Jürgen Taeger/Mihaela Drăgan/Sebastian Louven (Hrsg.)

Rechtsfolgen der Digitalisierung im rumänisch-deutschen Ländervergleich

Beiträge zur 2. Rumänisch-Deutschen Konferenz zum Europäischen Informationsrecht

OlWIR Oldenburger Verlag für Wirtschaft, Informatik und Recht

Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Gedruckt auf alterungsbeständigem säurefreiem Papier.

Oldenburger Verlag für Wirtschaft, Informatik und Recht
Rudolf-Kinau-Str. 54, 26188 Edewecht
mail@olwir.de

Edewecht 2018

ISBN: 978-3-95599-053-4

INHALT

Jürgen Taeger

Vorwort VII

Alexis Daj

DAOs und Blockchain-Technologien: Ökonomisches Potenzial und Regulatorische Herausforderungen von Smart Contracts und Virtual Currencies 1

David Saive

Unification through distribution? 17

Carmen Lupsan

Blockchain und die DSGVO 27

Cristiana Fernbach/Cătălina Fînaru

GDPR compliance in the Industry 4.0 33

Boris Reibach

Die Regulierung von Algorithmen unter der DSGVO 43

Dennis-Kenji Kipker/Sven Müller

Internationale Cybersecurity-Regulierung 51

Sebastian J. Golla

Robocop streift durch das Netz: Grundrechtseingriffe durch die automatisierte Unterstützung von Polizeiarbeit im Social Web 67

Thorsten Feldmann

Presse- und Öffentlichkeitsarbeit unter der DSGVO 81

Anna K. Bernzen

Der EuGH als Lehrmeister: Was deutsche Gerichte beim Umgang mit den Medien von internationalen Gerichten lernen können 89

Kathrin Schürmann

Location Based Advertising – Eine Analyse aus datenschutz- und wettbewerbsrechtlicher Sicht 105

Hans-Christian Gräfe

Werbung auf Online-Plattformen: Influencer Marketing 115

Sebastian Louven

Kartellrechtliche Grenzen des Informationsaustauschs 135

Anselm Brandi-Dohrn

German Supreme Court on licensing agreements: a new understanding of the legal nature of licensing contracts 145

Michaela Braun-Noviello

Elektronische Verträge im rumänischen Recht 155

Matthias Baumgärtel

Chancen für ländliche Räume aufgrund der WiFi4EU-Verordnung 167

BLOCKCHAIN UND DIE DSGVO

Av Carmen Lupsan

Stalfort Legal. Tax. Audit.
clupsan@stalfort.ro

Zusammenfassung

Blockchains erfreuen sich unter anderem wegen des Schutzes, den die unveränderbare Speicherung von Daten mit sich bringt, einer wachsenden Beliebtheit und werden immer mehr in unterschiedlichen Bereichen eingesetzt. Dadurch wird einerseits eine hohe Sicherheit für die gespeicherten Daten gewährleistet, andererseits aber ist durch die Natur der Blockchain die Gewährleistung bestimmter Rechte und Pflichten gem. der DSGVO (fast) unmöglich. Dieser Beitrag möchte einige Widersprüche zwischen Blockchain und DSGVO hervorheben und gleichzeitig einige existierende Lösungsansätze aufzeigen. Ferner ist die Erkenntnis wichtig, dass Blockchain zukünftig in immer mehr Bereichen angewendet wird und entsprechend eine Lösung für die Konformität mit der DSGVO gefunden werden muss. Hierbei wird eine enge Zusammenarbeit erforderlich sein, um technische Ansätze zu finden, die mithilfe der gesetzlichen Anpassungen die Blockchain in die DSGVO-Konformität befördern sollten.

1 Blockchain-Arten

Die Anwendbarkeit der DSGVO auf Blockchain kann nur im Kontext der unterschiedlichen Arten der Blockchains beurteilt werden. Hierbei ist insbesondere zwischen den öffentlichen und privaten Blockchains zu unterscheiden. Obwohl es auch komplexere Blockchain-Konstruktionen (z.B. Hybride zwischen öffentlichen und privaten Blockchains) gibt, wird nur auf diese zwei Arten eingegangen.

1.1 Unpermissioned Blockchains (öffentlich)

Unpermissioned Blockchains sind offen, dezentral und verteilt (*distributed ledger*) geführte Register. Jeder Teilnehmer am Blockchain, der Daten speichert und verarbeitet, hat dieselben Rechte und Befugnisse. Somit fügt jeder dieser Teilnehmer Informationen hinzu (neuer Block). Die Entscheidung über das Hinzufügen eines neuen Blocks wird durch Mehrparteienkonsens (*peer-to-peer consensus*) getroffen; alle Kopien werden daraufhin um diesen Block ergänzt.

1.2 Permissioned Blockchains (privat)

Permissioned Blockchains sind geschlossene (nur für bestimmte Teilnehmer zugängliche) Blockchains. Die Rechte und Befugnisse der Teilnehmer werden von einer zentralen Stelle eingeräumt. Dies bedeutet, dass bestimmte Teilnehmer berechtigt sind, neue Blocks hinzuzufügen, während

andere Teilnehmer lediglich die Befugnis haben, die Informationen einzusehen.

2 Blockchain im Rahmen der DSGVO

Während die DSGVO eine änderbare Speicherung von Daten fordert – z.B., um diese auf Anforderung der betroffenen Person ändern zu können, und von einem identifizierbaren Verantwortlichen und der Verarbeitung durch den Verantwortlichen oder einen Auftragsverarbeiter ausgeht, lebt die Blockchain gerade davon, dass die Daten unveränderbar und somit deren Verarbeitung als besonders sicher gelten. Hier gibt es nicht einen Verantwortlichen; jeder Teilnehmer kann vielmehr Blocks einfügen.

2.1 Was sind personenbezogene Daten im Blockchain?

Personenbezogene Daten werden im Blockchain (i) als Klartext, (ii) verschlüsselt oder (iii) durch Hashing verarbeitet. Während es eindeutig ist, dass Klartext und verschlüsselte Daten, die mit dem richtigen Schlüssel entschlüsselt werden können und somit auf die betroffene Person zurückzuführen sind, personenbezogene Daten darstellen, stellt sich die Frage, wie dies im Falle von Hashing zu deuten ist.

Eine Hashfunktion kann im Gegensatz zur Verschlüsselung nicht rückgängig gemacht werden. Obwohl das Hashing wesentlich sicherer als die Verschlüsselung ist, hat die WP 29 es ebenfalls als Pseudonymisierung ausgelegt und so behandelte Daten damit als personenbezogen gedeutet.[1]

Public keys, die im Rahmen der Transaktionen genutzt werden, obwohl sie nicht mehr einer bestimmten Person zugeordnet werden können, sind ebenfalls personenbezogene Daten, weil diese mithilfe der private keys wieder bestimmten Personen zugeordnet werden können.

2.2 Wer ist Verantwortlicher?

Der Verantwortliche gem. der DSGVO ist derjenige, der über den Zweck und das Mittel der Verarbeitung entscheidet. Die DSGVO geht davon aus, dass Daten entweder von einem Verantwortlichen oder von einem Auftragsverarbeiter verarbeitet werden.

Sollte es im Rahmen einer permissioned Blockchain möglich sein, unter Umständen die zentrale Stelle, die Teilnehmern Rechte und Befugnisse erteilt, als Verantwortlichen zu sehen, so ist es im Falle der unpermissioned Blockchains unmöglich, einen Verantwortlichen zu finden. Verantwortlicher können entweder alle oder kein Teilnehmer (Knoten) sein. Aus diesem Grund ist es auch schwierig, die Rechte und Pflichten sowie die durch

[1] WP 29 Opinion 5/2014 on Anonymisation Techniques, Pkt 4.

die DSGVO eingeräumten Grundsätze in der Blockchain umzusetzen und einzuhalten. Weiterhin stellt sich in dieser Situation auch die Frage der Haftung und Haftbarkeit. Eine unpermissioned Blockchain ist keine Rechtsperson als solche.

2.3 Beispiele von DSGVO-Grundsätzen, die nicht (oder nur schwierig) im Blockchain umgesetzt werden können

Aufgrund der unveränderbaren Speicherung von Daten in der Blockchain ist es fast unmöglich, die aufgrund der DSGVO (und übrigens auch zuvor) einzuhaltenden Grundsätze in der Blockchain umzusetzen. Aus diesem Grund ist es sehr wichtig, bestimmte technische Lösungen zu finden, die die große Kluft zwischen der DSGVO und Blockchain einigermaßen verringert.

2.3.1 Berichtigung und Löschung personenbezogener Daten

Aufgrund der Unveränderbarkeit der Blocks ist eine Berichtigung oder Löschung auf Anfrage der betroffenen Person nicht möglich. Blockchain lässt die Änderung eines Blocks nicht zu; es kann lediglich ein neuer berichtigender Block hinzugefügt werden. Dies bedeutet jedoch, dass auch die frühere Information weiterhin in der Blockchain bestehen bleibt und für alle sichtbar ist. Folgende Lösungsansätze wurden unter anderem angesprochen:

2.3.1.1 Off-chain Storage

Als Lösungsansatz wird die Aufbewahrung der personenbezogenen Daten außerhalb der unpermissioned Blockchain (*off-chain storage*) angesprochen. Dies ermöglicht es, von der zentralen Stelle die personenbezogenen Daten zu ändern, die in einer unpermissioned Blockchain nur mit einem Hashpointer verbunden und somit nicht im unpermissioned Blockchain gespeichert sind.

2.3.1.2 Redactable Blockchain

In einer redactable Blockchain kann die Hash-Verbindung aufgetrennt und der alte Block mit einem neuen geänderten Block ersetzt werden. Die Bearbeitung bleibt für alle ersichtlich (wie eine Narbe), zum alten Block erhalten jedoch nur die Teilnehmer, die an der Änderung beteiligt waren, Zugang. Somit sind die alten Informationen/Daten auch nur für diese ersichtlich.

2.3.1.3 Löschung des private key

Für die Löschung der personenbezogenen Daten wird schließlich die Löschung des private keys als Lösung betrachtet. Infolgedessen bleiben zwar die Daten in der Blockchain bestehen, der Zugang zu diesen Daten wird jedoch gesperrt. Obwohl dies keine Löschung im Sinne der DSGVO ist, muss unter Berücksichtigung der Merkmale einer Blockchains allerdings

auch angemerkt werden, dass die Rechte auf Berichtigung und Löschung der personenbezogenen Daten keine absoluten Rechte sind. Eine solche Lösung könnte durchaus als angemessene Maßnahme erachtet werden, was aber entsprechend vom Gesetzgeber bzw. vom Europäischen Datenschutzausschuss berücksichtigt und geregelt werden sollte.

2.3.2 Auskunftsrecht

Sollte eine betroffene Person, die nicht Teilnehmer an der Blockchain ist, wissen wollen, welche ihrer personenbezogenen Daten verarbeitet werden, so müsste sie der Blockchain beitreten, um so eine Kopie aller in der betreffenden Blockchain gespeicherten Daten zu erhalten. Ob dies als Auskunftsrecht unter der DSGVO gedeutet werden kann, ist allerdings fraglich.

2.3.3 Datenminimierung

Die personenbezogenen Daten müssen entsprechend eines festgelegten, eindeutigen und legitimen Zweckes verarbeitet werden und die Verarbeitung muss auf ein notwendiges Maß beschränkt sein. Hier sind die Schwierigkeiten ähnlich mit denjenigen, die unter Punkt 2.3.1 angesprochen wurden.

2.3.4 Speicherbegrenzung

Aufgrund des für die Blockchain essenziellen Merkmals der Transparenz ist eine Löschung nach Ablauf einer bestimmten Zeit nicht möglich.

2.4 Blockchain im Alltag

Obwohl die oben dargestellten Diskrepanzen zwischen Blockchain und DSGVO existieren, wird die Blockchain im Alltag immer häufiger in unterschiedlichen Situationen eingesetzt:

2.4.1 Blockchain in der Logistik

Gesellschaften mit Tätigkeiten im Bereich Logistik testen Blockchain, um einerseits eine höhere Effizienz durch die Verfolgung der Güter zu gewährleisten und andererseits die Zurückverfolgung der Lieferkette durch den Verbraucher zu erlauben. Nicht zuletzt ermöglicht dies, den Stand der Waren zu verfolgen und die Transparenz im Rahmen des Zollaufenthaltes zu erhöhen.

2.4.2 eHealth

Estland hat in seinem medizinischen System die Blockchain eingeführt. Patientendaten werden außerhalb der Blockchain eingetragen. Wenn auf Daten zugegriffen wird oder diese geändert werden, wird die entsprechende Aktivität in der Blockchain eingetragen und eine „keyless signature“ neben den Eintragungen gespeichert. Diese Signaturen dienen als elektronischer Zeitstempel, der beweist, wann Änderungen vorgenommen wurden.

2.4.3 Blockchain für bestimmte Sicherheiten

Frankreich hat einen Rechtsrahmen für die Verwendung der Blockchain-Technologie bei der Registrierung und Übertragung nicht-börsennotierter Sicherheiten geschaffen.

2.4.4 Bankdaten der Kunden im Blockchain

Immer mehr Banken aus Polen wollen in ihrem System Blockchain für eine Speicherung und einen sicheren Zugriff auf sensible Kundendaten implementieren. Diese Blockchain-Technologie ist eine Lösung, die eine vollständige Transparenz garantiert und eine nachvollziehbare Historie sowie den Zugriff auf alle kundenbezogenen Daten gewährleistet. Zusätzlich sei sie, so Billon, der Entwickler dieser DLT-Technologie DSGVO-konform, obwohl sie auf Blockchain-Technologie basiert.

2.4.5 Digitale Identität und e-voting

Durch Blockchain hat die Stadt Zug einerseits die Möglichkeit für ihre Bürger eingeräumt, eine E-ID zu erhalten, und andererseits ein elektronisches Abstimmungssystem implementiert.

Literatur

Finck, Michèle: Blockchains and Data Protection in the European Union, Max Planck Institute for Innovation and Competition Research Paper No. 18-01.

Marnau, Ninja: Die Blockchain im Spannungsverhältnis der Grundsätze der Datenschutzgrundverordnung, Informatik 2017, S. 1025-1036.

Salmensuu Cagla: The General Data Protection Regulation and Blockchains (January 1, 2018), Liikejuridiikka 1/2018.