BLOCKCHAIN REALLABOR RHEINISCHES REVIER

Blockchain und die Datenschutzgrundverordnung

Prof. Dr. T. Hoeren[1], E. Rabovskaja[1], A. Bauer[2]
[1] Institut für Informations-, Telekommunikations- und Medienrecht (ITM) der WWU Münster, Münster, Deutschland
[2] Fraunhofer-Institut für Angewandte Informationstechnik (FIT), Sankt Augustin, Deutschland
kontakt_reallabor@fit.fraunhofer.de

Ausgangssituation und Problemstellung

Die Gestaltung jeglicher Use Cases muss in datenschutzkonformer Weise erfolgen. Aus Anwendersicht können Verstöße gegen die DSGVO Bußgelder nach sich ziehen. Für die Betroffenen geht es darum, dass ein zuverlässiger Schutz ihrer personenbezogenen Daten garantiert werden kann. Letzteres kann auch Auswirkungen für eine breite Akzeptanz von Blockchain-Lösungen haben. Vor allem folgende Fragen stellen sich konkret:

- Welche Daten stellen im Kontext von Blockchain-Anwendungen personenbezogene Daten dar?
- Stellen die Hashwerte von personenbezogenen Daten auf der Blockchain wiederum selbst personenbezogene Daten nach der DSGVO dar?
- Wer ist in Blockchain-Systemen als datenschutzrechtlich Verantwortlicher anzusehen?
- Welche Rechtfertigungsgrundlage(n) für die Datenverarbeitung bietet/n sich aus der Sicht von Anwendern an? Welche Anforderungen sind im Blockchain-Kontext an die Einwilligung zu stellen?
- Wie können die Betroffenenrechte auf Berichtigung (Art. 16 DSGVO) und Löschung (Art. 17 DSGVO) effektiv gewährleistet werden?
- Steht Art. 22 DSGVO (automatisierte Entscheidung im Einzelfall) dem Einsatz von Smart Contracts entgegen? Wenn nein: Welche Anforderungen sind an deren Gestaltung zu stellen, um eine rechtmäßige Verarbeitung zu gewährleisten?
- Wann findet im Zusammenhang mit Blockchain-Anwendungen eine Übermittlung personenbezogener Daten an Drittländer statt? Welche Konsequenzen ergeben sich daraus?

Anwendungskontext

Es handelt sich um Fragen, die sich unabhängig vom konkreten Anwendungsfall stellen, sobald personenbezogene Daten natürlicher Personen betroffen sind. Aufgrund der Weite des Begriffs der personenbezogenen Daten, welcher insbesondere auch pseudonymisierte Daten umfasst, haben Fragen des Datenschutzrechts somit für einen Großteil der Use Cases Bedeutung. In jedem Fall ist daher stets sorgfältig zu prüfen, ob personenbezogene Daten verarbeitet werden und das Datenschutzrecht somit einschlägig ist.

Lösungsansätze

Es besteht weitestgehend Einigkeit darüber, dass sowohl Public Keys als auch sonstige Daten im Zusammenhang mit Blockchain-Transaktionen (Transaktionsdaten) personenbezogene Daten darstellen können.[1] Regelmäßig wird Pseudonymität, jedoch keine Anonymität bestehen, sodass der Anwendungsbereich des Datenschutzrechts eröffnet ist. Auch die Hashwerte von personenbezogenen Daten können selbst wiederum personenbezogene Daten darstellen.[2] Insoweit kann nur dann davon ausgegangen werden, dass Hashwerte keine personenbezogenen Daten darstellen, wenn die Eigenart der jeweiligen Hashwerte und des dazugehörigen Datensatzes vor Herausgreifen, Verknüpfbarkeit und Inferenz derart schützen, dass eine Identifikation – wenn überhaupt – nur mit einem unverhältnismäßig hohen Aufwand möglich ist.[3] Ausschlaggebend ist hierfür wohl stets die sog. Entropie des Ausgangsdatensatzes, also seine Variabilität, die durch sog. „Salted Hashes“ und „Peppered Hashes“ erhöht werden kann.[4] Keine personenbezogenen

[1] Finck, Blockchain and the General Data Protection Regulation, S. 28.
[2] Hierzu etwa Erbguth, MMR 2019, 654 ff.
[3] Vgl. zum Schutzniveau Art. 29 Datenschutzgruppe, Stellungnahme 5/2014 (WP216, 0829/14/DE), S. 25 f.; So schlussfolgernd etwa auch Erbguth, MMR 2019, 654, 660; Lyons et al., Blockchain and the GDPR, S. 21 f.
[4] Lyons et al., Blockchain and the GDPR, S. 21 f.

Daten liegen jedoch vor, wenn der Bezug zu natürlichen Personen ausgeschlossen ist. Handelt es sich also ausschließlich um Maschinendaten[5] oder Daten über juristische Personen[6], die auch keine Rückschlüsse auf natürliche Personen zulassen, ist die DSGVO nicht anwendbar.

Die datenschutzrechtliche Verantwortlichkeit richtet sich danach, wer über die Zwecke und Mittel der Datenverarbeitung entscheidet (Art. 4 Nr. 7 DSGVO). Während in zulassungsbeschränkten Systemen eine zentrale, entscheidungsbefugte Stelle existiert, die als Verantwortlicher identifiziert werden kann[7], ist die Bestimmung des oder der Verantwortlichen in zulassungsfreien Systemen deutlich komplexer. Nutzer solcher Systeme, die Transaktionen einstellen, welche nicht nur deren eigene personenbezogene Daten enthalten, sind regelmäßig als Verantwortliche einzustufen.[8] Problematisch und ungeklärt ist aber die rechtliche Stellung der Nodes (Netzwerkknoten) und eine potenzielle gemeinsame Verantwortlichkeit nach Art. 26 DSGVO.[9]

Jede Datenverarbeitung bedarf nach Art. 6 DSGVO einer Rechtfertigung. Eine Einwilligung als Grundlage ist insofern problematisch, als dass die Einwilligung frei widerruflich ist und in diesem Fall eine Löschung der Daten notwendig wäre. Ansonsten würde mit jeder neuen Transaktion eine erneute, nicht mehr gerechtfertigte, Verarbeitung dieser Daten stattfinden. Zusätzlich ist angesichts des neuartigen Charakters der Blockchain-Technologie zweifelhaft, ob eine ausreichend informierte Entscheidung der betroffenen Person erreicht werden kann.[10] Hier, aber auch bei der Anwendbarkeit anderer Rechtfertigungsgrundlagen, offenbart sich weiterer Forschungsbedarf. Diese Unsicherheit führt dazu, dass Gestaltungen vorzugswürdig erscheinen, bei denen keine personenbezogenen Daten direkt auf der Blockchain verarbeitet werden.

Auch um die Erfüllung von Betroffenenrechten zu gewährleisten, ist die Vermeidung einer on-chain-Speicherung personenbezogener Daten vorzuziehen. Sind die personenbezogenen Daten in einer Datenbank außerhalb der Blockchain abgelegt, können die Rechte auf Berichtigung oder Löschung vergleichsweise einfach erfüllt werden.[11] Wo dies aufgrund der Besonderheiten des Anwendungsfalls nicht möglich ist, werden verschiedene technische Lösungen erwogen, um die on-chain gespeicherten Daten zu anonymisieren, d.h. die Identifizierbarkeit von Personen auf Grundlage dieser Daten auszuschließen. Anonymisierte Daten stellen keine personenbezogenen Daten dar. Erheblicher weiterer Forschungsbedarf besteht sowohl aus technischer Sicht bezüglich der Praxistauglichkeit und Sicherheit solcher Verfahren[12], als auch aus rechtlicher Sicht bezüglich der Anforderungen an eine ausreichende Anonymisierung[13]. Zu prüfen ist ferner, ob eine Anonymisierung für den jeweiligen Use Case überhaupt erwünscht ist.[14] Es existieren schließlich Ansätze für Blockchain-Modelle, die eine nachträgliche Anpassung von Blöcken erlauben.[15] Hier ist allerdings darauf zu achten, dass die Vorteile der Blockchain gegenüber anderen Systemen nicht vollständig aufgehoben werden.

Smart Contracts können in den Anwendungsbereich des Art. 22 Abs. 1 DSGVO[16] und somit unter das Verbot der automatisierten Einzelfallentscheidung fallen. Eine Rechtfertigung nach Art. 22 Abs. 2 DSGVO bleibt aber möglich. Hierfür müssen weitere Anforderungen eingehalten, d.h. durch die technische Gestaltung ermöglicht werden, etwa ein Recht auf menschliches Eingreifen.

Insgesamt lässt sich festhalten, dass die Nutzung zulassungsbeschränkter Systeme und/oder das Heraushalten personenbezogener Daten aus der Blockchain aus Sicht des

[5] Auch Sachdaten genannt, siehe Klar/Kühling, in: Kühling/Buchner, DS-GVO BDSG, Art. 4 Nr. 1 DSGVO, Rn. 12; Fries/Scheufen, MMR 2019, 721, 723.
[6] Arning/Rothkegel, in: Taeger/Gabel, DSGVO BDSG, Art. 4 DSGVO, Rn. 16.
[7] Finck, Blockchain and the General Data Protection Regulation, S. 43.
[8] Finck, Blockchain and the General Data Protection Regulation, S. 48; Lyons et al., Blockchain and the GDPR, S. 18.
[9] Siehe hierzu etwa Bechtolf/Vogt, ZD 2018, 66, 69; Blockchain Bundesverband, Blockchain, data protection and the GDPR, S. 6; Boehme/Pesch, DuD 2017, 473, 479; Finck, EDPL 2018, 17, 26; Lyons et al., Blockchain and the GDPR, S. 18; Martini/Weinzierl, NVwZ 2017, 1251, 1253 ff.
[10] Quiel, DuD 2018, 566, 571.
[11] Finck, EDPL 2018, 17, 29 f.
[12] Bundesamt für Sicherheit in der Informationstechnik, Blockchain sicher gestalten, S. 39 f.
[13] Finck, EDPL 2018, 17, 26; vgl. auch Artikel-29-Datenschutzgruppe, Stellungnahme 5/2014 (WP216, 0829/14/DE).
[14] Finck, Blockchain and the General Data Protection Regulation, S. 35 f.
[15] Ateniese et al., Redactable Blockchain – or – Rewriting History in Bitcoin and Friends.
[16] Zum Ganzen siehe Finck, Smart Contracts und Art. 22 DSGVO.

Datenschutzrechts aktuell die vielversprechendsten Lösungen darstellen.

Lösungsbedarf

Wie sich bei der Darstellung der Lösungsansätze bereits gezeigt hat, stellen sich noch viele datenschutzrechtliche Fragen, sodass in diesem Bereich erheblicher juristischer und interdisziplinärer Forschungsbedarf besteht. Neben den aufgeworfenen Fragen der Verantwortlichkeit, Rechtfertigung, Anonymisierung sowie der datenschutzrechtskonformen Gestaltung von Smart Contracts ist bisher kaum beachtet, inwiefern im Blockchain-Kontext die Bestimmungen zur Datenübermittlung an Drittländer (Art. 44 ff. DSGVO) einschlägig sind. Insbesondere bei zulassungsfreien Blockchains liegt es nahe, dass ein Transfer in Drittländer stattfindet.[17] In welcher Form sichergestellt werden kann, dass dieser rechtmäßig erfolgt, bedarf weiterer und vertiefter Auseinandersetzung.

Soweit regulatorische Anpassungen notwendig erscheinen, sollte eine erhebliche Absenkung des Datenschutzniveaus stets vermieden werden. Wünschenswert wären klarstellende Anpassungen der DSGVO bezüglich grundlegender Konzepte und die Aufnahme von Regelungen, die die Besonderheiten der Blockchain-Technologie berücksichtigen.

Abgesehen von gesetzlichen Anpassungen kommt der künftigen Rechtsprechung zu zentralen Aspekten der DSGVO erhebliche Bedeutung zu. Ein Großteil der rechtlichen Unsicherheit im Bereich des Datenschutzrechts rührt daher, dass es aufgrund der relativ neuen gesetzlichen Regelungen der DSGVO noch viele Rechtsfragen gibt, welche bisher nicht höchstrichterlich geklärt werden konnten. Die Rechtsprechung sollte daher stets aufmerksam verfolgt werden, weil sie in vielen Fällen erstmals rechtssichere Aussagen ermöglichen wird. Besonderer Fokus sollte dabei auch auf Entscheidungen liegen, die Rückschlüsse bezüglich der Besonderheiten der Blockchain-Technologie erlauben.

Literatur

Artikel-29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken (WP216, 0829/14/DE); Ateniese et al., Redactable Blockchain – or – Rewriting History in Bitcoin and Friends, 2017 IEEE European Symposium on Security and Privacy, 111; Bechtolf/Vogt, Datenschutz in der Blockchain – Eine Frage der Technik, ZD 2018, 66; Blockchain Bundesverband, Blockchain, data protection and the GDPR; Boehme/Pesch, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, DuD 2017, 473; Bundesamt für Sicherheit in der Informationstechnik, Blockchain sicher gestalten; Erbguth, Wann sind kryptografische Hashwerte von personenbezogenen Daten selbst wieder personenbezogene Daten?, MMR 2019, 654; Finck, Blockchain and the General Data Protection Regulation - Study for the Panel for the Future of Science and Technology; Finck, Blockchains and Data Protection in the European Union, EDPL 2018, 17; Finck, Smart Contracts und Art. 22 DSGVO (Automatisierte Entscheidungen im Einzelfall), in: Braegelmann/Kaulartz (Hg.), Rechtshandbuch Smart Contracts, S. 195 ff.; Fridgen et al., Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik; Janicki/Saive, Privacy by Design in Blockchain-Netzwerken, ZD 2019, 251; Lyons et al., Blockchain and the GDPR - A thematic report prepared by the European Union Blockchain Observatory & Forum; Martini/Weinzierl, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251; Quiel, Blockchain-Technologie im Fokus von Art. 8 GRC und DS-GVO, DuD 2018, 566.

Forschungseinrichtungen

Juristische Forschungseinrichtungen mit Schwerpunkt im Datenschutz- bzw. Informationstechnologierecht. Forschungseinrichtungen für Informatik und Informationssicherheit zur Ausarbeitung und Überprüfung der technischen Umsetzung datenschutzkonformer Gestaltungen. Interdisziplinäre Forschungseinrichtungen an der Schnittstelle zwischen Recht und Technik.

[17] Finck, EDPL 2018, 17, 28; Lyons et al., Blockchain and the GDPR, S. 26.