ecolex

FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT

JULI 2019

07

www.ecolex.at

561 – 652

Rsp-Nr 243 – 282

Kollektiver Rechtsschutz

Österreich Deutschland im Wettlauf

Kick-back-Provision für Herrn und Knecht

Wissenszurechnung gegen „chinese walls“

Recht smart – RL digital zum Vertragsinhalt

Fehlerbestimmung

Totengesang für den

Unabhängigen Untersuchungsrichter

Änderung Unternehmensstruktur

Verzichtsmöglichkeiten

Kartellschadenersatzrecht

Konzernhaftung?

DSGVO-Geldbußen

Gegen den Betriebsrat?

Investitionsschiedsgerichtsbarkeit – CETA

Verrichterlichung des ISDS?

Datenschutz und Blockchain: Ein unauflösbares Dilemma?

Die Blockchain wird von vielen als revolutionäre Zukunftstechnologie gefeiert. Im letzten Jahr erfuhr sie durch die Datenschutz-Grundverordnung (DSGVO) allerdings einen Dämpfer: Beide Konzepte sind nämlich nur schwer in Einklang zu bringen. Es stellen sich einige bislang weitgehend ungeklärte datenschutzrechtliche Fragen.

AXEL ANDERL / DOMINIK SCHELLING

A. Problemaufriss

Die Blockchain ist eine in einem Netzwerk verteilte Datenbank. Ihre einzelne Datensätze sind durch ein

Dr. *Axel Anderl,* LL. M. (IT-Law), ist Partner bei DORDA Rechtsanwälte GmbH und leitet das IT/IP und Datenschutz Team sowie die Digital Industries Gruppe der Kanzlei. Mag. *Dominik Schelling* ist Rechtsanwaltsanwärter in seinem Team und insb auf Datenschutzrecht, IT-Recht und Digitalisierung spezialisiert.

kryptographisches Verfahren miteinander verkettet und aneinandergereiht. Dabei werden Informationen zu Datenblöcken zusammengefasst und durch ihre digitalen Fingerabdrücke (sog *Hashes*) miteinander verknüpft. Nach der Verkettung kann der Inhalt praktisch nicht mehr manipuliert werden, weil jede Veränderung eines Blocks zu einem neuen Hashwert und damit zu einer Durchbrechung der Kette führt. Kurzum: Die Blockchain kann unendlich erweitert, aber nachträglich nicht mehr geändert werden. Die so generierte Datenkette wird schließlich nicht zentral gespeichert, sondern in einem Netzwerk verteilt. Jeder Teilnehmer verfügt über eine vollständige und laufend synchronisierte Kopie der Datenbank. Wesensmerkmale einer Blockchain sind somit va die unveränderbare Verknüpfung der Informationen miteinander und deren dezentrale Speicherung.

Diese schon seit Jahrzehnten bekannte Technologie wurde durch die Kryptowährung Bitcoin weltweit bekannt. Dezentrale und fälschungssichere Datenbanken sind aber auch für mannigfaltige andere Anwendungsbereiche und viele Branchen interessant. Technisch können auf Basis einer Blockchain etwa bereits alle möglichen Arten von Transaktionen abgewickelt, Gesellschaftsanteile verwaltet, Grundbücher geführt oder Lieferketten dokumentiert werden.

Allerdings führen gerade die beiden wesentlichen Architektur-Merkmale der Blockchain – ihre Unveränderbarkeit und Dezentralität – zu datenschutzrechtlichen Bedenken: So geht das Datenschutzrecht üblicherweise davon aus, dass es eine zentrale Stelle gibt, die die Daten verarbeitet und dafür verantwortlich ist. Dies fehlt allerdings bei der Blockchain. Außerdem forciert die DSGVO den Grundsatz der Speicherbegrenzung und das Recht auf Löschung. Eine nachträgliche Entfernung oder Veränderung von Daten ist beim Grundtypus der Blockchain allerdings nicht möglich.

Die Blockchain-Technologie und die DSGVO sind daher auf den ersten Blick nicht wirklich kompatibel. Dieser Beitrag zeigt Lösungsansätze für dieses Spannungsverhältnis auf.

B. Anwendbarkeit des Datenschutzrechts

Die DSGVO ist nur auf die Verarbeitung personenbezogener Daten natürlicher Personen anwendbar.[1] Es stellt sich daher die Vorfrage, ob in der Blockchain *„personenbezogene Daten"* verarbeitet werden. Dieser Begriff ist sehr weit auszulegen und umfasst alle Informationen, die sich auf eine direkt oder indirekt identifizierte oder identifizierbare natürliche Person (den Betroffenen) beziehen.[2] Maßgebend ist, ob eine bestimmte Person auf Basis der jeweiligen Daten zumindest ermittelbar ist – selbst wenn dafür weitere Informationen oder Zusatzwissen Dritter erforderlich ist.[3] In diesem Sinne sind auch bloße Kennnummern in der Onlinewelt als personenbezogene Daten zu qualifizieren.[4]

In der Blockchain werden häufig keine unmittelbar personenbezogenen Daten gespeichert und treten die Teilnehmer nicht mit ihren Klarnamen, sondern unter einer Kennnummer (sog *Keys*) auf.[5] Auf Basis der gebotenen weiten Auslegung und der strengen Rsp sind aber bereits diese *Keys* als personenbezogene Daten im Sinne des Datenschutzes zu werten.[6] Außerdem werden in der Blockchain regelmäßig weitere Informationen verarbeitet – etwa Datum und Zeitpunkt des Eintrags und Details zur jeweiligen Aktivität bzw Transaktion – und die IP-Adresse mitgespeichert.[7] Aus diesen Informationen kann oft auf die dahinterstehenden Akteure geschlossen werden.[8] Somit ist es auch unter Hinzuziehung zusätzlicher Informationen möglich, die Person hinter einem *Key* zu identifizieren.

Aus diesen Gründen ist die DSGVO unabhängig vom konkreten Inhalt *grds auf jede Blockchain anwendbar.*[9] Eine komplett anonyme Datenkette ist praktisch nicht vorstellbar. Datenschutzrechtliche Erwägungen sind somit bei allen Blockchain-Anwendungen zu berücksichtigen.

C. Datenschutzrechtliche Rollenverteilung

Bei der Blockchain als verteilte Datenbank tragen alle Teilnehmer und die sog *Miner* zur Datenverarbeitung bei: Die Teilnehmer, indem sie den Inhalt der Datensätze generieren (zB eine Transaktion anlegen) bzw die Datenbank auf ihrem Rechner speichern. Die Miner, indem sie den Datenblock (also zB mehrere Transaktionen) validieren und der Kette anhängen.[10]

1. Rolle der Teilnehmer

Die Blockchain-Teilnehmer entscheiden völlig eigenständig darüber, ob sie das Netzwerk nutzen, welches Ziel sie damit verfolgen, welche Daten sie damit verarbeiten und mit welcher Infrastruktur sie auf die Blockchain zugreifen.[11] Aufgrund ihrer faktischen Einflussmöglichkeit auf die Verarbeitung personenbezogener Daten in der Blockchain sind sie daher

1) Vgl zum nicht mehr bestehenden Schutz von Daten juristischer Personen *Anderl/Hörlsberger/Müller,* Kein einfachgesetzlicher Schutz für Daten juristischer Personen, ÖJZ 2018, 14.
2) *Hübl/Schmidl* in *Gantschacher/Jelinek/Schmidl/Spanberger,* Kommentar zur DSGVO (2017) Art 4 Rz 2.
3) ErwGr 26 DSGVO; Art-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136 (16); EuGH C-582/14 *(Breyer).*
4) Vgl ErwGr 30 DSGVO.
5) *Bechtolf/Vogt,* ZD 2018, 66.
6) CNIL, 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 (abgefragt am 27. 5. 2019).
7) *Biryukov/Khovratovich/Pustogarov,* Deanonymisation of clients in Bitcoin P2P network.
8) So auch *Satoshi Nakamoto,* Bitcoin: A Peer-to-Peer Electronic Cash System: *„Some linking is still unavoidable . . ."*, https://bitcoin.org/bitcoin.pdf (abgefragt am 27. 5. 2019).
9) So etwa auch *Krupar/Strassemeyer,* DSRITB 2018, 343; *Bechtolf/Vogt,* ZD 2018, 66; *Böhme/Pesch,* DuD 2017, 473; *Jakúbek/Panic,* MR 2018, 255; *Schrey/Thalhofer,* NJW 2017, 1431; *Martini/Weinzierl,* NVwZ 2017, 1251; *Erbguth/Fasching,* ZD 2017, 560; *Gorzala/Hanzl,* RdW 2018/368.
10) In weiterer Folge wird lediglich auf die beiden zentralen und in der Praxis relevantesten Rollen der Blockchain-Teilnehmer und -Miner eingegangen.
11) Vgl Art-29-Datenschutzgruppe, WP 169, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", 17.

grds jeder für sich als eigenständige *Verantwortliche* nach Art 4 Z 7 DSGVO zu qualifizieren.[12] Auch die ungarische und die französische DSB kommen zu diesem Ergebnis.[13]

Eine gemeinsame Verantwortlichkeit iSd Art 26 DSGVO scheidet dagegen regelmäßig aus, weil die Teilnehmer meist nicht bewusst und gewollt zusammenwirken.[14] Etwas anders gilt nur, wenn die Teilnehmer ausnahmsweise ein gemeinsames Ziel verfolgen. Das kann etwa bei einer konzernweiten oder von mehreren Unternehmen betriebenen Blockchain der Fall sein. Bei solchen privaten (dh geschlossenen oder permissioned) Blockchains sind die Teilnehmer üblicherweise als *gemeinsame Verantwortliche* zu qualifizieren.[15]

2. Rolle der Miner

Miner haben auf den eigentlichen Inhalt der Blockchain grds keinen Einfluss. Ihre Tätigkeit erschöpft sich darin, die von den Teilnehmern stammenden Einträge zu validieren und neue Blöcke zu errechnen – kurzum, Rechenleistung zur Verfügung zu stellen. Dabei verfolgen sie eigene Zwecke bei der Datenverarbeitung. Weiters sind sie idR an keine Weisungen der Blockchain-Teilnehmer gebunden. In der Praxis kennen sich die Akteure oft gar nicht. Im Übrigen entscheiden sie völlig frei darüber, welche Mittel sie zur Verarbeitung verwenden, also bspw welche Hardware sie für das Mining einsetzen. Im Ergebnis sind Miner daher idR als eigenständige *Verantwortliche* zu qualifizieren.[16]

Etwas anderes gilt allerdings bei beauftragten Minern. So kann es bspw bei zulassungsbeschränkten Blockchains – etwa einem staatlichen Grundbuch oder einer von einem Unternehmenskonsortium betriebenen Anwendung – vorkommen, dass die Betreiber nur Rechenleistung zukaufen. In dieser Konstellation werden Miner regelmäßig an Weisungen der Teilnehmer gebunden. Sie sind dann bloße *Auftragsverarbeiter* nach Art 4 Z 8 DSGVO.[17] In diesem Sinne geht auch die französische DSB davon aus, dass Miner nur *„in some cases"* – wenn sie im Einzelfall an die Weisungen der Verantwortlichen gebunden sind – Auftragsverarbeiter sind.[18] Die Weisungsgebundenheit ist damit das entscheidende Kriterium.

3. Ausnahme für Privatpersonen

Das Datenschutzrecht ist auf die Verarbeitung von Daten *„durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten"* nicht anwendbar (Art 2 Abs 2 lit c DSGVO; Haushaltsprivileg).[19] Diese Ausnahme greift etwa für eine Privatperson, die ihren Onlineeinkauf mit einer Kryptowährung bezahlt, deren Eigentumsrecht an einer Liegenschaft in einem Blockchain-Grundbuch eingetragen ist oder deren Kontobewegungen von ihrer Hausbank in einer Blockchain abgespeichert werden. Mangels Anwendbarkeit der DSGVO auf diese Akteure können sie selbst daher nicht als Verantwortliche (oder Auftragsverarbeiter) qualifiziert werden. Vielmehr sind Privatpersonen, die mit einer Blockchain zu persönlichen oder familiären Tätigkeiten interagieren, stets nur *Betroffene* iSd Art 4 Z 1 DSGVO und damit zentrales Schutzobjekt der DSGVO.

4. Konsequenzen in der Praxis

Die Rollenverteilung hat erhebliche Konsequenzen für den einzelnen Akteur: Alle *Verantwortlichen* müssen sämtliche DSGVO-Pflichten erfüllen. Sie haben etwa die Rechtmäßigkeit der Datenverarbeitung sicherzustellen, Informationspflichten gegenüber den Betroffenen zu erfüllen, die Betroffenenrechte zu wahren und angemessene Datensicherheitsmaßnahmen zu implementieren. Im Übrigen haben sie ein Verzeichnis der Verarbeitungstätigkeiten zu erstellen sowie ggf eine Datenschutz-Folgenabschätzung durchzuführen und etwaige Datenschutzverletzungen erforderlichenfalls an die zuständige Aufsichtsbehörde zu melden. Zudem müssen die Verantwortlichen mit ihren jeweiligen *Auftragsverarbeitern* eine Vereinbarung nach Art 28 DSGVO abschließen.[20] Im Fall der *gemeinsamen Verantwortlichkeit* bedarf es zudem einer Vereinbarung nach Art 26 DSGVO, deren wesentlicher Inhalt den Betroffenen zur Verfügung gestellt werden muss.

Sämtliche datenschutzrechtliche Anforderungen und insb der Abschluss entsprechender Vereinbarungen lassen sich in der Praxis bei einer geschlossenen Blockchain wesentlich leichter umsetzen als bei einem offenen System, an dem jeder teilnehmen kann. Bei *geschlossenen* Blockchains kann die Rollenverteilung einfacher geklärt und damit die DSGVO-Compliance besser sichergestellt werden. So können dort bspw die wesentlichen Regelungsinhalte in AGB abgebildet werden, die jeder Teilnehmer bzw Miner bei seiner Zulassung zum System akzeptiert.[21]

D. Datenübermittlung in Drittländer

Im Rahmen von Blockchain-Anwendungen kommt es oftmals zu Datenübermittlungen an Empfänger außerhalb des EWR. So etwa bei *public* Blockchains, an denen jeder teilnehmen kann, sowie bei *private* Blockchains mit Teilnehmern bzw Minern aus Drittländern. Ein solcher internationaler Datentransfer ist nach Art 44 ff DSGVO nur dann zulässig, wenn *„geeignete Garantien"* getroffen werden.

Bei *privaten* Blockchains kommt in der Praxis va der Abschluss von Standarddatenschutzklauseln nach

12) *Bechtolf/Vogt,* ZD 2018, 66; *Schrey/Thalhofer,* NJW 2017, 1431; *Martini/Weinzierl,* NVwZ 2017, 1251; *Erbguth/Fasching,* ZD 2017, 560; *Jakúbek/Panic,* MR 2018, 255.

13) 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 (abgefragt am 27. 5. 2019); CNIL (FN 6).

14) *Böhme/Pesch,* DuD 2017, 473; *Martini/Weinzierl,* NVwZ 2017, 1251.

15) Vgl *Gorzala/Hanzl,* RdW 2018/368; CNIL (FN 6).

16) Aa etwa *Erbguth/Fasching,* ZD 2017, 560; *Martini/Weinzierl,* NVwZ 2017, 1251.

17) *Martini/Weinzierl,* NVwZ 2017, 1251.

18) CNIL (FN 6).

19) ErwGr 18 DSGVO.

20) Diese Verpflichtung trifft den Verantwortlichen und den Auftragsverarbeiter gleichermaßen; s dazu auch https://www.heise.de/newsticker/meldung/DSGVO-5000-Euro-Bussgeld-fuer-fehlenden-Auftragsverarbeitungsvertrag-4282737.html (abgefragt am 27. 5. 2019).

21) *Schrey/Thalhofer,* NJW 2017, 1431.

Art 46 Abs 2 lit c DSGVO in Betracht.[22] Diese können zwischen allen Akteuren der Blockchain bspw auch über AGB vereinbart werden.

Schwieriger ist die Situation bei *public* Blockchains, sofern der Blockchain-Initiator nicht für die Einbeziehung der erforderlichen Vertragswerke gesorgt hat. Bei transaktionsbasierten Blockchains kommen insb Art 49 Abs 1 lit b und c DSGVO als Rechtsgrundlagen in Betracht. Danach ist die Datenübermittlung an Empfänger in Drittländern zulässig, sofern dies zur Vertragserfüllung erforderlich ist. Auf dieser Basis kann argumentiert werden, dass der Datenfluss an einen Miner in den USA zur Funktionsfähigkeit der Blockchain, zur Durchführung der Transaktion und damit zur Erfüllung der vertraglichen Verpflichtung des Senders eines Assets gegenüber dem Empfänger erforderlich ist.

Im Übrigen sind die in der DSGVO aufgezählten geeigneten Garantien zur Absicherung internat Datenübermittlungen nicht abschließend (arg *„können"* in Art 46 Abs 2 bzw *„insbesondere"* in Art 46 Abs 3). Daher kommen auch weitere Möglichkeiten in Betracht, um den Datentransfer in Drittländer zu legitimieren.[23] So kann bei öffentlichen Blockchains etwa argumentiert werden, dass bereits durch die Charakteristik des Systems ein angemessenes Schutzniveau erreicht wird. Schließlich werden idR gar keine direkt personenbezogenen Daten in der Datenbank zu finden sein. Mitunter ist es auch nur mit entsprechend hohem Aufwand möglich, eine konkrete Person hinter dem jeweiligen Datensatz herauszufinden. Im Übrigen kann sich jeder Betroffene gleichermaßen an die im EWR ansässigen Verantwortlichen wenden und seine Rechte gegenüber diesen entsprechend geltend machen. Der tatsächliche Sitz einzelner Verantwortlicher hat daher oft keine praktischen Auswirkungen auf die Rechte der Betroffenen und benachteiligt sie daher nicht.

Im Ergebnis können daher auch öffentliche Blockchains die Anforderungen der DSGVO an Datenübermittlungen in Drittländer erfüllen. Am Ende des Tages kommt es darauf an, die für die konkrete Anwendung passende Rechtsgrundlage zu finden und diese entsprechend zu dokumentieren.

E. Wahrung der Betroffenenrechte

Auch die vermeintliche Inkompatibilität der Blockchain mit den Rechten der Betroffenen wird oft datenschutzrechtlich kritisiert. Die Rechte auf Berichtigung (Art 16 DSGVO) und Löschung (Art 17 DSGVO) erfordern nämlich üblicherweise die tatsächliche Veränderung des Datensatzes. Bei klassischen Blockchain-Anwendungen ist das allerdings unmöglich. In der Praxis gibt es im Wesentlichen drei Ansätze, dieses Dilemma zu lösen:

Erstens kommen *Adaptionen auf technischer Ebene* in Betracht, die einzelnen Akteuren Änderungsmöglichkeiten an der Datenbank einräumen (sog *redactable* Blockchains). Dadurch geht allerdings das Grundprinzip der Unveränderbarkeit der Blockchain verloren und wird damit der Grund ihrer erhöhten Akzeptanz wegen Vertrauenswürdigkeit untergraben. Dieser in das Wesen der Blockchain eingreifende technische Lösungsansatz hat sich in der Praxis daher nicht durchgesetzt.

Zweitens bleibt eine *rechtliche Argumentation,* wonach die Blockchain-Daten auf ewige Zeit erforderlich und damit nicht löschungsreif sind oder wonach die Rechte der Betroffenen einzuschränken sind. Diese Argumente sind allerdings bisher weder gerichtlich noch behördlich erprobt und daher mit einem unüberschaubaren Risiko verbunden.

Drittens kann am eigentlichen Inhalt der Blockchain angesetzt werden: So können die in der Blockchain abgelegten Daten *pseudonymisiert* werden.[24] Dabei werden die Daten verschlüsselt und der Schlüssel zur Wiederherstellung des Personenbezugs von den eigentlichen Daten separiert. Nur der Inhaber des jeweiligen Schlüssels kann den Personenbezug wiederherstellen. Die Identifizierbarkeit des Betroffenen wird dadurch zumindest eingeschränkt.[25] Damit ein solches Pseudonymisierungsverfahren die Rechte der Betroffenen in der Blockchain datenschutzkonform wahren kann, ist erforderlich, dass der Verantwortliche

- lediglich pseudonymisierte Daten in der Blockchain speichert und
- für jeden Betroffenen einen individuellen Schlüssel zur Wiederherstellung des Personenbezugs verwendet.

Wenn nun ein Betroffener berechtigt die Löschung seiner Daten begehrt, kann der Verantwortliche den außerhalb der Blockchain aufbewahrten, individuellen Schlüssel zur Identifizierung des Betroffenen und etwaige weitere *off-chain* gespeicherte Daten löschen.[26] Dadurch ist niemand mehr in der Lage, die – weiterhin in der Blockchain integrierten Informationen – einer bestimmten Person zuzuordnen.[27] Faktisch werden die Daten in der Blockchain damit dauerhaft anonymisiert. Nach einer kürzlich ergangenen E der DSB stellt ein Entfernen des Personenbezugs ein DSGVO-konformes Mittel zur Löschung dar.[28]

In derselben Weise lässt sich auch das Recht der Betroffenen auf Berichtigung ihrer Daten wahren: So kann der Verantwortliche etwa den Datensatz berichtigten, ihn mit einem neuen Schlüssel versehen, einen neuen Block der Datenkette anhängen und den veralteten Schlüssel löschen. Damit werden die unrichtigen Daten anonymisiert, dh gelöscht. Durch die Pseudonymisierung der in der Blockchain gespeicherten Daten können somit in der Praxis die Betroffenenrechte gewahrt werden. Dementsprechend hat auch die französische DSB dieses Verfahren empfohlen.[29]

22) Vgl CNIL (FN 6).
23) *Pauly* in *Paal/Pauly,* DS-GVO Art 46 Rz 6.
24) Vgl CNIL (FN 6).
25) *Schwartmann/Weiß,* Whitepaper zur Pseudonymisierung (2017) 22 ff; Art-29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216 (24 ff); Art-29-Datenschutzgruppe (FN 7) WP 136 (21).
26) Vgl *Ibáñez/O'Hara/Simperl,* On Blockchains and the General Data Protection Regulation 8.
27) Vgl *Hansen* in *Simitis/Hornung/Spiecker,* Datenschutzrecht DSGVO Art 4 Nr 5 Rz 50.
28) DSB-D123.270/0009-DSB/2018.
29) Vgl CNIL (FN 6).

SCHLUSSSTRICH

Bei entsprechender Vorbereitung und Berücksichtigung grundlegender Parameter ist ein datenschutzkonformer Einsatz der Blockchain-Technologie möglich. Dafür muss zunächst die Rolle der Beteiligten sauber definiert und umgesetzt werden, wobei in Zweifel von eigenständigen Verantwortlichen auszugehen ist. Darüber hinaus muss ein ggf stattfindender internationaler Datentransfer an Empfänger in Drittländer DSGVO-konform ausgestaltet werden. Es ist auch ratsam, von Verschlüsselungstechniken Gebrauch zu machen, um die Rechte der Betroffenen wahren zu können. Generell ist der Einsatz privater und zulassungsbeschränkter Blockchains zu bevorzugen, weil es hier leichter möglich ist, datenschutzrechtliche Themen durch Vereinbarungen zwischen den Akteuren zu regeln (so auch das Fazit in EU Blockchain Observatory and Forum, Blockchain and the GDPR).