellen kann.[7]

Das AG Berlin-Mitte schloss sich im Ergebnis dem objektiven Ansatz an.[8] Der BGH legte die Frage dem EuGH vor.[9]

Der EuGH entschied im Jahr 2016, dass es beim Vorliegen dynamischer IP-Adressen darauf ankäme, ob die verantwortliche Stelle mit den ihnen zur Verfügung stehenden Mitteln in der Lage sei, die betreffenden Angaben einer bestimmten Person zuzuordnen.[10] Aus Art. 4 Nr. 1 2. Hs. DSGVO und aus dem Erwägungsgrund 26 ergibt sich, dass es keiner direkten Identifizierung bedürfe, um das Vorliegen von personenbezogenen Daten zu bejahen. Es sei vor allem nicht nötig, dass die Information zur Bestimmung der Person einem Dritten zur Verfügung stehe. Der Ansatz wird als „verschärfter" relativer Personenbezug bezeichnet.[11] Die Beurteilung, welche Mittel vernünftigerweise in Betracht kommen, bleibt allerdings weiterhin unklar. Der EuGH scheint diese Beurteilung bewusst in das Ermessen der einzelnen Mitgliedsstaaten zu stellen.

Dabei wird für die Frage der Verhältnismäßigkeit des zu betreibenden Aufwandes neben den wirtschaftlichen Erwägungen auch zu berücksichtigen sein, welche Sensibilität den jeweiligen Daten zukommt.[12]

Bei der Anwendung der DSGVO auf die Bitcoin-Blockchain könnte im Hinblick auf die Speicherung der Daten von einer Pseudonymisierung der Daten ausgegangen werden.[13]

Eine Pseudonymisierung von Daten schließt das Vorliegen von personenbezogenen Daten nicht aus. Gemäß Art. 4 Nr. 5 DSGVO ist Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Von der Pseudonymisierung ist die Anonymisierung zu unterscheiden. Eine Anonymisierung der Daten liegt dann vor, wenn die personenbezogenen Daten derart verändert werden, dass die dahinterstehende Person

4 Alle Transaktionen des Bitcoins hier abrufbar (Stand: 24.05.21).
5 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 5. Aufl. 2016, § 3 Rn. 13; *Pahlen-Brandt*, DuD 2008, 34, 36.
6 *Kaulartz*, CR 2016, 474; *Hofert*, TD 2017, 161 (163).
7 *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 3 Rn. 10; Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff personenbezogene Daten, hier abrufbar (Stand 25.05.21).
8 AG Berlin-Tiergarten, 13.08.2008 - 2 C 6/08, datenspeicherung.de (Stand 27.05.21).
9 BGH, VersR 2015, 370.
10 EuGH, C-582/14 - Breyer.
11 Ebd.
12 *Schefzig*, K&R 2014, 772, 774; *Hofert*, ZD 2017, 161, (163).
13 *Ernst* in: Paal/Pauly, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 40.

nicht mehr identifiziert werden kann.[14] Von einer Anonymisierung kann auch dann gesprochen werden, wenn die an sich pseudonymisierten Daten von der verarbeitenden Stelle nur mit einem unverhältnismäßig großen Aufwand einer bestimmbaren Person zugeordnet werden können.[15]

Vor dem Hintergrund der Nutzung und Verfügbarkeit von *Big Data* ist fraglich, ob die Identifizierung der Person einen nicht unerheblichen Aufwand darstellt. Kryptowährungen gewinnen immer mehr an Beliebtheit und Marktgängigkeit. Durch die Schnittstellen zwischen dem genutzten Blockchain-System und dem Drittnutzer können Verbindungen z.B. zwischen Liefer-/ Rechnungsadresse dargestellt werden.[16] Selbst wenn man vermeintlich „sicher" ohne Angaben persönlicher Daten bezahlt, ist eine Identifizierung mittels *Big Data* möglich.[17]

Die versendeten Daten werden immer bestimmbarer und der Aufwand zur Identifizierung immer geringer. Das dürfte im Ergebnis dazu führen, dass es in der Regel immer mehr personenbezogene Daten bei der Verarbeitung in den verwendeten Blockchains geben wird. Der Anwendungsbereich ist in diesen Fällen eröffnet.

C. Zulässigkeit der Verarbeitung

Im nächsten Schritt stellt sich die Frage, in welchen Fällen die Verarbeitung personenbezogener Daten durch die Blockchain-Technologie überhaupt zulässig ist.

Die Datenverarbeitung ist nur dann zulässig, wenn ein Legitimationsgrund vorliegt. Man spricht von einem Verbot mit Erlaubnisvorbehalt.[18] Einen Katalog an Erlaubnistatbeständen für die Verarbeitung findet sich in Art. 6 DSGVO.

In Betracht kommt zunächst die Einwilligung als möglicher Erlaubnistatbestand gemäß Art. 6 Abs. 1 S. 1 lit. a DSGVO. Eine Einwilligung nach Art. 4 Nr. 11 DSGVO ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Erwägungsgrund 42 stellt zudem die Anforderung, dass die betroffene Person zumindest in der Lage sein muss, zu erkennen, wer Verantwortlicher für die Datenverarbeitung ist und welche personenbezogenen Daten verarbeitet werden. Vor dem Hintergrund, dass bei öffentlichen Blockchains meist nicht klar ist, wer Verantwortlicher ist und in welches Land die Daten zu den Nodes übertragen werden, ist eine informierte Einwilligung bei öffentlichen Blockchains kaum möglich.[19] Unter einem Node versteht man Knotenpunkte in einem dezentralen Netzwerk, durch den die Teilnehmer direkt miteinander (*peer-to-peer*) interagieren können.[20]

In Betracht kommt jedoch der gesetzliche Erlaubnistatbestand des überwiegenden Interesses aus Art. 6 Abs. 1 lit. f. DSGVO. Ein überwiegendes Interesse liegt dann vor, wenn die Interessen des Betroffenen die Interessen der verarbeitenden Stelle überwiegen. Dabei wird eine Abwägung insbesondere im Hinblick auf die Grundrechte und Grundfreiheiten des Betroffenen vorgenommen.[21] Das überwiegende Interesse der verarbeitenden Stelle könnte hier in der Speicherung von Daten liegen, die zur Sicherheit und Vertrauenswürdigkeit der Blockchain maßgeblich beitragen. Ein schützenswertes Interesse des Betroffenen fehlt in diesem Falle, da er die Blockchain freiwillig nutzt und seine Daten anonymisiert verarbeitet werden.[22]

Im Bereich der zulassungsbeschränkten Blockchains kommt zudem die Erforderlichkeit zur Vertragserfüllung gemäß Art. 6 Abs. 1 lit. b DSGVO in Betracht, wenn Gegenstand des Vertrages die Nutzung einer Blockchain ist.[23]

14 Ebd. Rn. 48.
15 *Ernst* in: Paal/Pauly, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 50.
16 *Jo Pesch*, Blockchain, Smart Contracts und Datenschutz Risiken und Grenzen Blockchain-basierter Smart Contracts, hier abrufbar (Stand 23.05.21); *Bechtolf/Vogt*, ZD 2018, 66; *Guggenberger*, ZD 2017, 49, (50).
17 Vgl. zu Bitcoin Transaktionen: *Reid/Harrigan*, hier abrufbar (Stand 23.05.21); *Jawaheri/Basil*, Deanonymizing tor hidden service users through bitcoin transactions analysis – abstract, hier abrufbar (Stand 26.05.21).
18 *Buchner/Petri* in: Kühling/Buchner, 3. Aufl. 2020, DSGVO Art. 6 Rn. 11.
19 BITKOM, Faktenpapier Blockchain und Datenschutz, hier abrufbar (Stand: 03.05.21) danach abgekürzt „BITKOM".
20 *Frink*, CTRL 1/2021, 15 f.
21 *Wolff* in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Auflage 2017, Rn. 648.
22 BITKOM, 31.
23 Ebd.

Folglich dürfte in der Regel auf den Erlaubnistatbestand des überwiegenden Interesses aus Art. 6 Abs. 1 lit. f DSGVO oder aber auf die Verarbeitung der Daten zur Vertragserfüllung gemäß Art. 6 Abs. 1 lit. b DSGVO abgestellt werden können.

D. Verantwortlichkeit

Entscheidend ist, wer bei einer Blockchain für die Verarbeitung der Daten verantwortlich ist. Wenig hilfreich ist insoweit das Prinzip einer Blockchain, nach dem die Daten dezentral gespeichert und verarbeitet werden und nicht an einer Stelle zentral gespeichert und verarbeitet werden, wie zum Beispiel bei *Facebook*.

Eine Verantwortlichkeit der Programmierer entfällt bereits bei Veröffentlichung der Blockchain, da die nach Art. 4 Nr. 7 DSGVO für den Verantwortlichen nötige Kontrolle über Art und Zweck der Verarbeitung verloren geht.[24] Auch die Miner und die Nutzer, die eine Transaktion vornehmen, haben keine Kontrolle über Zwecke und Mittel der Verarbeitung.[25] Letztlich kommt nur noch der Betreiber einer Node als Verantwortlicher i. S. d. DSGVO in Betracht.

Jeder Betreiber einer Node erhebt, speichert und verarbeitet Daten, sobald die Informationen an die anderen Nodes übertragen werden.[26] Sie verfolgen auch einen Zweck: die Teilnahme am Netzwerk.[27] Sofern diese Daten einen Personenbezug aufweisen, ist der Betreiber einer Node deshalb Verantwortlicher i. S. d. DSGVO.[28] Darüber hinaus könnten die Betreiber der Nodes auch eine gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO für die Verarbeitung haben.
Gemäß Art. 26 Absatz 1 Satz 1 DS-GVO liegt eine gemeinsame Verantwortlichkeit vor, wenn zwei oder mehrere Verantwortliche gemeinsam die Mittel und Zwecke der Verarbeitung festlegen.[29] Die Betreiber einer Node legen jedoch in der Regel nicht gemeinsam Mittel der Verarbeitung fest. Ein Betreiber einer Node hat typischerweise keinen Einfluss auf die Art und Weise der Datenverarbeitung bei den anderen Knoten des Netzwerkes.[30]

Folglich fehlt es hier in der Regel an einer gemeinsamen Verantwortlichkeit i. S. d. Art. 26 DSGVO.[31]

Trotzdem bleibt der einzelne Betreiber der Node alleiniger Verantwortlicher, insbesondere ist er unabhängig von einer gemeinsamen oder alleinigen Verantwortlichkeit Adressat für beispielsweise die Durchsetzung der Betroffenenrechte.[32]

E. Betroffenenrechte und Informationspflichten

Die DSGVO und das BDSG stellen dem Betroffenen verschiedene Rechte zur Seite, mit denen er über seine Daten beim Verantwortlichen verfügen kann.

Art. 17 DSGVO beinhaltet das Recht auf Löschung der Daten (Abs. 1) und das Recht auf Vergessenwerden (Abs.2). Das Recht auf Löschung der Daten verpflichtet den Verantwortlichen die personenbezogenen Daten unverzüglich zu löschen.
Das Recht auf Vergessenwerden, welches sich maßgeblich aus Art. 8 und 9 EU-GRCh ableitet, geht darüber hinaus und verlangt vom Verantwortlichen, dass im Falle der Veröffentlichung personenbezogener Daten Dritte über das Löschungsverlangen in Kenntnis gesetzt werden.[33]
Dagegen hat das BVerfG das Recht auf Vergessenwerden aus dem Allgemeinen Persönlichkeitsrecht abgeleitet.[34] Eine Veröffentlichung der Daten ist im Falle der zulassungsfreien Blockchains gegeben, sodass der Verantwortliche dem Recht auf Vergessenwerden nachkommen muss.

Problematisch erscheint insoweit, dass die Blockchain auf der Grundidee der Unveränderbarkeit der Daten basiert. Die Unveränderbarkeit trägt zum Vertrauen in die Blockchain-Technologie bei und sorgt dafür, dass Intermediäre nicht notwendig sind.[35] Ist ein Block in der Blockchain einmal validiert, so ist eine Löschung der Informationen praktisch nicht mehr möglich.[36]
Ein Recht auf Löschung oder auf Vergessenwerden ist insoweit technisch nicht umsetzbar.

24 *Martini/Weinzierl*, NVwZ 2017, 1251 (1253).
25 Anders *Schrey/Thalhofer*, NJW 2017, 1431.
26 *Martini/Weinzierl*, NVwZ 2017, 1251 (1253).
27 Geht es dabei um persönliche und familiäre Zwecke, so ist die DSGVO gemäß Art. 2 Abs. 2 lit. c DSGVO nicht anwendbar.
28 *Martini/Weinzierl*, NVwZ 2017, 1251 (1254); *Schrey/Thalhofer*, NJW 2017, 1431.
29 BITKOM, 28 f.
30 *Martini/Weinzierl*, NVwZ 2017, 1251 (1254).
31 So BITKOM; a.A. *Schrey/Thalhofer*, NJW 2017, 1431.
32 BITKOM, 29.
33 Ebd.
34 BVerfG, NJW 2020, 314.
35 *Bechtolf/Vogt*, ZD 2018, 66.
36 Ebd.

Will man die Blockchain-Technologie und ihre Vorteile nutzen, müssen Betroffene akzeptieren, dass diese Rechte nicht gewährt werden können.
Im Rahmen der zulassungsbeschränkten Blockchains dürfte allerdings in der Abwägung der Gedanke zu berücksichtigen sein, dass das Datenschutzrecht kein „Supergrundrecht" ist.[37]
Der Löschungsanspruch würde die Existenz der gesamten Blockchain gefährden, da ansonsten die Löschung den Weiterbetrieb der Nodes unmöglich machen würde. So müsste eine Interessenabwägung zugunsten der verantwortlichen Node-Betreiber ausfallen.[38]
Insoweit sollte sich der Nutzer im Vorhinein der Unveränderbarkeit im Klaren sein.
Auch der Anspruch auf Berichtigung oder Korrektur gemäß §§ 20 Abs. 1, 35 Abs. 1 BDSG, Art. 16 DSGVO ist insoweit problematisch.
Die Berichtigung der Daten gemäß Art. 16 S. 1 DSGVO beinhaltet den Anspruch, unrichtige personenbezogene Daten zu berichtigen.[39]
Unter dem Anspruch der Korrektur aus Art. 16 S. 2 DSGVO versteht man den Anspruch auf Vervollständigung der personenbezogenen Daten. Vor dem Hintergrund der Unveränderbarkeit sind auch diese Ansprüche grundsätzlich auf der Blockchain nicht umsetzbar.
Es gibt jedoch bereits mehrere Ansätze, eine Berichtigung oder Korrektur zu ermöglichen.
In Betracht kommen beispielsweise sogenannte *Reversed Transactions*. Bei *Reversed Transactions* werden so lange fiktive Transaktionen ausgeführt, bis der Status der Blockchain wieder inhaltlich korrekt ist.[40] Zwar bleiben die personenbezogenen Daten dabei in der Blockchain erhalten, jedoch könnten so zumindest die Daten zu einem späteren Zeitpunkt berichtigt bzw. korrigiert werden. Im Ergebnis führt dies jedoch nicht dazu, dass ein Anspruch auf Berichtigung oder Korrektur vollständig durchgesetzt werden kann. Es kann nur von einer „Gegendarstellung" als Korrektur gesprochen werden.[41]
Die Durchsetzung der Betroffenenrechte des einzelnen Nutzers ist schwierig, da der Einfluss des einzelnen Teilnehmers häufig so gering sein dürfte, dass eine Realisierung von Betroffenenrechten in fast allen Fällen ausgeschlossen erscheint.[42]
Auch die Aufsichtsbehörden stehen bei der Durchsetzung von Auskunftsansprüchen vor ungelösten Problemen.[43]
Die fehlende Durchsetzbarkeit von Betroffenenrechten wurde bereits im Zuge des BDSG und der DS-RL kritisiert.[44]

F. Ausblick

Ungeachtet der Probleme, die das Datenschutzrecht in Verbindung mit der Blockchain aufwirft, besonders in Bezug auf das Recht auf Vergessenwerden, bieten sich hier auch Chancen für den Datenschutz. Unter anderem gibt es Ansätze, ein Identitätsmanagement basierend auf einer Blockchain zu erschaffen.[45]
Die Idee ist, dass die Nutzer ihre physischen Identitäten in der Blockchain speichern und selbst darüber verfügen können, ob etwa Firmen oder Behörden Zugriff auf die Daten haben sollen. Anschließend könnte der Zugriff auf die Daten auch wieder entzogen werden. Der Einzelne hätte so die Möglichkeit die Kontrolle über seine Daten zurückzuerlangen.
Abschließend kann festgehalten werden, dass das Potenzial der Blockchain-Technologie trotz datenschutzrechtlicher Unsicherheiten sehr groß ist. Abzuwarten bleibt, ob der Gesetzgeber spezifische Betroffenenrechte einführt, die auf Blockchains technisch umsetzbar sein werden. In Betracht käme hier die Schaffung eines Rechts auf die Pseudonymisierung der Daten für zulassungsfreie Blockchains.[46]

Talking Legal Tech - Folge 5:
„was ist die blockchain,
florian glatz?"

37 *Veil*, NVwZ 2018, 686.
38 BITKOM, 33.
39 *Reif* in: Gola DS-GVO, 2. Aufl. 2018, DS-GVO, Art. 16 Rn. 11.
40 *Schrey/Thalhofer*, NJW 2017, 1431.
41 Vgl. zu Transaktionen: *Schrey/Thalhofer*, NJW 2017, 1431.
42 *Bechtolf/Vogt*, ZD 2018, 66.
43 Mehr zur Problematik mit Aufsichtsbehörden BITKOM, 29.
44 *Bechtolf/Vogt*, ZD 2018, 66.
45 *Gipp/Mienert*, ZD 2017, 514.
46 *Martini/Weinzierl,* NVwZ 2017, 1251 (1255).

2/21

1. Jahrgang, 2. Ausgabe
www.legaltechcologne.de/ctrl

CTRL

Cologne Technology Review & Law

+

Hier geht es zur ganzen Ausgabe.

Dort findest du auf über 100 Seiten in 15 Aufsätzen alles von NFTs über Legal Tech im Strafprozess bis hin zum Stand des E-Examens in NRW.

LTLC
LEGAL TECH LAB COLOGNE