Blockchain und Datenschutz: Widerspruch oder Chance?

27.03.2020, 13:56 | Politik, Recht & Gesellschaft

Pressemitteilung von: *Schürmann Rosenthal Dreyer Rechtsanwaelte*

Betrachtet man die Eigenschaften und die Funktionsweise von Blockchains, erscheint es auf den ersten Blick nicht unbedingt naheliegend, dass es Schwierigkeiten mit dem Datenschutzrecht geben könnte. Schließlich werden in der Regel nur Hashwerte, also Zahlenfolgen, auf der Blockchain gespeichert. Fehlt es nicht bereits am für die Anwendbarkeit der DSGVO notwendigen Bezug zu einer konkreten Person, deren Daten es zu schützen gilt? Art. 4 Nr. 1 DSGVO besagt allerdings, dass personenbezogene Daten alle Informationen sind, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Sie gilt also auch bei pseudonymisierten Daten, das heißt solchen, deren Zuordnung zu einer Person erst mit Heranziehung weiterer Informationen möglich ist. Je nach Ausgestaltung der Blockchain kann dies durchaus der Fall sein.

Bei einer privaten Blockchain, die im Gegensatz zur öffentlichen Blockchain nicht für jedermann zugänglich ist, sondern im Eigentum und unter der Verwaltung einer zentralen Stelle steht, kann über die Vergabe der Nutzerkennung die dahinterstehende Person identifiziert werden. Möglichkeiten zur Identifizierung gibt es aber auch bei öffentlichen Blockchains. Beispielsweise kann es sein, dass ein Teilnehmer die Dienste Dritter nutzt und dabei Informationen preisgibt, die Rückschlüsse auf seine Person zulassen. Tätigt er zum Beispiel einen Online-Kauf, der mittels Blockchain-Transaktion bezahlt wird, kann es sein, dass der verwendete Schlüssel, die Wallet, von der die Transaktion ausging, und die Lieferadresse miteinander in Verbindung gebracht werden. Analysen durch Big Data und die Ermittlung der IP-Adresse des teilnehmenden Rechners, über die die Person festgestellt werden kann, sind ebenso zu berücksichtigen. Somit kann man in der Regel von einem mittelbaren Personenbezug der auf der Blockchain gespeicherten Transaktionen ausgehen.

Verwendet man über eine Blockchain Anwendungen wie Smart Contracts, die ihrer Aufgabe nach personenbezogene Daten verarbeiten, ist die DSGVO ohnehin zu berücksichtigen. Welche Eventualitäten jeweils bestehen, sollte genau geprüft werden, um Probleme im Nachhinein zu vermeiden. Ist das Datenschutzrecht aufgrund des Personenbezugs anwendbar, kann der Einsatz von Blockchain-Technologie sicherlich als Herausforderung bezeichnet werden. Im Folgenden sollen einige der wichtigsten Problemfelder und einige Lösungsansätze vorgestellt werden.

Anonymisierung statt Pseudonymisierung?

Im ersten Schritt könnte man daran denken, den Anwendungsbereich der DSGVO auszuschließen, indem man die Daten anonymisiert. Im Gegensatz zu pseudonymisierten Daten kann die dahinterstehende Person mit anonymisierten Daten auch unter Heranziehung weiterer Informationen nicht mehr ermittelt werden. Eine Möglichkeit könnte sein, die Zuordnungsdaten zu löschen, die den Schlüssel, mit dem die Daten auf der Blockchain verschlüsselt wurden, mit einer konkreten Person verknüpfen. Doch bei der vorschnellen Annahme einer „Anonymisierung“ ist Vorsicht geboten. Es kann sein, dass sich die Person doch noch mit einem gewissen Aufwand anhand des vermeintlich anonymen Datensatzes ermitteln lässt. Dies ist zum Beispiel der Fall, wenn die betroffene Person mehrere Transaktionen getätigt hat und sich durch Kombination der Schluss zu einer bestimmten Person ziehen lässt. Eine vermeintliche Anonymisierung ist daher selten das Mittel der Wahl.

Die DSGVO ist zu beachten: Wer spielt welche Rolle bei Blockchains?

Auch für Technologien wie Blockchain gibt es keine Ausnahme in Bezug auf die aufsichtsrechtlichen Anforderungen: Die DSGVO und alle weiteren datenschutzrechtlichen Bestimmungen müssen vollumfänglich umgesetzt werden. Dazu gehören allgemeine Zielvorgaben für den Datenschutz und die Wahrung der sog. Betroffenenrechte, worauf weiter unten noch eingegangen wird. Doch zunächst ergeben sich im Rahmen von Blockchains Schwierigkeiten bereits bei den grundlegenden Fragen, etwa bei der Bestimmung, wer die datenschutzrechtlich verantwortliche Stelle ist und die Vorgaben der DSGVO umzusetzen hat. Dies ist nicht nur von allgemeinem Interesse, sondern auch notwendig, um die

Informationspflichten gegenüber den betroffenen Personen einhalten zu können. Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO die Stelle, die „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet."

Bei einem dezentralisierten System wie einer (öffentlichen) Blockchain ist die Ermittlung eines Verantwortlichen per se nicht einfach. Je nach Anwendungsfall und Art der Blockchain können der Anbieter der Anwendung und die teilnehmenden Rechner, die Transaktionen tätigen und somit Informationen in die Blockchain bzw. die Kopie auf ihrem teilnehmenden Rechner eingeben, als Verantwortliche in Betracht kommen. Hier kann je nach Einzelfall auch eine sogenannte gemeinsame Verantwortlichkeit nach Art. 26 DSGVO vorliegen, sodass eine entsprechende Vereinbarung abgeschlossen werden muss. In privaten oder zulassungsbeschränkten öffentlichen Blockchains gibt es hingegen zumeist doch eine zentrale Stelle, die dann als Verantwortlicher anzusehen ist.

Integrität und Vertraulichkeit einer Blockchain

Die DSGVO enthält eine Vielzahl verschiedener Grundsätze für die Verarbeitung personenbezogener Daten, die der bzw. die Verantwortliche(n) umzusetzen haben. Dazu gehören unter anderem die in Art. 5 Abs. 1 Buchstabe f DSGVO genannten Grundsätze der Integrität und Vertraulichkeit von Daten. Diese betreffen die grundsätzliche Sicherheit der betreffenden Daten. Der Verantwortliche muss sie mit geeigneten technischen und organisatorischen Maßnahmen vor unbefugter Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung und Schädigung schützen. Die Integrität der Daten ist gewährleistet, wenn diese nicht unrechtmäßig oder unbemerkt manipuliert werden können. Ihre Vertraulichkeit ist gewährleistet, wenn niemand unbefugt die Daten einsehen kann.

Im Rahmen einer Blockchain lassen sich diese Grundsätze teilweise relativ gut und teilweise nicht ohne Weiteres umsetzen. Indem die einzelnen Blöcke der Kette mit Hashwerten versehen und miteinander verbunden werden, entsteht eine schlüssige Folge von Zahlenwerten, die bei der kleinsten Veränderung bereits nicht mehr aufgeht. Im Grundsatz bleibt daher festzuhalten, dass sich die Integrität der Daten in der Blockchain gut garantieren lässt.

Anders verhält es sich mit der Vertraulichkeit der Daten, die der Transparenz als zentraler Eigenschaft der Blockchain zu widersprechen scheint. Denn um die gewünschte Integrität und Manipulationssicherheit zu erreichen, müssen die Daten von allen Teilnehmern einsehbar sein, was gerade ein besonderer Mehrwert der Blockchain-Technologie ist. Sofern man die Daten nicht verwenden, sondern nur deren Existenz und Integrität sicherstellen möchte, beispielsweise wenn man sein geistiges Eigentum mittels Blockchain sichern möchte, können die unverschlüsselten Informationen extern vertraulich abgelegt werden. Dieses Verfahren eignet sich weniger, wenn man die unverschlüsselten Informationen verwenden möchte, um damit etwa Smart Contracts auszuführen. Hierfür gibt es verschiedene technische Lösungen, deren richtige Wahl vom konkreten Anwendungsfall abhängt. So gibt es beispielsweise die Möglichkeit, die Sichtbarkeit der Daten durch individuell eingerichtete, geschützte Laufzeitumgebungen zu beschränken.

Die Betroffenenrechte am Beispiel des Rechts auf Löschung

Die Herausforderungen, welche die Blockchain-Technologie in Bezug auf die Gewährleistung der Betroffenenrechte der DSGVO aufwirft, zeigen sich am deutlichsten am Beispiel des Rechts auf Löschung (oder auch Recht auf Vergessenwerden) nach Art. 17 DSGVO. Dieses Recht besteht, wenn einer der Gründe des Art. 17 Abs. 1 DSGVO vorliegt. Danach muss der Verantwortliche dafür sorgen, dass es keine Möglichkeit mehr gibt, die Daten, ohne unverhältnismäßig großen Aufwand einzusehen.

Das Recht auf Löschung kollidiert mit der Manipulationssicherheit der Blockchain. Um beim grundsätzlichen System der Blockchain zu bleiben, kann eine Löschung nur im Wege des Konsensmechanismus vorgenommen werden, indem die Mehrheit der Teilnehmer diese bestätigt. Einfacher liegt es beim verwandten Recht auf Berichtigung unrichtiger Daten, da Korrekturen von Informationen oder Transaktionen einfach durch eine weitere Transaktion auf der Blockchain vorgenommen werden können, die die alte berichtigt. Sollen Daten aber im obigen Sinne wirklich gelöscht werden, hilft ein weiterer Block nicht weiter, da die Information des vorigen Blocks, die gelöscht werden soll, nicht überschrieben wird und demnach weiterhin einsehbar bleibt. Die Unveränderbarkeit von Transaktionen durch die Verkettung der Blöcke ist gerade ein Wesensmerkmal der Blockchain. Um dennoch ein angemessenes Datenschutzniveau und somit die Praxistauglichkeit von Blockchain-Lösungen zu bewerkstelligen, gibt es auch hier eine Vielzahl technischer Lösungen,

deren Umsetzbarkeit allerdings von der jeweiligen Blockchain und vom jeweiligen Anwendungsfall abhängt.

Beim sogenannten „Forking“ werden praktisch zeitgleich zwei Blöcke erstellt, sodass ein Zweig gebildet werden kann, in welchem die zu revidierende Transaktion in der gewünschten Ausformung vorgenommen werden kann. Doch diese Vorgehensweise ist verhältnismäßig aufwändig und verursacht weitere Schwierigkeiten dabei, den entstandenen unerwünschten Nebenzweig auch tatsächlich zu löschen. Dieses Verfahren wird vor allem bei starken Sicherheitsvorfällen angewandt und ist beispielsweise bei der Ethereum-Blockchain verwendet worden. Nach einem Hack sollten die Regeln geändert werden, was nicht alle mittragen wollten. Nach dem Einfügen neuer Blöcke teilte sich die Blockchain in Ethereum mit den neuen und Ethereum Classic mit den alten Regeln. Aufgrund des Aufwands ist das Forking allerdings häufig nicht geeignet, datenschutzrechtliche Betroffenenrechte wirksam und effizient durchzusetzen.

In nicht-öffentlichen Blockchains ist es zudem möglich, eine Gruppe teilnehmender Rechner zu bestimmen, die unter bestimmten Bedingungen das Recht erhält, Informationen auf der Blockchain im Nachhinein zu ändern.
Bei der Dokumentation von Informationen oder der Speicherung von Zertifikaten sollte auf der Blockchain nur der Hashwert hinterlegt und die eigentliche Information extern gespeichert werden. Auf diese Weise lässt sich dem Recht auf Löschung am besten Genüge leisten.

Fazit und Ausblick

Neben den vorgestellten technischen Lösungen existieren weitere Ansätze, die datenschutzrechtliche Problematik im Zusammenhang mit Blockchains in den Griff zu kriegen. Auf der einen Seite wird diese Aufgabe immer eine Herausforderung bleiben, da es nicht nur technische Schwierigkeiten gibt, sondern in der Natur der Sache liegt, dass sich Widersprüche mit den typischen Blockchain-Funktionen ergeben. Gibt man einer bestimmten Partei oder Gruppe das Recht in die Hand, gesondert in die Blockchain einzugreifen, ändert sich das Vertrauensprinzip des Systems. Auf der anderen Seite darf und sollte abgewartet werden, welche Möglichkeiten sich noch in Zukunft auftun. In jedem Fall sollte je nach Anwendungsfall bedacht werden, wie viele der Wesensmerkmale der Blockchain aufgegeben werden können, ohne ihre Vorteile in zu weiten Teilen obsolet zu machen.

Neben technischen Ansätzen sollten auch rechtliche Wege beschritten werden, damit das Datenschutzrecht neue Technologien nicht unverhältnismäßig stark beschränkt. So könnten Schutzmaßnahmen wie die Pseudonymisierung der Daten in Verbindung mit entsprechender Information der betroffenen Personen als ausreichend betrachtet werden, sofern nicht besonders sensible und persönliche Daten betroffen sind. Das gilt umso mehr, da sich durch die Blockchain-Technologie auch neue Möglichkeiten für das Datenschutzrecht auftun. Die Unveränderlichkeit und vollständige Nachvollziehbarkeit sowie die Transparenz von Daten kann auch datenschutzrechtlich positiv genutzt werden. Hier bieten sich Chancen zum Beispiel bei der Umsetzung technisch-organisatorischer Maßnahmen. Festzuhalten bleibt, dass Blockchain und Datenschutz sich schnell in einem Spannungsverhältnis befinden können und Nutzer abwägen müssen, dass andererseits aber auch Lösungsansätze existieren, deren Ausbau in technischer wie rechtlicher Hinsicht in Zukunft wünschenswert ist und erwartet werden kann.

Portrait

SCHÜRMANN ROSENTHAL DREYER bietet Mandanten maßgeschneiderte juristische Strategien und Lösungen vor allem in den Bereichen Urheber-, Medien-, IT- und Wettbewerbsrecht, Handels- und Gesellschaftsrecht, Datenschutzrecht sowie im Bereich des Gewerblichen Rechtsschutzes. Namhafte Unternehmen und Organisationen vertrauen uns. Dazu zählen vor allem nationale und internationale Unternehmen, Markenhersteller, IT-, E-Commerce- und Technologieunternehmen, Unternehmen aus der Film-, Fernseh- und Medienbranche sowie Verlage und Agenturen.

Wir machen uns stark für unsere Mandanten und denken in Lösungen. Wir arbeiten über Grenzen hinweg und betreuen Projekte interdisziplinär, innovativ und rechtskonform.

News-ID: 1081885 • Views: 366 (Stand: 28.05.2026)

Link zur Pressemitteilung:

https://www.openpr.de/news/1081885/Blockchain-und-Datenschutz-Widerspruch-oder-Chance.html