Smart Contracts und die DSGVO

**Welche Grenzen setzt die DSGVO der Verwendung von Smart Contracts?
Eine Betrachtung von Smart Contracts auf der Ethereum-Blockchain**

Jörn Erbguth[1]

Abstract: Über Smart Contracts auf der Ethereum-Blockchain wurden bereits Milliarden-Beträge transferiert. Allerdings wurde bislang wenig betrachtet, ob diese Abwicklung DSGVO-konform war. Dieser Beitrag erörtert, wer Verantwortliche für die Ausführung eines Smart Contracts sind. Dabei fällt auf, dass man hier je nach Gestaltung des Smart Contracts und der Situation der Vertragsparteien zu sehr unterschiedlichen Ergebnissen kommen kann. Darauf aufbauend wird die Verarbeitung personenbezogener Daten und die automatisierte Entscheidung durch einen Smart Contract betrachtet. Auch wenn das Ergebnis abhängig vom Einzelfall ist, so sind der Abschluss und die Abwicklung von Verträgen über Smart Contracts auf der Ethereum-Blockchain prinzipiell DSGVO-konform möglich.

Keywords: Smart Contracts, Blockchain, Ethereum, ADM, automatisierte Entscheidung, DSGVO, personenbezogene Daten, Verantwortlicher

1 Einleitung

Smart Contracts auf öffentlichen Blockchains wie z.B. Ethereum erlauben eine Art Treuhandfunktion. Man kann Verträge eingehen und der Smart Contract wacht darüber, dass z.B. der monetäre Transfer erst endgültig wird, wenn die Leistung auch erbracht ist. Umgekehrt können ggf. Leistungen blockiert werden, wenn die Bezahlung noch nicht erfolgt ist. Dabei bieten Smart Contracts auf der Blockchain die Sicherheit, dass die Bedingungen der Automatisierung nicht einseitig geändert werden können, wie das beispielsweise beim Digital Rights Management (DRM) der Fall ist. Im Folgenden wird betrachtet, ob die DSGVO einen Vertragsabschluss und eine Vertragsdurchführung via Smart Contract auf einer öffentlichen Blockchain wie z.B. Ethereum zulässt. Zur Frage der Vereinbarkeit von Blockchain und DSGVO kommt zudem die Problematik der automatisierten Entscheidung, welche durch Art. 22 DSGVO reguliert ist.[2]

[1] Universität Genf, Institute of Information Service Science, CUI Battelle bat A Route de Drize 7, CH-1227 Carouge Ort, joern@erbguth.net

[2] Bedanken möchte ich mich für wertvolle Anregungen von Mitgliedern der Arbeitsgruppe DIN SPEC 4997 Privacy by Blockchain Design, wobei ich besonders Katrin Kirchert und Michael Kolain hervorheben möchte.

doi:10.18420/inf2019_59

2 Rollen und Begriffe

Vorab sollen einige zentrale Begriffe und Rollen definiert werden. Bei Smart Contracts lassen sich folgende Rollen identifizieren. Dabei können mehrere Rollen in einer natürlichen oder juristischen Person zusammenfallen oder auch noch weiter differenziert werden.

Smart Contracts im Kontext von Blockchains werden hier nicht im weiten Sinne von Szabo[3] als automatisch ausgeführte Verträge verstanden. Vielmehr wird der Begriff auf solche Smart Contracts beschränkt, die Programme auf einer programmierbaren Blockchain sind und die Transaktionen ausführen.[4] Programme auf einer Blockchain, die keine Transaktionen ausführen, sind jedoch nicht mit umfasst.[5]

Die *Entwickler*in*[6] entwickelt den Code des Smart Contracts. Dies umfasst ggf. auch die Spezifikation, die Codierung und das Testen, aber nicht das Deployen auf einer produktiven Blockchain.

Die *Deployer*in* stellt den Smart Contract auf eine produktive Blockchain und macht ihn dadurch einsatzbereit. Danach ist ein Smart Contract an sich unveränderbar. Smart Contracts können jedoch so gebaut werden, dass Updates eingespielt oder sie dauerhaft deaktiviert werden können.

Die *Auftraggeber*in* beauftragt die Entwicklung und Wartung des Smart Contracts. Sie hat dazu Verträge mit der Entwickler*in und der Deployer*in.

Vertragsparteien können über Smart Contracts Verträge schließen oder/und ausführen.[7] Dabei können wie bei anderen juristischen Verträgen die Bedingungen ausgewogen oder auch recht einseitig definiert sein. Vertragsparteien können jedoch nicht den Code des Vertrages ändern. Könnte eine Vertragspartei dies, so wäre sie gleichzeitig Deployer*in.

Orakel sind Dritte, die Informationen an einen Smart Contract liefern und die dieser zur Entscheidung über Transaktionen verwendet. Orakel sind in der Regel keine Vertragsparteien.

Eine *Knotenbetreiber*in* betreibt einen Knoten der Blockchain. Sie führt dabei alle Smart-Contract-Transaktionen aus, speichert den Inhalt der Blockchain und gibt diesen weiter. Sie nimmt jedoch keinen Einfluss auf die Verarbeitung. Würde sie Einfluss auf die Verarbeitung nehmen, so würde sie aus der Blockchain ausgeschlossen werden. Etwas anderes kann im Fall einer *Hard Fork* gelten, bei dem die kollektive Abweichung zur Spaltung einer Blockchain in zwei unabhängige Blockchains führt.

[3] [Sz97] Nick Szabo, first monday, Vol. 2, Nr. 9, 1.9.1997.

[4] [Bu14] Vitalik Buterin et al., Ethereum White Paper.

[5] Siehe dazu etwa [Er18] Erbguth, 33.

[6] Es werden die mit * gegenderten Formen verwendet. Sind die weibliche und männliche Form identisch, so wird der weibliche Artikel ohne Markierung durch ein * verwendet. Gemeint sind immer alle Geschlechter.

[7] Zur Frage, in welchen speziellen Fällen sowohl Vertragsschluss als auch Festlegung des Vertragsinhalts über den Smart Contract selbst getätigt werden können, siehe beispielsweise [Dj16] Djazayeri jurisPR-BKR Anm. 1 E II; [Ka16] Kaulartz, 201 oder [Er19] Erbguth, 26.

Ein *Miner* erstellt neue Blöcke einer Blockchain. Dabei verwendet er beim Proof of Work Rechenleistung im Wettstreit mit anderen Minern. Bei anderen, weniger kompetetiven Konsensverfahren wird die Rolle ggf. auch *Blockproducer* genannt. Für die Zwecke dieses Aufsatzes wird allgemein der Begriff Miner verwendet. Charakteristisch für Miner ist, dass diese zwar einen kleinen Einfluss auf die Reihenfolge der Transaktionen einer Blockchain haben, ansonsten aber isoliert keinen Einfluss auf Blockchains ausüben können.

Neuere Blockchains wie z.B. EOS haben einen eingebauten Mechanismus zur *Dispute Resolution* und *Governance*.[8] Die Governance steuert dabei allgemein die Weiterentwicklung des Systems, die Änderung von Regeln und bei der On-Chain-Governance auch deren direkte Umsetzung. Eine solche Governance kann auch in Smart Contracts eingebaut werden. Zusätzlich kann auch eine Dispute Resolution ähnlich eines Schiedsgerichtsverfahrens in eine Blockchain oder einen Smart Contract eingebaut werden, um Einzelfälle zu entscheiden. Governance und Dispute Resolution können auch auf eine verbundene Blockchain ausgelagert werden.[9] Die Dispute Resolution wird dabei nicht von sich aus tätig, sondern muss von einer Vertragspartei angerufen werden. Die Umsetzung der Entscheidungen kann dabei im Smart Contract programmiert sein.

3 Abbildung auf die Rollen der DSGVO

Die DSGVO kennt die Rollen der Verantwortlichen (Art. 4 Nr. 7 DSGVO), der gemeinsam Verantwortlichen (Art. 26 Abs. 1 DSGVO), der Auftragsverarbeiter*in (Art. 4 Nr. 8 DSGVO) sowie der Betroffenen. Die Abbildung dieser Rollen auf die im Kontext eines Smart Contracts vorhandenen Rollen ist abhängig von der konkreten tatsächlichen, technischen und rechtlichen Gestaltung. Da bei der Frage der Anwendbarkeit der DSGVO auch auf diese Rollen abgestellt wird, müssen diese Rollen vorab geklärt werden.

3.1 Verantwortliche und Auftragsverarbeiter*innen

Verantwortliche bestimmen die Mittel und Zwecke der Datenverarbeitung (Art. 4 Nr. 7 DSGVO). Im englischen werden sie als *controller* bezeichnet, was deutlich macht, dass hier neben der rechtlichen Verantwortlichkeit der faktische Einfluss wichtig ist. Wer weder rechtlich noch tatsächlich Einfluss auf die Entscheidung über die Verarbeitung hat, kann nicht als für die Verarbeitung Verantwortliche angesehen werden.[10] Wer im Auftrag der Verantwortlichen eine Verarbeitung durchführt, ist Auftragsverarbeiter*in (Art. 4 Nr. 8 DSGVO). Die französische Datenschutzaufsichtsbehörde CNIL hat in einer Stellungnahme[11] erwogen, Entwickler*innen als Auftragsverarbeiter*innen oder Verantwortliche anzusehen.

[8] ECAF, The EOS-Core Arbitration Forum, https://www.eoscorearbitration.io/
[9] [KW17] Kolain/Wirth.
[10] [Ar10] Artikel-29-Datenschutzgruppe WP169, 15.
[11] [Cn18] CNIL, 4.

Dabei hat die CNIL jedoch eingeschränkt, dass dies nur gelte, wenn sie Einfluss auf die Verarbeitung nehmen. Wenn sie keine weiteren Rollen, wie etwa die der Deployer*in übernehmen, ist dies jedoch nicht der Fall.

Deployer*innen stellen den Smart Contract zur Nutzung bereit. Dabei muss unterschieden werden, ob sie die Kontrolle behalten oder aufgeben. Es gibt dabei insgesamt fünf Fälle:

1. Die Deployer*in gibt die Kontrolle unmittelbar ab. Dies ist der klassische Fall eines Smart Contracts auf einer Blockchain. Einmal geschrieben ist er final und kann nicht aktualisiert oder deaktiviert werden.
2. Die Deployer*in behält die Kontrolle und kann über ihre privaten Schlüssel Updates einspielen oder den Smart Contract deaktivieren.
3. Die Deployer*in behielt beim ursprünglichen Deployment zwar die Kontrolle, deaktiviert die Kontrolle jedoch endgültig, bevor Vertragsparteien den Smart Contract verwenden.
4. Die Deployer*in deaktiviert die Kontrolle erst, nachdem Vertragsparteien den Smart Contract zu verwenden begonnen haben.
5. Die Deployer*in deaktiviert die Kontrolle in Absprache mit den Vertragsparteien, nachdem diese den Smart Contract zu verwenden begonnen haben oder gibt die Kontrolle in Absprache mit den Vertragsparteien an eine Dritte ab.

Im ersten Fall hat die Deployer*in keine Kontrolle darüber, welche Vertragsparteien den Smart Contract wofür verwenden. Sie kann die Verarbeitung auch nicht mehr beeinflussen. Sie hat lediglich den Code bereitgestellt, den andere dann verwenden. Wer den Code verwenden will, muss für die Ausführung bezahlen. Die Bezahlung für die Ausführung geht dabei an den Miner des entsprechenden Blocks, in dem die Ausführung festgehalten wird. Die CNIL sieht Smart-Contract-Entwickler*innen als Auftragsverarbeiter*innen, wenn sie nicht nur Code bereitstellen, sondern die Ausführung des Codes beeinflussen.[12] Weder die konkrete Ausführung des Codes noch ob der Code überhaupt (und wenn dann vom wem) ausgeführt wird, kann von der Deployer*in beeinflusst werden. Wer den Code ausführen möchte, kann ihn sich zudem vorab ansehen.[13]

Der dritte Fall ist dem ersten Fall gleichzustellen, da die Deployer*in die Kontrolle bereits aufgegeben hat, bevor der Smart Contract Verwendung findet. Behält sie dagegen wie im zweiten Fall die Kontrolle und kann die Bearbeitung weiterhin beeinflussen, so kann sie die Verarbeitung steuern und ist als Verantwortliche – oder falls sie dies im Auftrag macht, als Auftragsverarbeiter*in – einzustufen. Fraglich ist besonders der vierte Fall: Kann eine Deployer*in als Verantwortliche eingestuft werden, wenn sie keine Kontrolle mehr hat?

[12] [Cn18] CNIL, 2.
[13] [Er19] Erbguth, 29

Sie war Verantwortliche, als die Vertragsparteien mit der Verwendung des Smart Contracts begonnen haben. Entledigt sie sich dieser Kontrolle, können die Vertragsparteien deshalb nicht schutzlos gestellt werden und sie bleibt in der Verantwortung. Etwas anderes gilt im fünften Fall, falls eine Aufgabe oder Abgabe der Kontrolle und Verantwortung in Absprache mit den Vertragsparteien erfolgt. Im Ergebnis kann die Deployer*in Verantwortliche sein, wenn sie die Kontrolle behält oder sie beim Beginn der Verwendung hatte und sie behalten hätte sollen.

Die Akteur*innen der Blockchain, Knotenbetreiber*innen und Miner, könnten ebenfalls Verantwortliche der Ausführung des Smart Contracts sein. Dabei sind die gleichen Kriterien anzuwenden, die für die Blockchain gelten. Knotenbetreiber*innen und Miner haben demnach bei öffentlichen Blockchains in der Regel keine Kontrolle. Sie können jedoch als Auftragsverarbeiter*innen klassifiziert werden.[14]

Die Vertragsparteien entscheiden darüber, den Smart Contract verwenden zu wollen. Ist der Smart Contract unveränderbar, so sind die Vertragsparteien die Einzigen, die auf diese Entscheidung Einfluss haben. Daher entscheiden sie auch über die Zwecke und Mittel der Datenverarbeitung.[15] Gibt es bei den Vertragsparteien ein Machtgefälle, so kann sich die Verantwortlichkeit ggf. auf eine der beiden Vertragsparteien beschränken. Dies ist etwa der Fall, wenn der Smart Contract der einen Vertragspartei deutlich mehr Aktionsmöglichkeit gibt. Das gleiche kann gelten, wenn eine Vertragspartei direkt oder indirekt Einfluss auf die Entwicklung des Smart Contract genommen hat und damit die Bedingungen „diktiert“.

Bei Smart Contracts werden häufig unparteiische Dritte als Orakel eingebunden, die Informationen beisteuern, welche die Ausführung des Smart Contract maßgeblich beeinflussen. So muss etwa ein Smart Contract zur Versicherung von Flugverspätungen auf die geplanten und tatsächlichen Ankunftszeiten der Flüge zugreifen. Diese Information muss von einer vertrauenswürdigen Dritten bereitgestellt werden. Auf der einen Seite stellt die Dritte hier "nur" Informationen bereit. Auf der anderen Seite ist die Dritte hier möglicherweise die Einzige, die hier noch einen Einfluss auf die Auszahlung der Flugverspätung nehmen kann. Es ist fraglich, ob dies für die Annahme einer Verantwortlichkeit ausreicht. Solange sie diesen Einfluss jedoch in der von den Vertragsparteien vorgegebenen Art und Weise ausübt, macht sie dies allenfalls als Auftragsverarbeiter*in und ist nicht selbst Verantwortliche.

Smart Contracts können auch Funktionen zur Governance und zur Dispute Resolution eingebaut haben. Diese können die Ausführung des Smart Contracts ggf. blockieren oder auch verändern. Dabei muss unterschieden werden zwischen einer Dispute Resolution, die erst auf Initiative einer oder mehrerer Vertragsparteien aktiviert wird und den Eingriffsmöglichkeiten der Governance, die kein Zutun der Vertragsparteien erfordern. Im ersten Fall entsteht die Kontrolle erst dadurch, dass eine oder mehrere Vertragsparteien die Dispute

[14] So die CNIL in [Cn18], 2; davor bereits [MW17] Martini/Weinzierl, 1250; [EF17] Erbguth/Fasching, 563; ebenso Janicki/Saive mit weiteren Nachweisen [JS19], 253; Schrey/Thalhofer sehen dagegen alle Teilnehmer*innen einer Blockchain als Verantwortliche [ST17], 1433

[15] In Fortführung der Argumentation der CNIL in [CN18], 2.

Resolution anrufen. Im letzteren Fall besteht jedoch eine ständige Kontrollmöglichkeit und damit möglicherweise eine Verantwortlichkeit. Charakteristisch ist dabei auch, dass die Governance und Dispute Resolution nicht weisungsgebunden sind. Allerdings muss die Governance den vorgegebenen Governanceregeln folgen. Das alleine macht sie jedoch noch nicht zur Auftragsverarbeiter*in. Sofern die Governance nicht durch eine übergeordnete Auftraggeber*in kontrolliert wird, dürfte die Governance damit die letztendliche Instanz sein, die über die Mittel und Zwecke der Datenverarbeitung entscheidet. Fraglich ist jedoch, ob es angemessen ist, private Schieds- und Überwachungsinstanzen als Verantwortliche anzusehen. Gerade durch den Einbau solcher Instanzen soll die Compliance mit den vertraglichen und gesetzlichen Regeln sichergestellt werden. Aber genau der Einbau solcher Kontrollmöglichkeiten erhöht die Verantwortlichkeit. Das entspricht jedoch dem der DSGVO innewohnenden Prinzips, dass die Verantwortlichkeit dort angesiedelt wird, wo auch tatsächlich entschieden wird.

3.2 Gemeinsame Verantwortlichkeit

Je nach Konstellation können wie zuvor dargestellt neben den Vertragsparteien verschiedene weitere Akteur*innen Verantwortliche sein. Fraglich ist dabei, ob alle zusammen eine gemeinsame Verantwortlichkeit trifft oder ob bestimmte Verantwortlichkeiten auf Grund anderer, dominierender Verantwortlichkeiten zurücktreten. In C-210/16 hat der EuGH entschieden, dass gemeinsame Verantwortlichkeiten auch bestehen können, wenn die Verantwortlichkeit nicht gleich verteilt ist.[16] Ist der Beitrag einer Akteur*in jedoch verschwindend gering im Vergleich zur dominierenden Kontrolle anderer, so erscheint die Annahme gemeinsamer Verantwortlichkeit nicht angemessen.

Hier muss abgewogen werden:

- Hat eine Vertragspartei die Entwicklung und das Deployment beauftragt und kontrolliert damit die Ausführung des Smart Contract, so tritt demgegenüber die Kontrollmöglichkeit der anderen Vertragsparteien in den Hintergrund.
- Gibt es keine Kontrolle durch das Deployment, so haben die Vertragsparteien die alleinige Kontrolle. Ist hier kein starkes Machtgefälle zwischen den Vertragsparteien erkennbar, so spricht viel für eine gemeinsame Verantwortlichkeit.
- Hat nach Start des Smart Contracts durch die Vertragspartner*innen nur noch die Governance Kontrolle über die Ausführung des Smart Contracts, so ist die Governance als Verantwortliche zu qualifizieren.
- Ist eine Verantwortliche gleichzeitig Betroffene, so muss sie die Begrenzungen der DSGVO bzgl. der Verarbeitung ihrer eigenen Daten und bzgl. der sie betreffenden automatisierten Entscheidungen nicht beachten.

[16] EuGH Urteil vom 5. Juni 2018, C-210/16, Rn 43

3.3 Betroffene

Betroffene sind die Personen, auf die sich die personenbezogenen Daten beziehen. Bei automatisierten Entscheidungen (Artikel 22 DSGVO) sind Betroffene auch diejenigen, die einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen sind.

4 Anwendbarkeit der DSGVO

4.1 Sachlicher Anwendungsbereich

Die Definition von personenbezogenen Daten in Art. 4 Nr. 1 der DSGVO ist sehr weit. Sind Daten für diejenigen, die Zugriff auf die Daten haben können, mit einer natürlichen Person verknüpfbar, so dass Information zu diesen Personen abgeleitet werden können, dann handelt es sich bereits um personenbezogene Daten. Dabei müssen sämtliche Techniken und auch Daten einbezogen werden, die dazu herangezogen werden können. Der Erwägungsgrund 26 schränkt dies insofern ein, als nur rein theoretische Möglichkeiten ausgeschlossen werden. In C-210/16 legt der EuGH die Schwelle für eine Identifizierbarkeit recht hoch, in dem er eine Identifizierungsmöglichkeit bereits dann außer Acht lassen möchte, bei der das Risiko einer Identifizierung "de facto"vernachlässigbar wäre, da die Identifizierung verboten ist oder einen unverhältnismäßigen Aufwand erfordert.[17] Der Erwägungsgrund stellt dabei nicht nur auf die Verantwortliche ab, sondern bezieht auch *andere Personen* mit ein, die über Heranziehung weiterer Informationen oder sonstiger Mittel, natürliche Personen mit den Daten zu identifizieren. Das ist aber nur möglich, wenn diese andere Personen auch Zugriff auf die in Frage stehenden Daten erlangen könnten.

Privacy Enhancing Technology, also Techniken wie Verschlüsselung, kryptographische Hashwerte oder Zero Knowledge Proofs sind Werkzeuge für Datenschutz durch Technik, deren Verwendung in Art. 25 DSGVO eingefordert wird. Wegen eingeschränkter organisatorischer Schutzmöglichkeiten wird im Kontext öffentlichen Blockchains Datenschutz vor allem durch Technik sichergestellt. In einem speziellen Anwendungsfall der versuchten Anonymisierung von Datensätzen haben die Aufsichtsbehörden 2014 beschrieben, dass eine Anonymisierung durch Verschlüsseln, Hashing oder Löschen der direkt personenbezogenen Merkmale in der Regel nicht erfolgreich möglich ist.[18] Damit sind jedoch Techniken wie Hashing nicht generell ungeeignet, um auf Blockchains eingesetzt zu werden. Vielmehr muss im Einzelfall geprüft werden, wie die Technik eingesetzt wird und ob ein Personenbezug nach den in C-210/16 und im Erwägungsgrund 26 beschriebenen Kriterien noch hergestellt werden kann.[19] Dafür spricht auch eine Entscheidung der österreichischen Datenschutzbehörde: In diesem Fall, der weder Blockchain noch Smart Contracts betraf, stellt die Behörde

[17] EuGH, Urteil vom 19. Oktober 2016, C-582/14, Rn 46.
[18] [Ar14] Artikel-29-Datenschutzgruppe WP216, 29.
[19] so auch das EU Blockchain Observatory [Bl18], 22; a.A. Finck [Fi18], 22

fest, dass ein effektiv nicht mit einer Person in Verbindung zu bringender Datensatz als anonymisiert gilt und damit einem Löschen gleichkommt.[20] Erwägungsgrund 26 sieht allerdings auch vor, dass über die zum Zeitpunkt der Verarbeitung verfügbare Technologie hinaus auch technologische Entwicklungen zu berücksichtigen sind. Darunter könnte der Zuwachs an Rechenleistung nach dem Mooreschen "Gesetz"[21] oder Quantencomputer[22] fallen.

Sofern Bitcoin- oder Ethereum-Transaktionen mit einer öffentlichen Adresse einer Privatperson verknüpft sind, dürfte hier analog zu den IP-Adressen ein personenbezogenes Datum vorliegen.[23] Für Bitcoin gibt es beispielsweise kommerzielle Anbieter, die die Personen identifizieren, die hinter einer Adresse stehen.[24]

4.2 Haushaltsausnahme

Art. 2 Abs. 2 lit. c DSGVO stellt Datenverarbeitungen von der Anwendung der DSGVO frei, soweit die Datenverarbeitung ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten dient. In C-101/01[25] hat der EuGH in Bezug auf für die Öffentlichkeit zugängliche Information festgestellt, dass dies den Bereich der Haushaltsausnahme überschreite. Hieran hat der EuGH kürzlich in C345/17[26] ausdrücklich festgehalten. Mit dem Schreiben eines Eintrags auf eine öffentliche Blockchain ist der Eintrag nicht nur öffentlich zugreifbar, sondern wird auch zehntausendfach kopiert.[27] Die CNIL hat dagegen angenommen, dass eine privat motivierte Transaktion auf einer öffentlichen Blockchain unter die Haushaltsausnahme fällt.[28] Allerdings sind eine Blockchain-Transaktion und eine Äußerung im Web oder Social Media nicht unbedingt vergleichbar. Die Transaktion ist nur mit größeren Aufwand zuordenbar. Eine Öffentlichkeit wird damit meistens effektiv nicht hergestellt. Zudem würde eine enge Interpretation der Haushaltsausnahme dazu führen, dass Privatpersonen mit ihren Transaktionen auf Blockchains selbst zu Verantwortlichen werden. Sie müssten sich gegenüber den Betroffenen identifizieren. Die DSGVO würde damit z.B. "anonyme" Bitcoin-Zahlungen verbieten. Ohne hier näher auf die umfangreiche Diskussion zu den Schutzzwecken der DSGVO[29] einzugehen, wäre das wohl eine Konsequenz, die möglicher-

[20] DSB-D123.270/0009-DSB/2018.

[21] Das Mooresche "Gesetz"beschreibt die Beobachtung, dass neue Rechner alle 2 Jahre etwa doppelt so leistungsfähig sind. Dies bedeutet, dass Rechner in 40 Jahren etwa eine Million mal schneller sein werden.

[22] Quantencomputer rechnen nicht schneller, sondern anders und können dadurch Dinge berechnen, die konventionell nur durch langwieriges Ausprobieren ermittelbar wären. Eine Abschätzung, welche kryptographische Technik dadurch unsicher wird und welche sicher bleibt, gibt es bei [Ch16] Chen et al., 2.

[23] [EF17] Erbguth/Fasching, 561, a.A. [ST17] Schrey/Thalhofer, 1433.

[24] So etwa Chainalysis.com 01.05.2019.

[25] EuGH, Urteil vom 06.11.2003, C-101/01, Rn 47.

[26] EuGH, Urteil vom 14.02.2019, C-345/17, Rn 41.

[27] Die Anzahl der Knoten ist etwa über `https://www.ethernodes.org` sichtbar.

[28] [Cn18] CNIL, 2; a.A. Janicki/Saive [JS19], 252.

[29] So etwa die Diskussion von Winfried Veil und Kirsten Bock auf dem CRonline-Blog vom 6.2.2019, 18.3.2019, 22.3.2019 und 29.3.2019 `https://www.cr-online.de/blog/01.05.2019`.

weise nicht dem Normzweck der DSGVO entspricht. Dies stützt die Position der CNIL und spricht für eine etwas weitere Interpretation der Haushaltsausnahme.

4.3 Räumlicher Anwendungsbereich

Der räumliche Geltungsbereich wird in Art. 3 DSGVO geregelt. Dabei wird nicht auf den Ort der Datenverarbeitung abgestellt, vielmehr genügt, wenn eines der folgenden Merkmale einschlägig ist:

- Die Verarbeitung erfolgt im Rahmen der Niederlassung einer Verantwortlichen oder einer Auftragsverarbeiter*in in der Europäischen Union.
- Die Datenverarbeitung steht im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen an Personen in der Europäischen Union.
- Die Datenverarbeitung steht im Zusammenhang mit der Beobachtung des Verhaltens von Personen in der Europäischen Union.

Bei einer öffentlichen Blockchain mit an die 10.000 Knoten sitzen sicher auch Knotenbetreiber in der EU, so dass daher die DSGVO räumlich Anwendung findet. Dies gilt selbst dann, wenn die anderen Akteure, wie etwa die Vertragsparteien, nicht in der EU ansässig sind.

5 Rechtfertigung zur Verarbeitung personenbezogener Daten

Bei Smart Contracts muss zwischen rein lesenden Aufrufen und Transaktionen unterschieden werden. Nur bei Letzteren wird die Verarbeitung durch jeden Knoten wiederholt und dabei Input und Output sowie Zustandsänderung auf der Blockchain abgespeichert. Bei Ethereum stehen diese Inhalte danach unveränderlich auf der öffentlichen Blockchain. Es stellen sich daher folgende Fragen:

1. Sind Ein- und Ausgabedaten sowie abgelegte Zustandsdaten personenbezogene Daten? Dies muss auf Grund der Daten beurteilt werden. Da die Definition von personenbezogenen Daten recht weit gezogen ist, dürfte dies häufig der Fall sein.
2. Wer sind Betroffene und wer Verantwortliche dieser Daten. Unproblematisch ist es dabei, wenn Verantwortliche mit Hilfe eines Smart Contracts eigene personenbezogene Daten verarbeiten.
   Gibt es jedoch keine Personenidentität zwischen Verantwortlichen und Betroffenen und ist zudem die Haushaltsausnahme nicht einschlägig, so ist eine Rechtfertigung für diese Verarbeitung erforderlich.

5.1 Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO)

Nach Art. 6 Abs. 1 lit. a DSGVO könnten die Betroffenen in die Verarbeitung der personenbezogenen Daten einwilligen. Problematisch daran ist, dass die Einwilligung jederzeit widerrufbar ist (Art. 7 Abs. 2 S. 1 DSGVO). Der Widerruf wirkt jedoch nur für künftige Verarbeitungen (Art. 7 Abs. 3 S. 2 DSGVO). Die Rechtmäßigkeit der vor dem Widerruf erfolgten Verarbeitung ist daher davon nicht betroffen. Die Transaktion muss dementsprechend nicht rückgängig gemacht werden. Allerdings bleiben die Daten auch danach noch gespeichert, was nach Art. 4 Nr. 2 DSGVO ebenfalls eine Verarbeitung ist. Die Speicherung ist logische Folge der Verarbeitung des Smart Contracts. Selbst wer Kontrolle über den Smart Contract, dessen Deaktivierung oder ein Update hat, kann die Daten nicht entfernen. Daher muss die Speicherung der für die Vornahme der Transaktion Verantwortlichen zugerechnet werden. Fraglich ist, ob dies bedeutet, dass die dauerhafte Speicherung auch als direkter statischer Erfolg der Transaktion des Smart Contracts gilt und daher beim Widerruf der Einwilligung nicht rückgängig gemacht werden muss. Für eine solche Auslegung spricht, dass nach Einwilligung genau das getan wurde, worin eingewilligt wurde und der Widerruf eben das nicht rückabwickeln soll. Damit wäre jedoch das Recht auf Widerruf und im Endeffekt auch das Recht auf Vergessenwerden (Art. 17 DSGVO) deutlich eingeschränkt. Selbst wenn man dieser Überlegung folgte, so müsste das zumindest auf Fälle begrenzt sein, in denen sich die dauerhafte Speicherung zwingend ergibt, in diesem Kontext auch vom Betroffenen gewollt war und in denen vor der Einwilligung sehr deutlich auf diesen Umstand hingewiesen wurde. Keineswegs sollten Unternehmen sich dadurch der Löschpflicht entziehen können, indem ihre Verfahren keine Löschmöglichkeit vorsehen. Im Ergebnis bleibt die Einwilligung daher ein eher ungeeignetes Instrument der Rechtfertigung.

5.2 Erfüllung eines Vertrages (Art. 6 Abs. 1 S. 1 lit. b DSGVO)

Erfolgt die Verarbeitung zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, könnte die Verarbeitung zulässig sein. Dies gilt auch, wenn die Verarbeitung für vorvertragliche Maßnahmen erforderlich ist. Die Erforderlichkeit wurde vom EDSA näher ausgeführt.[30] Sofern der Vertrag originär mit dem Smart Contract begründet wird oder zumindest ein anderweitig geschlossener Vertrag eine Ausführung als Smart Contract auf einer Blockchain erfordert, kann das hier einschlägig sein. Allerdings können nicht beliebige Sachverhalte durch Implementierung als Smart Contract über Art. 6 Abs. 1 S. 1 lit. b DSGVO datenschutzrechtlich gerechtfertigt werden. Vielmehr muss der Sachverhalt an sich eine Implementierung als Smart Contract mit dauerhafter Speicherung rechtfertigen.

[30] [Ed19] EDPB: Guidelines 2/2019, Rn 13.

5.3 Rechtliche Verpflichtung (Art. 6 Abs. 1 S. 1 lit. c DSGVO)

Sofern die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der die Verantwortliche unterliegt, ist die Verarbeitung ebenfalls gerechtfertigt. Sofern es Verpflichtungen gibt, Transaktionen dauerhaft einsehbar und überprüfbar zu machen, können Smart Contracts ein gutes Hilfsmittel sein. Ist dagegen eine solche Transparenzpflicht zeitlich begrenzt, so müsste eine spezielle Blockchain gebaut werden, die Daten ebenfalls nur genau so lange speichert.

5.4 Berechtigtes Interesse (Art. 6 Abs.1 S. 1 lit. f DSGVO)

Im Fall von berechtigtem Interesse, dem kein überwiegendes Interesse der Betroffenen entgegen steht, ist eine Verarbeitung ebenfalls zulässig. Das berechtigte Interesse kann allerdings durch einen Widerspruch der Betroffenen nach Art. 21 Abs. 1 DSGVO auf den Fall zwingender schutzwürdiger Gründe beschränkt werden, die die Interessen der Betroffenen überwiegen. Ein so starkes legitimes Interesse könnte man sich etwa vorstellen, wenn durch Maßnahmen des technischen Datenschutz nur ein sehr geringes Restrisiko für die Rechte der Betroffenen verbleibt.[31] Solch zwingende schutzwürdige Gründe sind ebenfalls denkbar, wenn ein Smart Contract als Vertrag unwirksam ist, zurückabgewickelt werden muss und die Einträge auf der Blockchain zur Richtigstellung der Einträge erforderlich sind. Im Kontext der Unveränderbarkeit werden zwingende schutzwürdige Interessen jedoch nur in seltenen Fällen die Interessen der Betroffenen dauerhaft überwiegen, so dass Art. 6 Abs. 1 S. 1 lit. f DSGVO als generelles Rechtfertigungsinstrument wenig geeignet ist.

6 Automatisierte Entscheidung

Art. 22 DSGVO gibt Betroffenen das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung personenbezogener Daten beruht.

6.1 Entscheidung

Smart Contracts arbeiten an sich vollständig automatisiert. Doch beruht die Entscheidung über eine Transaktion eines Smart Contracts auf dessen automatisierter Verarbeitung oder aber auf den vorab manuell festgelegten sehr einfachen Regeln? Ist die eigentlich Entscheidung nicht bereits bei der Festlegung dieser einfachen Regeln bzw. bei der Auswahl des transparenten Smart Contracts zur Abwicklung einer Transaktion getroffen worden? Dies würde im Endeffekt bedeuten, dass Art. 22 nur dann Anwendung finden würde, wenn die

[31] [Cn18] CNIL, Premiers éléments d'analyse de la CNIL, 6.

Entscheidungsregeln nicht manuell vorgegeben wurden. Dies ist etwa bei Blackbox-Verfahren der KI der Fall. *Finck* lehnt eine solche restriktive Interpretation mit dem Argument ab, dass diese nicht vom Gesetzgeber gemeint gewesen sein könne. Denn bei dieser Auslegung würde die Ausnahme für *Entscheidungen zur Erfüllung eines Vertrags* in Art. 22 Abs. 2 lit. a DSGVO keinen Sinn mehr machen, da bei manuell geschlossenen Verträgen die Bedingungen einer Transaktion vorab festlegt würden.[32] Gegen eine restriktive Interpretation spricht auch das von der Artikel 29-Gruppe genannte Beispiel der automatisierten Erstellung von Bußgeldbescheiden auf Basis der Messwerte einer Geschwindigkeitsüberwachung. Auch dort sind die Entscheidungskriterien einfach und vorab festgelegt.[33]

Art. 22 DSGVO beschränkt das Verbot auf Entscheidungen, die gegenüber der Betroffenen eine *rechtliche Wirkung* entfalten oder sie *in ähnlicher Weise erheblich beeinträchtigt*. Mit Smart Contracts werden häufig Verträge abgeschlossen, erfüllt und/oder Assets auf der zugrunde liegenden Blockchain verschoben. Da wird eine rechtliche Wirkung meistens gegeben sein.[34] Zudem relativiert die Artikel-29-Gruppe die Begrenzung auf *erhebliche Beeinträchtigungen* so weit, dass selbst die Auswahl von Werbung darunter fallen könnte.[35]

Diese weite Interpretation der *Entscheidung* sollte nicht unkritisch gesehen werden. Denn sie könnte dazu führen, dass nicht nur Transaktionen von Smart Contracts, sondern dass jedwede Ethereum-Blockchain-Transaktion unter Artikel 22 subsumiert werden kann, da dabei Berechtigungen und Kontostände geprüft sowie Kryptocoins bewegt werden.

6.2 Ausnahmen

Art. 22 DSGVO nennt in Absatz 2 mehrere Ausnahmen, die automatisierte Entscheidungen trotzdem erlauben. Hier sind insbesondere Abschluss oder Erfüllung eines Vertrages zwischen Verantwortlichen und Betroffenen (lit. a) sowie die ausdrückliche Einwilligung der Betroffenen (lit. b) zu nennen. Bei Smart Contracts dürfte häufig ein Vertrag abgeschlossen oder erfüllt werden. Da der Umgang mit Smart Contracts auf einer Blockchain meistens bewusst gewählt wird, wird eine ausdrückliche Einwilligung häufig vorliegen oder erteilt werden können.

6.3 Recht auf manuelles Eingreifen, Anhörung und Anfechtung

Art. 22 Abs. 3 gibt in den Fällen der beiden Ausnahmen nach Abs. 2 lit. a und lit. c den Betroffenen das Recht auf ein manuelles Eingreifen, bei dem sie von den Verantwortlichen angehört werden und die Entscheidung anfechten können. Dieses Recht könnte z.B. durch

[32] [Fi19] Finck, 8.
[33] [Ar17] Artikel-29-Gruppe, WP251, 8.
[34] [Fi19] Finck, 10.
[35] [Ar17] Artikel-29-Gruppe, WP251, 23.

eine in den Smart Contract eingebaute Dispute Resolution gewährleistet werden. Hierfür wird beispielsweise eine unabhängige Vertrauensperson kontaktiert, die bei Meinungsverschiedenheiten zwischen den Vertragsparteien eingreifen kann. Ist eine Dispute Resolution weder in den Smart Contract noch der Blockchain an sich eingebaut, ist die Ausführung des Smart Contracts final. Das manuelle Eingreifen kann jedoch auch nachträglich erfolgen.[36] Allerdings muss auch effektiv ein Eingreifen möglich sein, d.h. eine falsche Entscheidung muss korrigiert oder zumindest kompensiert werden können. Etwas unpassend erscheint in Art. 22 Abs. 3 die Anforderung, dass die Verantwortliche die entsprechenden Maßnahmen treffen und eine Person seitens der Verantwortlichen eingreifen muss. Reicht es nicht, sie letztendlich dafür verantwortlich zu machen, dass die Maßnahmen zur Verfügung stehen? Eine neutrale Entscheidungsinstanz sollte hier doch keinen Nachteil darzustellen.

6.4 Ergebnis

Sofern auf Grund der Rollenverteilung die DSGVO für eine Smart-Contract-Transaktion Anwendung findet, muss ein manuelles Eingreifen möglich sein. Dieses Eingreifen muss jedoch die Transaktion auf der Blockchain nicht komplett ungeschehen machen, sondern es reicht, diese außerhalb der Blockchain rückabzuwickeln oder kompensieren zu können.

7 Fazit

Bereits mit der öffentlichen Ethereum-Blockchain sind eine Vielzahl sehr unterschiedlicher Rollenverteilungen möglich, die im Detail zu deutlich unterschiedlichen Ergebnissen führen können. Nicht jede Konstellation ist dabei DSGVO-konform. Im Ergebnis sind z.B. zwei Arten von Smart Contracts DSGVO-konform: Zum einen komplett autonome Smart Contracts z.B. als dezentralisierte Börsen zum Austausch von Tokens. Hier sind die Bedingungen transparent festgelegt und die Vertragsparteien sind die Verantwortlichen i.S.d. DSGVO, in dem sie direkt mit diesem Mechanismus interagieren, sofern nicht die Haushaltsausnahme die Anwendung der DSGVO ausschließt. Zum anderen kontrollierte Smart Contracts bei denen die Verantwortlichen Mechanismen zur Dispute Resolution eingebaut haben oder externe Kompensationsmechanismen für falsche Entscheidungen bereitstellen.

In der Regel unzulässig dürfte es dagegen sein, einen anderweitig geschlossenen Vertrag ohne zwingende Erfordernis einseitig zur Ausführung auf eine Ethereum-Blockchain zu übertragen.

Literatur

[Ar10] Artikel-29-Datenschutzgruppe WP169, 0264/10/DE: Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010.

[36] [Fi19] Finck, 16.

[Ar14] Artikel-29-Datenschutzgruppe WP216, 0829/14/DE: Stellungnahme 5/2014 zu Anonymisierungstechniken, 10.04.2014.

[Ar17] Artikel 29 Data Protection Working Party: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 03.10.2017.

[Bl18] The European Union Blockchain Observatory and Forum, Blockchain and the GDPR, 16.10.2018, https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf[37].

[Bu14] Buterin V.: Etherum White Paper, A next-generation smart contract and decentralized application platform, https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[Ch16] Chen L. et al. Report on Post-Quantum Cryptography, NISTIR 8104, https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf.

[Cn18] CNIL: La blockchain: Premiers éléments d'analyse de la CNIL, 9/2018, https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf englische Version https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf.

[Dj16] Djazayeri, A.: Rechtliche Herausforderungen durch Smart Contracts, jurisPR-BKR 12/2016.

[Ed19] edpb: 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects' 09.04.2019.

[EF17] Erbguth, J.; Fasching J.: Wer ist Verantwortlicher einer Bitcoin-Transaktion? ZD 2017, 560-565.

[Er18] Erbguth, J.: 'Was sind Smart Contracts, wofür werden sie eingesetzt und wann gilt Code is Law?' Telemedicus Sommerkonferenz 2018.

[Er19] Erbguth, J.: 'Transparenz von Smart Contracts' in: Smart Contracts, hrsg. Fries, M.; Paal, B. 2019, Mohr-Siebeck, ISBN 978-3-16-156910-4.

[Fi18] Finck, M.: Blockchains and Data Protection in the European Union, EDPL 2018, 17.

[Fi19] Finck, M.: Smart Contracts as a Form of Solely Automated Processing Under the GDPR, 08.01.2019, Max Planck Institute for Innovation & Competition Research Paper No. 19-01. http://dx.doi.org/10.2139/ssrn.3311370.

[JS19] Janicki, T.; Saive, D.: Privacy by Design in Blockchain-Netzwerken, ZD 2019, 251.

[Ka16] Kaulartz, M.: Herausforderungen bei der Gestaltung von Smart Contracts, InTer 2016, 201.

[KW17] Kolain M.; Wirth C.: Multi-Chain Governance, DSRITB 2017, 845.

[MW17] Martini, M.; Weinzierl, Q.: Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251.

[ST17] Schrey J.; Thalhofer T.: Rechtliche Aspekte der Blockchain, NJW 2017, 1431.

[Sz97] Szabo N.: Formalizing and Securing Relationships on Public Networks, first monday, Vol. 2, Nr. 9, 9/1997, https://ojphi.org/ojs/index.php/fm/article/view/548/469.

[37] Alle Internetquellen wurden zuletzt am 20.6.2019 überprüft.