Blockchain und DSGVO:

Datenschutzrechtliche Herausforderungen

Bild: Golden Bitcoin with judge hammer von Marco Verch unter Creative Commons 2.0

Alexander Bauer I Dipl.-Jur. I Wissenschaftl. Mitarbeiter am Fraunhofer FIT I Doktorand am ITM der WWU Münster

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

Ziel des Vortrags

Ziel: Sensibilisierung für die grundsätzlichen Herausforderungen der DSGVO an die Entwicklung von Blockchain-Applikationen.

1. Tragweite der DSGVO
2. Problemfelder – Einführung
3. Anwendbarkeit der DSGVO
4. Verantwortlichkeit
5. Betroffenenrechte
6. Zusammenfassung

Alexander Bauer I Dipl.-Jur. I Wissenschaftl. Mitarbeiter am Fraunhofer FIT I Doktorand am ITM der WWU Münster

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

1. Tragweite der DSGVO

- Als EU-Verordnung direkte (unmittelbare) Geltung (Art. 288 AEUV) im EU-Raum.
- Schutz des Art. 8 der EU-Grundrechtecharta – „Recht des Schutzes der personenbezogenen Daten“.
- Schutzwirkung endet nicht zwingend an den EU-Außengrenzen, vgl. Art. 3 DSGVO.

Alexander Bauer I Dipl.-Jur. I Wissenschaftl. Mitarbeiter am Fraunhofer FIT I Doktorand am ITM der WWU Münster

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

2. Problemfelder – Einführung

- Die Kompatibilität zwischen der Blockchain-Technologie und der DSGVO kann immer nur von Fall zu Fall unter Berücksichtigung der jeweiligen technischen und kontextabhängigen Faktoren bestimmt werden.

- Aufgrund des Zusammenspiels bestimmter Elemente der Technologie und des rechtlichen Rahmens können aber allgemeine Problemfelder identifiziert werden, die im Folgenden vorgestellt werden sollen.

Alexander Bauer I Dipl.-Jur. I Wissenschaftl. Mitarbeiter am Fraunhofer FIT I Doktorand am ITM der WWU Münster

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

3. Anwendbarkeit der DSGVO

- In sachlicher Hinsicht muss (1) die Verarbeitung von (2) personenbezogenen Daten vorliegen.
- Der Begriff der Verarbeitung (Art. 4 Nr. 2 DSGVO) ist weit zu verstehen.
- Der EuGH hat bestätigt, dass „*darunter die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung von Daten*“ zu verstehen ist (EuGH, Rechtssache C -101/01 – *Lindqvist*), somit faktisch jeder Umgang.
- Das erstmalige Einfügen von personenbezogenen Daten auf eine Blockchain, die weitere Speicherung, Bereitstellung und Weiterverarbeitung ist demnach eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO.

Alexander Bauer I Dipl.-Jur. I Wissenschaftl. Mitarbeiter am Fraunhofer FIT I Doktorand am ITM der WWU Münster

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

3. Anwendbarkeit der DSGVO

- Größere Probleme bereitet hingegen der Begriff der personenbezogenen Daten nach Art. 4 Nr. 1 DSGVO

„identifizierte“

Identität unmittelbar erkennbar
(z. B. Klarnamen)

„identifizierbare“

Zuordnung der Daten nicht direkt,
aber mit Zusatzwissen möglich

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

3. Anwendbarkeit der DSGVO

Hauptproblem: Was ist der Maßstab der Identifizierbarkeit nach Art. 4 Nr. 2 DSGVO?

1) Auf wen und was ist abzustellen?

→ alle Mittel sind zu berücksichtigen, „*die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren*“ (Erwägungsgrund 26).

2) Müssen alle notwendigen Informationen bei einer Person konzentriert sein?

→ laut EuGH müssen nicht alle zur Identifizierung notwendigen Mittel bei einer Person liegen. Es genügt, dass diese Person über rechtliche Mittel verfügt, um diese Informationen zu erhalten (EuGH, Rechtssache C-582/14 – *Breyer*).

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

3. Anwendbarkeit der DSGVO

Betrachtung der üblicherweise auf der Blockchain verwendeten Daten:

1) Klarnamen etc. → personenbezogene Daten im Sinne der DSGVO.
2) Transaktionsdaten → verschiedene Arten von Daten, die bei Transaktionen übermittelt werden können, daher im Einzelfall möglich.
3) Public Keys → dahinterstehende Person nicht direkt erkennbar, aber mittels Gesamtschau mit zusätzlichen Informationen Personenbezug ggf. herstellbar.
4) Hashwerte von personenbezogenen Daten → Anonymisierung nur dann, wenn die Identifizierung „*vernünftigerweise unmöglich geworden*“ ist (so laut Artikel-29-Datenschutzgruppe). Risiken sind aber v. a. Verknüpfbarkeit, Herausgreifen und Inferenz. Dann lediglich Pseudonymisierung, die vom Anwendungsbereich der DSGVO umfasst ist.

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

3. Anwendbarkeit der DSGVO

Weitere Betrachtung der üblicherweise auf der Blockchain verwendeten Verfahren:

5) Verschlüsselung → ebenfalls lediglich pseudonymisierte Daten, solange die Schlüssel für das Auslesen existieren.

6) Anonymisierungstechniken wie Mixing, Ring-Signaturen und Zero-Knowlege-Verfahren → sind hinsichtlich ihrer Zuverlässigkeit umstritten (BSI) und nicht bei jedem Blockchain-Design erwünscht.

→ Ein weiterer Aspekt ist, dass die unveränderliche Speicherung auf einer Blockchain besonders relevant ist, sodass der Aspekt der Langzeitsicherung von Daten im Hinblick auf künftige Technologien besonders ins Gewicht fällt.

→ Maßgeblicher Zeitpunkt der Bewertung ist zwar die Verarbeitung. Dabei sind aber zumindest absehbare technologische Entwicklungen einzukalkulieren (Piltz, K&R 2016, S. 557 (561).

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

4. Verantwortlichkeit im Sinne der DSGVO

Bestimmbarkeit des Verantwortlichen nach der DSGVO nicht einheitlich möglich

→ dieser ist aber der Adressat der datenschutzrechtlichen Pflichten!

Zentrale Norm ist Art. 4 Nr. 7 DSGVO:

„„Verantwortlicher“ [ist] die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; […]“

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

4. Verantwortlichkeit im Sinne der DSGVO

Unterscheidung nach Art der Blockchain notwendig

Private Blockchain mit einer zentralen Stelle

Verantwortlicher ist die zentrale Stelle

Private Blockchain mit einem Konsortium (zust. v. Governance)

Verantwortlicher ist das entscheidende Konsortium nach Art. 26 DSGVO

Public permissionless Blockchain

Unklar, wohl aber Nutzer, die fremde (Transaktions-) Daten in die Blockchain einstellen

Alexander Bauer I Dipl.-Jur. I Wissenschaftl. Mitarbeiter am Fraunhofer FIT I Doktorand am ITM der WWU Münster

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

5. Betroffenenrechte

- Recht auf Berichtigung, Art. 16 DSGVO: Berichtigung unrichtiger (S. 1) / Vervollständigung unvollständiger personenbezogener Daten (S. 2)
- Recht auf Löschung, Art. 17 DSGVO: Recht auf unverzügliche Löschung der personenbezogenen Daten (Abs. 1) / Recht auf Vergessenwerden (Abs. 2)

→ Eingriff in den Datenbestand

Geltendmachung dieser Rechte  Charakter der Blockchain-Technologie

Alexander Bauer I Dipl.-Jur. I Wissenschaftl. Mitarbeiter am Fraunhofer FIT I Doktorand am ITM der WWU Münster

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

5. Betroffenenrechte

Lösungsmöglichkeiten?

1) Hard Forking (-)
2) Rückwirkende Änderung von Blöcken durch privilegierte Knoten (Rollback)
3) Einsatz von sog. Chameleon-Hashes

→Bei Blockchain-Designs mit unkontrollierter Konsensfindung sind solche Lösungsmöglichkeiten kaum zu implementieren.

→Nachteile sind dabei der Integritätsverlust sowie neue Angriffs- und Missbrauchspotenziale.

→Off-Chain-Speicherung und Nachweis der Existenz der Daten mittels Hashing ist auch mit datenschutzrechtlichen Risiken belegt.

Alexander Bauer I Dipl.-Jur. I Wissenschaftl. Mitarbeiter am Fraunhofer FIT I Doktorand am ITM der WWU Münster

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

5. Betroffenenrechte

- Recht auf Auskunft, Art. 15 DSGVO: Recht auf Transparenz

→ Kein Problem bei public Blockchains oder generell bei Leserechten

→ Informationen über verarbeitende Stellen, Empfänger, Verarbeitungszwecke oder Ähnliches aber problematisch, wenn bspw. bei public permissionless Blockchains aufgrund fehlender Regulierung keine validen Auskünfte möglich sind (BSI, Blockchain sicher gestalten, S. 62).

- Recht auf Datenübertragung, Art. 20 DSGVO: Recht auf Kontrolle

→ Problematisch ist das Format der Daten (Abs. 1), da sie in einer strukturierten, gängigen und maschinenlesbaren Form erhalten werden müssen (Piltz, in: Gola, DSGVO, Art. 20, Rn. 21). Unklar, ob dies bei public Blockchains schon der Fall ist. Zudem würde bei off-Chain-Speicherung eine weitere Verpflichtung entstehen.

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER

6. Zusammenfassung

- Die DSGVO-Konformität stellt eine der größten rechtlichen Herausforderungen für die Entwicklung von Blockchain-Applikationen dar.
- Eine genaue Prüfung der jeweiligen Blockchain-Applikation auf ihre DSGVO-Konformität ist daher regelmäßig sinnvoll.
- Ein Augenmerk sollte dabei vor allem bei den auf der Blockchain abgelegten Daten, der genauen Identifikation des Verantwortlichen innerhalb des jeweiligen dezentralen Netzwerks und der Möglichkeit der Geltendmachung von Betroffenenrechten liegen.
- Idealerweise werden schon beim Design von Blockchain-Applikationen die gängigen datenschutzrechtlichen Herausforderungen beachtet.

Alexander Bauer I Dipl.-Jur. I Wissenschaftl. Mitarbeiter am Fraunhofer FIT I Doktorand am ITM der WWU Münster

Gefördert durch das Land Nordrhein-Westfalen
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
BLOCKCHAIN REALLABOR RHEINISCHES REVIER