www.jusletter-it.eu

Stephan Cejka / Franz Zeilinger / Peter Stern / Mark Stefan / Ksenia Poplavskaya / Gregor Taljan / Julia Petek

Datenschutz in Blockchain-basierten Erneuerbaren-Energie-Gemeinschaften

Darstellung anhand des Ansatzes im Projekt «Blockchain Grid»

Im Rahmen der Erneuerbare-Energien-Richtlinie werden Erneuerbare-Energie-Gemeinschaften (EEG) vorgesehen, die durch den Austausch lokal erzeugter Energie die Nutzung erneuerbarer Energie erhöhen sollen. Im österreichischen Projekt «Blockchain Grid» wird eine EEG über einen Blockchain-basierten Ansatz realisiert und in einem umfassenden Feldtest validiert. Die Autoren beleuchten in diesem Beitrag die Herausforderungen des Betriebs einer EEG in Bezug auf den Datenschutz und stellen die im Projekt entwickelte datenschutzfreundliche Umsetzung einer Blockchain-Anwendung vor.

Kategorie: Wissenschaftliche Beiträge
Region: Österreich
Rechtsgebiete: Blockchain; Datenschutz

Zitiervorschlag: Stephan Cejka / Franz Zeilinger / Peter Stern / Mark Stefan / Ksenia Poplavskaya / Gregor Taljan / Julia Petek, Datenschutz in Blockchain-basierten Erneuerbaren-Energie-Gemeinschaften, in: Jusletter IT 26. September 2019

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

1. Einleitung

[1] Im derzeitigen Hype um die Blockchain-Technologie und den zahllosen Projekten, die sich mit dieser befassen oder diese einsetzen, wird nicht immer auf die rechtlichen Rahmenbedingungen Rücksicht genommen. Auch wenn bisher keine speziellen Rechtsnormen zur Blockchain-Technologie existieren, bewegt man sich nicht im rechtsfreien Raum und es ist daher zu untersuchen, inwiefern bereits bestehende Rechtsnormen auf Blockchain-Anwendungen angewendet werden können.[1] Insbesondere im Datenschutzrecht ist hierbei ein Spannungsfeld festzustellen, womit sich bereits einige Autoren früherer Beiträge[2], aber auch die ersten nationalen Datenschutzbehörden[3] beschäftigt haben. Blockchain-Technologie wird in den verschiedensten Anwendungsfällen eingesetzt oder diskutiert[4], u.a. auch in der Energiewirtschaft.[5] In diesem Artikel soll konkret die im Projekt «Blockchain Grid»[6] entwickelte datenschutzfreundliche Umsetzung einer

1 Sofie Schock, Ausgewählte rechtliche Aspekte der Blockchain-Technologie *in* Philip Raffling/Sofie Schock, Digitale Wirtschaft und Industrie 4.0, Manz, 2018, S. 177.

2 Beispielsweise: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom), Blockchain und Datenschutz – Faktenpapier, 2017, https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf (zuletzt abgerufen am 28.08.2019); Rainer Böhme/Paulina Pesch, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, DuD, 2017, 473; Michèle Finck, Blockchains und Data Protection in the European Union, European Data Protection Law Review, 4, 1, 17-35, 2018; Ninja Marnau, Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung, INFORMATIK 2017, Lecture Notes in Informatics (LNI), 2017, 1025.

3 NAIH (Ungarn), http://naih.hu/files/Blockchain-Opinion-2018-01-29.pdf (zuletzt abgerufen am 28.08.2019); CNIL (Frankreich), https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf (zuletzt abgerufen am 28.08.2019).

4 Fran Casino/Thomas Dasaklis/Constantinos Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues, Telematics and Informatics, 36, 55-81, 2019.

5 Merlinda Andoni/Valentin Robu/David Flynn/Simone Abram/Dale Geach/David Jenkins/Peter McCallum/Andrew Peacock, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, Renewable and Sustainable Energy Reviews, 100, 143-174, 2019.

6 Projekt «Blockchain Grid», FFG Projektnummer 3089755, (https://projekte.ffg.at/projekt/3089755, zuletzt abgerufen am 28.08.2019).

Blockchain-Anwendung in einer lokalen Erneuerbaren-Energie-Gemeinschaft (EEG) beschrieben werden.

2. Blockchain

[2] Eine kurze, dennoch sehr prägnante Definition der Blockchain gibt Hosp als «eine digitale Datei, in der dieselben Information von allen Mitgliedern einer Gesellschaft abgespeichert und Updates in regelmäßigen Zeitblöcken an die bereits bestehende Information gehängt werden, sodass jeder Teilnehmer die gesamte Information besitzt und sich nicht auf andere verlassen muss».[7] Dabei können Blockchains hinsichtlich der beteiligten Akteure eingeteilt werden in:

- Permissionless Blockchains, in welchen die Teilnehmer nicht beschränkt sind; eine zentrale Stelle ist per Design nicht vorgesehen.
- Permissioned Blockchains, in welchen der Kreis der Teilnehmer beschränkt ist und daher ein Verwalter als (zentrale) Stelle erforderlich ist.

[3] In weiterer Folge wird sich zeigen, dass es bei diesen Ausprägungen insbesondere Unterschiede bei der Frage nach der datenschutzrechtlichen Verantwortlichkeit gibt.[8]

[4] Jeder Teilnehmer speichert und verarbeitet hierbei seine eigene Kopie der Blockchain. Da Blockchains nur das Anhängen von neuen Daten erlauben, nicht jedoch das Modifizieren oder Löschen alter Daten, ist einerseits eine hohe Integrität gewährleistet, andererseits eröffnet sich hiermit ein Spannungsverhältnis mit Grundsätzen des Datenschutzes und Rechten der von der Datenverarbeitung Betroffenen. In jedem Anwendungsfall muss im Vorhinein überprüft werden, ob die Verwendung einer Blockchain-Technologie in concreto hilfreich und notwendig ist – insbesondere deshalb, weil durch den derzeitigen Hype viele Anwendungen auf Blockchain-Technologien setzen, obwohl diese mit klassischen IT-Technologien gelöst werden könnten. Ein wesentlicher Vorteil der Blockchain-Nutzung kann dabei unter anderem die Verwendung von Smart Contracts sein. Dies sind Programme, die in der Blockchain gespeichert sind und auf deren Knoten automatisiert ablaufen, wenn die Bedingungen dafür eintreten.

3. Erneuerbare-Energie-Gemeinschaften

[5] Erneuerbare-Energie-Gemeinschaften (EEG) sind eine Erweiterung der bereits im österreichischen Elektrizitätswirtschafts- und -organisationsgesetz 2010 (ElWOG 2010)[9] geregelten gemeinschaftlichen Erzeugungsanlagen (Mieterstrommodelle), bei welchen derzeit gesetzlich weder der direkte Anschluss an Leitungsanlagen des Verteilnetzbetreibers, noch die Durchleitung eigenerzeugter Energie an Teilnehmer zulässig ist.[10] Diese sind damit auf eine Liegenschaft und übli-

7 Julian Hosp, Blockchain 2.0 – einfach erklärt – weit mehr als nur Bitcoin, FinanzBuch Verlag, 2018, S. 42.

8 Häufige erfolgende Einteilungen in öffentlich und private Blockchains sind für diesen Artikel nicht relevant.

9 Bundesgesetz, mit dem die Organisation auf dem Gebiet der Elektrizitätswirtschaft neu geregelt wird (Elektrizitätswirtschafts- und -organisationsgesetz 2010 – ElWOG 2010) BGBl I 110/2010 idF BGBl I 108/2017.

10 § 16a ElWOG 2010.

cherweise auf deren Photovoltaik-Anlage eingeschränkt.[11] EEG werden nun durch die Erneuerbare-Energien-Richtlinie[12] vorgesehen, deren nationale Umsetzung durch eine Novelle des ElWOG 2010 im Zusammenhang mit einem neuen «Erneuerbaren Ausbau Gesetz 2020 (EAG 2020)» geplant war.[13] Durch das vorzeitige Ende der Legislaturperiode in Österreich wurde jedoch das Gesetz nicht mehr in Begutachtung geschickt und es kann daher erwartet werden, dass sich die Novelle verzögern wird. Die im Juli 2019 im Nationalrat unabhängig voneinander eingebrachten Initiativanträge der ÖVP und der SPÖ umfassen nur die als unbedingt notwendig erachtete Novelle des Ökostromgesetzes 2012, nicht jedoch die Einführung der EEG. Zu beachten ist weiters, dass die Elektrizitätsbinnenmarktrichtlinie[14] für ein wohl zumindest sehr ähnliches Konzept den anderen Begriff «Bürgerenergiegemeinschaft» verwendet.[15]

[6] Die EEG ist eine unabhängige Rechtsperson, deren Anteilseigner oder Mitglieder natürliche Personen, lokale Behörden und KMU sein können.[16] Ihr Ziel besteht nicht vorrangig im finanziellen Gewinn, sondern ihren Mitglieder ökologische, wirtschaftliche oder sozialgemeinschaftliche Vorteile zu bringen.[17] Dazu erzeugen sie (beispielsweise durch Photovoltaik-Anlagen) lokal Energie und teilen diese innerhalb der Gemeinschaft, um eine möglichst hohe Eigennutzung zu erzielen.[18] Dies erlaubt bilaterale Lieferverträge, sowie die Erzeugung, Speicherung und Lieferung von erneuerbarer elektrischer Energie auch über Liegenschaftsgrenzen hinweg.[19] Daher kann neu auch ein Energieaustausch über das Verteilnetz in den Netzebenen 6 und 7 (entspricht der Umspannung zwischen Mittel- und Niederspannung, sowie das Niederspannungsnetz) erfolgen. Die Netznutzung sollte dem Netzbetreiber durch ein Netznutzungsentgelt abgegolten werden, welches allerdings im Vergleich zum normalen Netztarif geringer ausfallen könnte, da durch den lokalen Verbrauch der erzeugten Energie höhere Netzebenen nicht genutzt werden und daher das dafür festgelegte Entgelt entfallen kann.

[7] Überschüsse können durch die EEG am elektrischen Energiemarkt verkauft werden; hierzu ist ein diskriminierungsfreier Zugang zu ermöglichen.[20] Zu beachten ist auch, dass derzeit erzeugte erneuerbare Energie jedenfalls abgenommen werden muss und somit auch bei negativen Preisen jederzeit ins Netz eingespeist werden kann.[21] Für «größere erneuerbare Stromerzeugungsanlagen» soll durch das EAG 2020 allerdings ein Eigenvermarktungsgrundsatz eingeführt werden.[22]

---

11 Zu Kleinwasserkraftwerken siehe Gerhard Moser, Möglichkeiten und Grenzen der Eigenverwertung aus rechtlicher Sicht, Präsentation, 2019, https://www.wassertirol.at/fileadmin/user_upload/Akademie/2019/19-06-11_Was_ist_mein_Strom_wert_/19-06-11_3_Eigenverwertung_Moser.pdf (zuletzt abgerufen am 28.08.2019).

12 Richtlinie 2018/2001 zur Förderung der Nutzung von Energie aus erneuerbaren Quellen.

13 BMNT, Vortrag an den Ministerrat, BMNT-555.300/0079-VI/3/2018, 5.12.2018, https://www.bundeskanzleramt.gv.at/dam/jcr:2b9fb6d1-550d-4e0e-a7fa-9d9c77ae32c8/38_17_mrv.pdf (zuletzt abgerufen am 28.08.2019).

14 Richtlinie 2019/944 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt [...].

15 Zu Gemeinsamkeiten und Unterschieden: Stiftung Umweltenergierecht, Die neuen EURegelungen zur Eigenversorgung aus Erneuerbaren Energien, 2019, https://stiftung-umweltenergierecht.de/wp-content/uploads/2019/04/stiftung_umweltenergierecht_vortrag_2019_04_10_lee-lsa_eigenversorgung_nysten.pdf (zuletzt abgerufen am 28.08.2019).

16 Art 2 Z 16 RL 2018/2001.

17 Ebenda.

18 Vgl Art 22 Abs 2 lit a,b RL 2018/2001.

19 BMNT (Fn 13), S. 6.

20 Art 22 Abs 2 lit c RL 2018/2001.

21 BMNT (Fn 13), S. 5.

22 Ebenda.

Eine Zwischenspeicherung von erzeugter Energie durch gemeinsam genutzte zentrale batterieelektrische Speichersysteme (BESS) erscheint daher sinnvoll. Die zwischengespeicherten Überschüsse können zu einem späteren Zeitpunkt der EEG wieder zur Verfügung gestellt werden. Folgende Szenarien sind in Hinblick auf die Speichernutzung möglich:

- Die EEG kann dabei das BESS selbst betreiben.
- Einzelne Teilnehmer der EEG haben Nutzungsrechte am zentralen BESS (z.B. angemietete Speicherkapazität).
- Das BESS ist ein gleichberechtigter Teilnehmer der EEG und nimmt selbständig am gemeinschaftlichen Energiehandel teil.

4. Anforderungen für eine datenschutzfreundliche Umsetzung einer Blockchain-basierten Erneuerbaren-Energie-Gemeinschaft

4.1. Anforderungen aus dem Projektumfeld

[8] Im Projekt «Blockchain Grid» wird konkret eine EEG über einen Blockchain-basierten Ansatz untersucht. Neben dem (Peer-to-Peer-)Energiehandel zwischen den Teilnehmern wird der Einsatz eines BESS, an dem die Teilnehmer der EEG Nutzungsrechte haben, umgesetzt und in einem umfangreichen Feldtest validiert. Zusätzlich wird ein Engpassmanagement der Verteilnetzressourcen implementiert, sodass das zugrunde liegende Verteilnetz der EEG basierend auf den aktuellen Auslastungen sowie Prognosen über zukünftige Zustände und daraus abgeleiteten Kapazitätsfreigaben optimal ausgenutzt werden kann. Im Projekt wird der Ansatz verfolgt, dass der Verteilnetzbetreiber (Distribution System Operator – DSO) Betreiber der Infrastruktur für den Betrieb der EEG ist.

[9] Neben dem Infrastrukturbetreiber (dieser ist verantwortlich für den Betrieb der Blockchain, der notwendigen Messgeräte und letztlich für die Abrechnung) wird im Projekt «Blockchain Grid» eine zweite Rolle mit folgenden Aufgaben als EEG-Repräsentant definiert:

- Festlegung der Rahmenbedingungen für den Energiehandel zwischen den Teilnehmern und Regelung des Ablaufs im Betrieb.
- Ansprechpartner für alle Teilnehmer der EEG in Hinblick auf technische und abrechnungsrelevante Fragen.
- Abrechnung des lokalen Energiehandels.
- Gewinnung neuer Teilnehmer, bzw. Verwaltung von Austritten von Teilnehmern aus der EEG.

[10] Es wäre zwar grundsätzlich denkbar, dass diese Rolle ein Energiehändler als zusätzliche Dienstleistung übernimmt. Hierbei ist aber notwendigerweise zu beachten, dass jeder Teilnehmer der EEG zu jeder Zeit aus der EEG austreten, bzw. seinen Energielieferanten wechseln kann.[23] Auch erfordert die Elektrizitätsbinnenmarktrichtlinie die Entscheidungshoheit jedenfalls innerhalb der Gemeinschaft.[24]

[23] Art 4 RL 2019/944.

[24] ErwG 44 RL 2019/944.

[11] Zur Motivation der Teilnehmer sollte diesen laufend Informationen zu deren Energiedaten, sowie zum getätigten Handel zur Verfügung gestellt werden. Weiters sollte ein gewisser Spielraum im Teilnahmeverhalten eingeräumt werden, beispielsweise durch die – im Projekt «Blockchain Grid» verfolgte – Wahlmöglichkeit bezüglich der Nutzung des eigenen Erzeugungsüberschusses:

1. Unter der Voraussetzung eines Nutzungsrechts am zentralen BESS, kann überschüssige Energie zunächst im Speicher für einen späteren Eigenbedarf vorgehalten werden. Weiterer Überschuss (z.B. aufgrund eines bereits vollständig geladenen Speichers) wird anschließend der EEG zum Kauf angeboten, welche sodann selbst am Energiemarkt aktiv werden könnte.
2. Der Überschuss wird zunächst primär innerhalb der EEG zum Kauf angeboten. Finden sich keine Abnehmer oder kann nicht die gesamte Menge verteilt werden, wird der Speicher für spätere Entnahmen genutzt.

4.2. Datenschutzrechtliche Probleme mit Blockchain-Anwendungen

[12] Seit Mai 2018 ist die Datenschutz-Grundverordnung (DS-GVO) im gesamten Unionsgebiet anwendbar. Diese bezieht sich nicht allgemein auf jede Art von Daten, sondern gilt nur «für die [...] Verarbeitung personenbezogener Daten [...], die in einem Dateisystem gespeichert sind oder gespeichert werden sollen».[25] Dies sind «alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden «betroffene Person») beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt [...] identifiziert werden kann».[26] Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, sofern nicht eine der Bedingungen für die Rechtmäßigkeit erfüllt ist («Verbot mit Erlaubnisvorbehalt»).[27] Dies kann insbesondere die Einwilligung des Betroffenen, die Notwendigkeit der Datenverarbeitung zur Erfüllung eines Vertrags oder eine rechtliche Verpflichtung zur Datenverarbeitung sein. Zu beachten ist allerdings auch, dass eine Einwilligung des Betroffenen jederzeit widerrufen werden kann.

[13] Die Frage nach der Kompatibilität der Blockchain mit dem Datenschutzrecht kann nicht für die Technologie per se beantwortet werden, sondern nur für einen konkreten Anwendungsfall. Abhängig von diesem können beliebige Daten auf der Blockchain gespeichert werden, somit auch datenschutzrechtlich bedenkliche personenbezogene Daten. Hierbei stehen in erster Linie Permissionless Blockchains unter kritischer Beobachtung, da diese eine grundsätzliche Sichtbarkeit der Daten auf der Blockchain erlauben.[28] Permissioned Systeme gewährleisten hingegen ein höheres Maß für den Schutz von Daten, da zentrale, identifizierte Punkte im System als Verant-

25 Art 2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung; DS-GVO).

26 Art 4 DS-GVO.

27 Art 6 DS-GVO.

28 Bitkom (Fn 2), S. 16.

wortliche agieren.[29] Allerdings ist bei diesen in der Regel immer ein Personenbezug feststellbar, ist doch der Zugang auf bestimmte identifizierbare Teilnehmer beschränkt.[30]

4.2.1. Spannungsverhältnisse mit den Grundsätzen der Datenverarbeitung

[14] Nur beispielsweise sollen Spannungsverhältnisse der Blockchain-Technologie mit den Grundsätzen der Datenverarbeitung aufgezählt werden:

- Problematisch sind zunächst die Grundsätze der Datenminimierung[31] und der Speicherbegrenzung[32], da die Datenverarbeitung «für die Zwecke der Verarbeitung notwendige Maß beschränkt» sein muss und die Daten in einer Form gespeichert werden müssen, «die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist». Das Erfordernis nach einer Begrenzung der Speicherfrist auf «das unbedingt erforderliche Mindestmaß»[33] kann in einer Blockchain nicht erfüllt werden, da Daten dauerhaft vorhanden bleiben und im Nachhinein nicht gelöscht werden können. Erlaubt ist jedoch «eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke». In der Tat archiviert die Blockchain mangels möglicher Modifizierbarkeit und Löschbarkeit alter Daten, alle jemals auf diese geschriebenen Informationen. Ein öffentliches Interesse wird aber bei den meisten Anwendungen nicht gegeben sein.
- Ähnlich verhält es sich mit dem Grundsatz der Richtigkeit[34], wonach Daten «sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein» müssen; diese müssen so sie unrichtig sind «unverzüglich gelöscht oder berichtigt werden», was durch die Unmöglichkeit, Daten auf der Blockchain nachträglich zu modifizieren, nicht erfüllbar ist.
- Der Grundsatz der Integrität und Vertraulichkeit[35] erfordert eine Verarbeitung personenbezogener Daten in einer Weise, «die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet». Unbefugte dürfen «keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können».[36] In diesem Zusammenhang zeigen sich auch Probleme mit dem Grundsatz der Zweckbindung[37], da Daten, die einmal auf die Blockchain geschrieben wurden, allgemein für jeden Teilnehmer verfügbar sind und daher von jedem auch für nicht umfasste Zwecke verwendet werden könnten. Die Blockchain-Technologie gewährleistet allerdings hohe Integrität, da eine Manipulation von Blöcken nicht einfach zu bewerkstelligen ist. Zu beachten ist jedoch, dass in Permissioned Blockchains diese Möglichkeit durch Absprache der Teilnehmer größer ist.[38]

29 Ebenda, S. 17.

30 Schock (Fn 1), S. 178.

31 Art 5 Abs 1 lit c DS-GVO.

32 Art 5 Abs 1 lit e DS-GVO.

33 ErwG 39 DS-GVO.

34 Art 5 Abs 1 lit d DS-GVO.

35 Art 5 Abs 1 lit f DS-GVO.

36 ErwG 39 DS-GVO.

37 Art 5 Abs 1 lit b DS-GVO.

38 Marnau (Fn 2), S. 1032.

4.2.2. Der datenschutzrechtlich Verantwortliche in Blockchain-Anwendungen

[15] Eine faire und transparente Verarbeitung ist nur gewährleistet, weil dem Grundsatz der Rechenschaftspflicht[39] entsprechend für jede Datenverarbeitung ein datenschutzrechtlicher Verantwortlicher benannt werden muss, der für die Einhaltung der soeben erwähnten Grundsätze zuständig ist. Die DS-GVO führt diverse Betroffenenrechte ein, durch welche die betroffene Person gegenüber dem Verantwortlichen u.a. Rechte auf Information und Auskunft[40], Berichtigung unrichtiger Daten[41], Löschung[42], bzw. Einschränkung der Verarbeitung[43] erhält. Diese sind großteils sprachlich gleich aufgebaut: «Die betroffene Person hat das Recht, von dem Verantwortlichen [...] zu verlangen». Der Verantwortliche ist eines der zentralen Subjekte des Datenschutzrechts; insbesondere ist er der primäre Adressat der Verpflichtungen der DS-GVO.[44] Als «Person, [...] die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet»[45], hat er die Kontrolle über die Verarbeitung, als auch die Entscheidungshoheit, zu welchem Zweck und mit welchen Mitteln diese erfolgen soll.[46]

[16] Der Grundsatz der Transparenz[47] erfordert zunächst Informationen über die Identität des Verantwortlichen.[48] Je nach Ausprägung der verwendeten Blockchain ist es jedoch fraglich, wer als der datenschutzrechtliche «Verantwortliche» fungiert. Für Permissionless Blockchains ist diese Frage tatsächlich schwer zu beantworten und strittig, kann jedoch bei einem Großteil der beteiligten Akteure mangels Kontrolle über Zwecke und Mittel der Verarbeitung die Verantwortung ausgeschlossen werden.[49] Insbesondere bei weltumspannenden öffentlichen Blockchains mit Knoten in unterschiedlichen Jurisdiktionen wird eine Durchsetzung der Betroffenenrechte nahezu unmöglich sein.[50] Verantwortliche haben außerdem keinerlei Einfluss auf die Datenverarbeitung anderer Blockchain-Knoten.[51] Daher ist der Einfluss einzelner, gegebenenfalls identifizierbarer Akteure so gering, dass ihre datenschutzrechtliche Inanspruchnahme keinen Erfolg verspricht.[52]

---

39 Art 5 Abs 2 DS-GVO.

40 Art 13-15 DS-GVO.

41 Art 16 DS-GVO.

42 Art 17 DS-GVO.

43 Art 18 DS-GVO.

44 Dietmar Jahnel/Angelika Pallwein-Prettner/Christian Marzi, Datenschutzrecht, Facultas, 2018, S. 56.

45 Art 4 Z 7 DS-GVO.

46 Jahnel/Pallwein-Prettner/Marzi (Fn 44), S. 56.

47 Art 5 Abs 1 lit a DS-GVO.

48 ErwG 39 DS-GVO.

49 Mögliche Akteure sind beispielsweise der Programmierer der Blockchainanwendung, der Inititator der Anwendung, jeder Teilnehmer, der eine Transaktion vornimmt, der Miner, jeder Knotenbetreiber; Zusammenfassend: EU Blockchain Observatory and Forum, Blockchain and the GDPR, 2018, https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (zuletzt abgerufen am 28.08.2019), S. 17-18; unterschiedliche Ansichten u.a. Bitkom (Fn 2), S. 28: jeder Knotenbetreiber, jedenfalls nicht der Teilnehmer oder Miner; CNIL (Fn 3), S. 1: jeder Teilnehmer, jedenfalls nicht der Knotenbetreiber oder Miner; NAIH (Fn 3), S. 4: ebenfalls jeder Teilnehmer, aber auch jeder Miner.

50 Vgl die Bitcoin-Blockchain, welche derzeit weltweit etwa 9500 aktive Nodes besitzt, https://bitnodes.earn.com (zuletzt abgerufen am 28.08.2019).

51 Nikolaus Forgó/Žiga Škorjanc, Ausgewählte datenschutzrechtliche Fragen im Zusammenhang mit der Personenzertifizierung in der Blockchain, Gutachten, 2018, https://www.wko.at/service/netzwerke/gutachten-personenzertifizierung-blockchain-forgo.pdf (zuletzt abgerufen am 28.08.2019), S. 41.

52 Böhme/Pesch (Fn 2), S. 479.

[17] Einfacher zu beantworten ist die Frage nach dem datenschutzrechtlich Verantwortlichen jedenfalls für Permissioned Blockchains, da es hier eine organisierende Einheit gibt, die über Zugangsrechte entscheidet. Dieser Verwalter übt die Kontrolle über Zwecke und Mittel der Verarbeitung aus und ist damit Verantwortlicher im datenschutzrechtlichen Sinn.[53] Betroffenenrechte sind somit grundsätzlich in einer Permissioned Blockchain leichter durchzusetzen. Zu beachten ist jedoch, dass eine Blockchain per Design im Nachhinein unveränderbar ist, und damit Rechte auf Berichtigung und Löschung so nicht durchsetzbar sind.

4.2.3. Datenschutzrechtliche Fragestellungen im Zusammenhang mit Smart Contracts

[18] Vergleichsweise wenig untersucht wurden bisher datenschutzrechtliche Fragestellungen im Zusammenhang mit Smart Contracts, welche wohl unter «automatisierte Entscheidungen» im Sinne des Art 22 DS-GVO fallen.[54] Doch hat die betroffene Person «das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung [...] beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet».[55] Diese Regelung gilt dann nicht, wenn die Entscheidung unter anderem «für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist» oder «mit ausdrücklicher Einwilligung der betroffenen Person erfolgt».[56] Zu beachten ist, dass Verträge, die mittels Smart Contracts auf der Blockchain abgeschlossen werden, nach den oben angeführten Punkten nicht notwendigerweise zwischen der betroffenen Person und einem Verantwortlichen abgeschlossen werden. Allerdings gibt es auch im Bezug auf Smart Contracts Stimmen, die einerseits den «Publisher» des Smart Contracts, andererseits jeden, der diesen ausführt (und damit wiederum jeden Knoten) als Verantwortlichen sehen.[57] In jedem Fall muss bei der Verwendung automatisierter Entscheidungen das Eingreifen einer Person möglich sein.[58] Dies erscheint bei Smart Contracts zunächst als unmöglich, doch dürfte auch ein «Review» und eine nachträgliche Änderung der Entscheidung durch den Verantwortlichen umfasst sein.[59]

4.2.4. Verwendung neuer Technologien in der DS-GVO

[19] Im Sinne des Gedankens «Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen» (Privacy by Design and by Default)[60], ist bei jedem Anwendungsfall von Anfang an auf die korrekte Handhabung personenbezogener Daten zu achten. Zu beachten ist insbesondere, dass einmal auf die Blockchain geschriebene Daten nicht mehr modifiziert oder gelöscht werden können. Daher sollte nach Möglichkeit vermieden werden, personenbezogene Daten auf der Blockchain zu speichern. Sollte dies in concreto nicht möglich sein,

53 Schock (Fn 1), S. 179; Bitkom (Fn 2), S. 30.

54 Michèle Finck, Smart Contracts as a form of solely automated processing under the GDPR, International Data Privacy Law, 9, 2, 78-94, 2019.

55 Art 22 Abs 1 DS-GVO.

56 Art 22 Abs 2 lit a,c DS-GVO.

57 EU Blockchain Observatory and Forum (Fn 49), S. 18.

58 Art 22 Abs 3 DS-GVO.

59 CNIL (Fn 3), S. 9; Finck (Fn 2), S. 10.

60 Art 25 DS-GVO.

so müssen weitere technische und organisatorische Maßnahmen, beispielsweise Pseudonymisierung, Anonymisierung, sowie Verschlüsselung personenbezogener Daten, getroffen werden.

[20] Unabhängig von der Verwendung von Blockchain-Technologie ist die Durchführung einer Datenschutzfolgeabschätzung (DSFA) vorgeschrieben, wenn die Verarbeitung «voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge» hat.[61] Exemplarisch wird die «Verwendung neuer Technologien» genannt;[62] diese sollen noch im Entwicklungsstadium an die Anforderungen des Datenschutzrechts angepasst werden und nicht erst wenn sie technisch ausgereift sind.[63] Die Art 29-Gruppe nennt in einem Working Paper unter anderem folgende Kriterien zur Durchführung einer DSFA:[64]

- Datenverarbeitung in großem Umfang (genannt werden: Zahl der Betroffenen, verarbeitete Datenmenge, Dauer oder Dauerhaftigkeit der Datenverarbeitung, geografisches Ausmaß der Datenverarbeitung)
- Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen,
- Fälle, in denen die Verarbeitung an sich «die betroffenen Personen an der Ausübung eines Rechts [...] hindert».

[21] Diese Kriterien dürften in vielen Blockchain-Systemen anwendbar sein.[65] Die DSFA soll unter anderem enthalten:[66]

- eine Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge,
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen, sowie
- Abhilfemaßnahmen, wie Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird.

[22] Diese ist nach dem Wortlaut des Art 35 DS-GVO vom Verantwortlichen durchzuführen. Sinnvollerweise sollte diese Aufgabe jedoch dem Initiator der Blockchain-Anwendung zukommen, da es dem Privacy by Design-Gedanken entspricht, die DSFA bereits vor der Aufnahme der Anwendung durchzuführen. Die Vereinbarkeit der Unveränderlichkeit der Blockchain mit Datenschutzaspekten, wie den Betroffenenrechten, muss dabei im Design des Anwendungsfalls berücksichtigt werden.

61 Art 35 DS-GVO.

62 Ebenda.

63 Gerald Trieb, Datenschutz-Folgeabschätzung und vorherige Konsultation der Aufsichtsbehörde *in* Rainer Knyrim, Datenschutzgrundverordnung, Manz, 2016, S. 220.

64 Datenschutzgruppe nach Artikel 29, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 «wahrscheinlich ein hohes Risiko mit sich bringt» (WP 248), 2017, S. 11-12.

65 Bitkom (Fn 2), S. 36.

66 Art 35 Abs 7 DS-GVO.

4.2.5. Datenschutz in Smart Grids

[23] Berechtigte Parteien erhalten Zugang zu Mess- und Verbrauchsdaten von Endkunden unter den Vorgaben der DS-GVO.[67] Energieverbrauchsdaten können jedoch Einsicht in die persönliche Energie- und Gerätenutzung, deren wirtschaftliche Lage, sowie deren Präferenzen und Lebensstil geben. Somit entstehen insbesondere bei einer hohen Auslesefrequenz daher massig personenbezogene Daten.[68] Zur Datenschutzproblematik in intelligenten Stromnetzen (Smart Grids), insbesondere bei der Verwendung von intelligenten Stromzählern (Smart Metern), existieren eine Menge an Beiträgen; diverse Lösungsansätze wurden von uns in früheren Beiträgen zusammengefasst.[69]

5. Umsetzung

5.1. Technische Umsetzung

[24] Zur Lösung der Datenschutzproblematik wird häufig die Verwendung eines kombinierten Systems mit einer klassischen verteilten Datenbank vorgeschlagen.[70] Personenbezogene Daten werden dann ausschließlich in dieser Datenbank gespeichert, die dort auch nachträglich geändert oder gelöscht werden können. Dadurch werden personenbezogene Daten nicht direkt auf der Blockchain, sondern off-chain gespeichert und in der Blockchain ausschließlich eine Verknüpfung zu dem Datensatz abgelegt.[71] Einen leicht anderen Ansatz verfolgt das Projekt «Blockchain Grid». Die in Abbildung 1 vorgestellte Architektur soll die genannten Anforderungen für den Betrieb einer EEG und des Datenschutzes erfüllen.

67 Art 23 Abs 1,2,3 RL 2019/944.

68 Beispielsweise sieht § 16a Abs 6 ElWOG 2010 für gemeinschaftliche Erzeugungsanlagen eine Auslesung von Energiewerten im Viertelstundenintervall vor.

69 Stephan Cejka, Vorschläge für Datenschutz und Privatsphäre bei Smart Metern und deren Umsetzung im österreichischen Recht, in: Jusletter IT 23. Februar 2017; Stephan Cejka/Felix Knorr/Florian Kintzler, Privacy Issues in Smart Buildings by Examples in Smart Metering, 25th International Conference on Electricity Distribution (CIRED), 2019.

70 Guy Zyskind/Oz Nathan/Alex Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, IEEE Security and Privacy Workshops, 2015; Finck (Fn 2), S. 23.

71 EU Blockchain Observatory and Forum (Fn 49), S. 29-30.

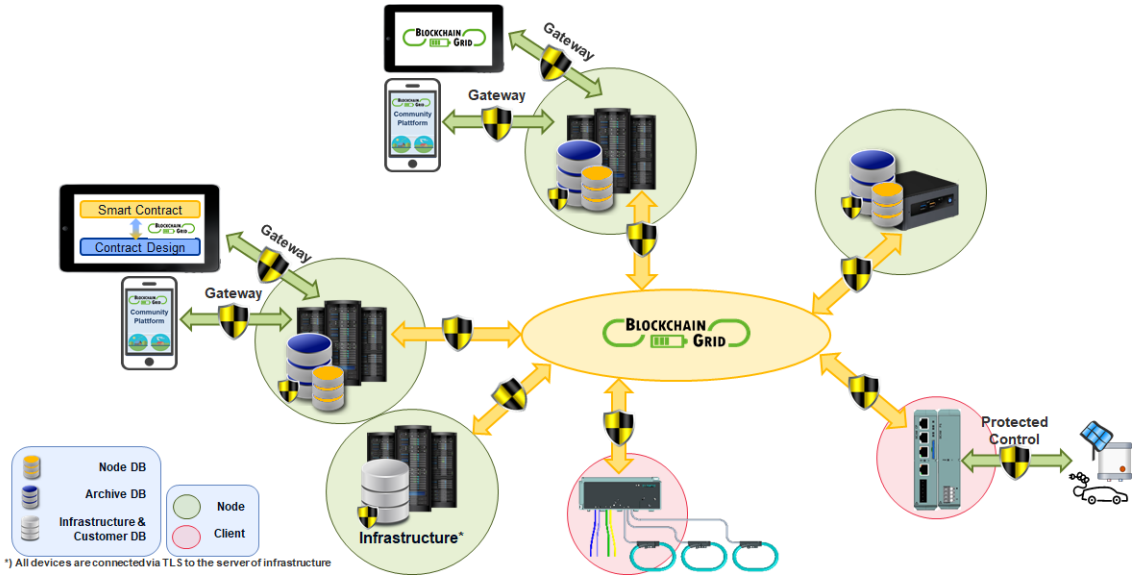

Abbildung 1: Struktur des Lösungsansatzes einer Blockchain-basierten EEG

[25] Das zentrale Element ist eine Permissioned Blockchain, womit der Kreis der Teilnehmer beschränkt ist und diese durch einen zentralen Verwalter hinzugefügt werden müssen. Als Konsensalgorithmus für die Bildung neuer Blöcke wird das «Proof of Authority»-Verfahren genutzt, in dem ausschließlich bestimmte speziell ausgezeichnete Teilnehmer (sogenannte «Sealer») die Transaktionen verschlüsselt in die Blockchain schreiben. Zusätzlich zu diesen Sealern, kann es auch «Full Nodes» geben, die ebenfalls ein Abbild der Blockchain lokal gespeichert haben («Node DB»), aber nicht zwingend auch EEG-Teilnehmer sein müssen.[72]

[26] Die Aufgabe der Nodes besteht darin, den Betrieb und das Fortschreiben der Blockchain für die EEG zu ermöglichen. Es wird davon ausgegangen, dass neben dem eigentlichen Betreiber der EEG (EEG-Repräsentant) auch andere, von den EEG-Teilnehmern akzeptierte Körperschaften ebenfalls einen Node betreiben (z.B. der Regulator oder eine Behörde). Im Ansatz von «Blockchain Grid» betreibt auf jeden Fall auch der Verteilnetzbetreiber (DSO) einen Node um Kapazitätsfreigaben über die Blockchain abwickeln zu können. Daher besteht die Blockchain aus mindestens zwei Nodes, welche die Daten der Blockchain halten und Blöcke hinzufügen. Nodes können auch dynamisch hinzugefügt oder entfernt werden, da im «Proof of Authority»-Verfahren Sealer in einer definierten Reihe die Blöcke generieren und bei Ausfall eines Sealers, der Block erst vom nächsten Sealer gebildet wird.

[27] Der Infrastrukturserver wird vom Infrastrukturbetreiber der EEG (im Falle von «Blockchain Grid» der DSO) betrieben und gewartet. Neben der Verteilung der notwendigen Informationen für den Betrieb der Blockchain, der aktiven Smart Contracts, der Konfiguration der Teilnehmern in der EEG (bzw. deren Messgeräte) sowie der Nodes werden den einzelnen Teilnehmer Rollen zugewiesen, um Zugriffsrechte auf Daten festzulegen. Eine Zuordnung von realen Kundendaten zum Pseudonym in der Blockchain ist nur dem Infrastrukturbetreiber als Verwalter möglich. Diese sind notwendig, um abrechnungsrelevante Informationen an den EEG-Repräsentanten über-

72 Sealer und Full Nodes sind in Abbildung 1 und weiterfolgend als «Nodes» zusammengefasst.

mitteln zu können. So wie die Daten in «Blockchain Grid» ausschließlich verschlüsselt gespeichert werden, um nur von Berechtigten ausgelesen werden zu können, erfolgt auch jeglicher Datenaustausch über verschlüsselte Verbindungen.

[28] Im Kontrast dazu, werden Endkunden nur als sogenannte Clients an die Blockchain angebunden. Die Anbindung erfolgt dabei ausschließlich über Messgeräte und andere Sensoren bzw. Aktoren. Bei diesen handelt es sich um Hardware, die die Energie bzw. Leistungsflüsse der EEG-Teilnehmer ins oder vom elektrischen Verteilnetz ermitteln und via entsprechender Datenaufbereitung und Kommunikationsinfrastruktur als (verschlüsselte) Daten in die Blockchain schreiben. Diese halten selbst kein vollständiges Abbild der Blockchain vor, sondern nur insofern, als sie Daten für das Durchführen von Transaktionen benötigen. Sollten Daten aus der Blockchain an andere Geräte weitergegeben werden müssen (z.B. zur Steuerung einer Ladestation für Elektrofahrzeuge) erfolgt dies ebenfalls über eine gesicherte Verbindung (Protected Control).

[29] Durch den grundsätzlichen Aufbau von Blockchain-Technologien, können den Teilnehmern zu jedem Zeitpunkt die gespeicherten Informationen (z.B. Abrechnungen) nachvollziehbar und transparent zur Verfügung gestellt werden. Somit wird eine hohe Akzeptanz gegenüber der Technologie und Vertrauen unter den Teilnehmern geschaffen. Der Zugriff auf die Daten der EEG-Teilnehmer entsprechend der definierten Zugriffsrechte erfolgt über Webserver oder Gateways, die von einzelnen Nodes betrieben werden. Beispiele für solche Daten sind Messungen, Ver- bzw. Einkäufe in der EEG oder die Speichernutzung des zentralen BESS. Weiters bieten Gateways die Möglichkeit, Einstellungen der Kunden entgegenzunehmen und diese an die Smart Contracts weiterzugeben (z.B. ob der Teilnehmer seine Überschüsse prioritär in das zentrale BESS speichern möchte oder diese zuerst in der EEG verteilt werden sollen).

[30] Der Peer-to-Peer-Handel innerhalb der EEG sowie die Nutzung des BESS wird vollautomatisiert durch das Ausführen von Smart Contracts in der Blockchain realisiert. Unter Berücksichtigung der Zugriffsrechte können über Gateways zusätzliche Tools (z.B. «Smart Contract/Contract Design») angebunden werden. Ebenso können von Berechtigten (z.B. dem EEG-Repräsentanten) sämtliche Energieflüsse in der EEG betrachtet und dadurch Schlüsse für eine Verbesserung des Betriebs in der EEG gewonnen werden.

5.2. Datenschutzrechtliche Umsetzung

[31] Durch die erwähnte technische Umsetzung und der Verwaltung der EEG durch den DSO, wird dieser im vorliegenden Anwendungsfall als datenschutzrechtlich Verantwortlicher identifiziert. Dies ist bei der Anwendung von Smart Contracts zwar fraglich, doch schließt die grundsätzliche Festlegung auf den DSO nicht aus, dass es bei einer konkreten Anwendung neben diesem auch weitere Verantwortliche gibt.

[32] Basierend auf den angeführten Anwendungsfällen, können folgende Daten abgeleitet werden, die von den EEG-Teilnehmern in pseudonymisierter Form in der Blockchain gespeichert werden:

- aktuelle Energiewerte in hoher zeitlicher Auflösung,
- verkaufte Energiemenge an die EEG oder andere EEG-Teilnehmer,
- eingekaufte Energiemenge von der EEG oder von anderen EEG-Teilnehmern,
- gespeicherte Energiemenge im zentralen BESS,
- abgerufene Energiemenge aus dem zentralen BESS.

[33] Zu beachten ist, dass auch pseudonymisierte Daten weiterhin unter den Begriff der personenbezogenen Daten fallen und damit die DS-GVO anwendbar bleibt. Im Zusammenhang mit dem vorliegenden Anwendungsfall ist dabei insbesondere auch zu erwähnen, dass eine EEG möglicherweise keine hohe Anzahl an Teilnehmern haben wird; daher ist die Zuordnung zu einem bestimmten Teilnehmer auch bei Pseudonymen einfach möglich. Auch eine Verschlüsselung von Daten stellt nur eine Form der Pseudonymisierung dar, die nichts an ihrem Personenbezug ändert.[73] Zusätzlich zu den Energiemengen werden Informationen über den Energiepreis abgelegt, um die Abrechnung zu ermöglichen und diese transparent jedem Teilnehmer zur Verfügung zu stellen. Anders als die zuvor erwähnten, dem jeweiligen EEG-Teilnehmer zuordenbaren, Energiedaten, stellen Preisdaten keine personenbezogenen Daten dar und sind daher vom Datenschutzrecht nicht umfasst.

[34] In weiterer Folge ist – dem Grundsatz der Zweckbindung entsprechend – festzustellen, zu welchen Zwecken personenbezogene Daten erhoben, bzw. verarbeitet werden:

- Ausführung der Smart Contracts (z.B. für die Abwicklung von Peer-to-Peer-Energiehandel, für die Vergabe von Netzressourcen oder für die Freigabe von Netzkapazitäten),
- Abrechnung des lokalen Energiehandels innerhalb der EEG,
- Ermöglichung der Nachvollziehbarkeit der Speichernutzung (u.a. als Nachweis für potenzielle Vermieter des zentralen BESS und deren Nutzer),
- Zurverfügungstellung von abrechnungsrelevanten Informationen und der Daten für den Nutzer (Kontrolle des laufenden Systems, Motivation der Teilnehmer, Grundlage für Entscheidungen bezüglich des Teilnehmerverhaltens).

[35] Den Grundsätzen der Datenminimierung und der Speicherbegrenzung folgend, werden Daten auf der Blockchain nur für den Lauf einer Rechnungsperiode gespeichert. Am Ende der Abrechnungsperiode wird somit der Start einer neuen Blockchain durch den Infrastrukturserver («Infrastructure» in Abbildung 1) initiiert. Die alte Blockchain wird sodann in einer Datenbank archiviert («Archive DB») und zur Verknüpfung deren Hashwert als initiale Transaktion in der neuen Blockchain gespeichert. Diese Umsetzung erleichtert die Durchsetzung der Rechte auf Berichtigung und auf Löschung. Da für den Betrieb der EEG eine Auslesung von Energiedaten weitaus öfter erforderlich ist, als gesetzlich vorgesehen, ist jedenfalls eine eindeutige Einwilligung zur Teilnahme erforderlich; diese kann auch jederzeit widerrufen werden.[74] Teilnehmer können über diesen Weg aus der EEG austreten, ihre Daten sind dann in der nächsten Blockchain nicht mehr verfügbar. Zwar sieht die DS-GVO eine unverzügliche Löschung von Daten nach dem Antrag der betroffenen Person vor, doch hat der Verantwortliche diese innerhalb eines Monats durchzuführen. Die nationale Regelung des § 4 Abs 2 DSG,[75] erlaubt eine spätere Löschung insofern «diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen

73 Bitkom (Fn 2), S. 24; Finck (Fn 2), S. 17; *a.A.* Jörn Erbguth, Datenschutz auf öffentlichen Blockchains, in: Jusletter IT 22. Februar 2018, S. 6: «Verschlüsselte personenbezogene Daten gelten nur für diejenigen als personenbezogene Daten [...], die den Schlüssel haben oder mit überschaubarem Aufwand erhalten können».

74 Art 7 Abs 3 DS-GVO.

75 Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) BGBl I 165/1999 idF BGBl I 14/2019.

werden kann».[76] In diesem Fall «ist die Verarbeitung der betreffenden personenbezogenen Daten [...] bis zu diesem Zeitpunkt einzuschränken»:[77]

[36] Archivierte Blockchains werden ausschließlich vom Infrastrukturbetreiber ein Jahr aufbewahrt; Verrechnungsdaten bis zu zehn Jahre. Dies ergibt sich einerseits aus der allgemeinen Verjährungsfrist des § 1486 ABGB[78](drei Jahre), andererseits aus steuerrechtlichen Aufbewahrungsfristen des § 132 BAO[79](sieben Jahren). Würden einzelne Blockchains aus dem Archiv gelöscht werden, kann der Energiehandel nicht mehr vollständig nachvollzogen werden; es stehen nur mehr die Abrechnungsinformationen zur Verfügung, nicht aber wie diese ermittelt wurden.

6. Conclusio

[37] Das von der FFG geförderte Projekt «Blockchain Grid» beschäftigt sich mit einer Blockchain-basierten Umsetzung der, in der RL 2018/2001, eingeführten Erneuerbaren-Energie-Gemeinschaften. Energiedaten von Endkunden stellen personenbezogene Daten dar, daher sind datenschutzrechtliche Vorschriften einzuhalten. Bei einem derartigen Projekt und der Verwendung neuer Technologien, wie Blockchains, sind von Anfang an, entsprechend der Regelungen der DS-GVO, die Grundsätze des «Privacy by Design» einzuhalten, sowie eine Datenschutzfolgeabschätzung durchzuführen. Datenschutzrechtliche Fragestellungen in Bezug auf den Einsatz der Blockchain-Technologie sind stark vom genauen Anwendungsfall abhängig. Daher ist die Frage nach der datenschutzrechtlichen Verantwortung in einer Blockchain-Anwendung bisher strittig, bzw. nicht allgemeingültig zu beantworten. Bei der Verwendung von Blockchain-Technologie können diverse Grundsätze der Datenverarbeitung, aber auch Rechte, der von der Datenverarbeitung Betroffenen, schwer gewährleistet werden. Daher müssen Lösungen in Kombination mit anderen Ansätzen gefunden werden. Da in der Blockchain gespeicherte Daten später nicht mehr modifizierbar oder löschbar sind, sind Zweck und Datenumfang so konkret wie möglich von Anfang an zu definieren.

Mag.iur. Dipl.-Ing. Stephan Cejka BSc, Research Scientist im Bereich Smart Grids & IoT, Siemens AG Österreich.

Dipl.-Ing. Franz Zeilinger BSc, Research Scientist im Bereich Smart Grids & IoT, Siemens AG Österreich.

Peter Stern, Fachsegmentleiter Forschung und Entwicklung im Bereich Energiemanagement, Siemens AG Österreich.

76 Diese Regelung ist laut Philipp Spring, Datenschutzrecht *in* Binder Grösswang, Digital Law – Rechtliche Aspekte der Digitalisierung, LexisNexis, 2018, S. 133 wohl nicht mit der DS-GVO vereinbar.

77 § 4 Abs 2 DSG.

78 Allgemeines bürgerliches Gesetzbuch für die gesammten deutschen Erbländer der Oesterreichischen Monarchie JGS 946/1811 idF BGBl I 74/2019.

79 Bundesgesetz über allgemeine Bestimmungen und das Verfahren für die von den Abgabenbehörden des Bundes, der Länder und Gemeinden verwalteten Abgaben (Bundesabgabenordnung – BAO) BGBl 194/1961 idF BGBl I 62/2019.

Dipl.-Ing. Dr.techn. Mark Stefan, Senior Research Engineer, Thematic Coordinator (Power System Digitalisation), AIT Austrian Institute of Technology GmbH.

Mag. Ksenia Poplavskaya MSc, Research Engineer im Bereich Strommärkte und Regulierung der Energiewirtschaft, AIT Austrian Institute of Technology GmbH, Doktorandin an der Technischen Universität Delft.

Dipl.-Ing. Dr.techn. Gregor Taljan, Asset Manager & Smart Grids Spezialist, Energienetze Steiermark GmbH.

Mag.iur. Julia Petek, Juristin im Netzkundenmanagement, Energienetze Steiermark GmbH.

Das Projekt «Blockchain Grid» (FFG Projektnummer 3089755) wird aus Mitteln des Klima- und Energiefonds gefördert und im Rahmen der FTI-Initiative «Vorzeigeregion Energie» durchgeführt.