Stiftung Umweltenergierecht

Würzburger Studien zum Umweltenergierecht

Asset Logging mittels Blockchain-Technologie aus rechtlicher Sicht

Eine erste Einordnung im Rahmen des Forschungsprojektes „InDEED“

 # 24 | 24.11.2021

erstellt von
Nikolas Klausmann
Anna Papke
Dr. Maximilian Wimmer
Dr. Johannes Hilpert

ISSN 2365-7146

Zitiervorschlag:
Klausmann/Papke/Wimmer/Hilpert, Asset Logging mittels Blockchain-Technologie aus rechtlicher Sicht, Würzburger Studien zum Umweltenergierecht Nr. 24 vom 24.11.2021.

Die Verfasser*innen danken Alexander Bogensperger, Andreas Zeiselmair (beide FfE e.V.), Alexander Djamali, Patrick Dossow, Michael Hinterstocker (alle FfE GmbH) sowie Fabiane Völter, Benjamin Schellinger und Vincent Schlatt (alle Universität Bayreuth) für wertvolle Hinweise und praktische Einblicke.

Entstanden im Rahmen des Vorhabens:
„InDEED – Konzeption, Umsetzung und Evaluation einer auf Blockchain basierenden energiewirtschaftlichen Datenplattform für die Anwendungsfälle ‚Labeling' und ‚Asset Logging'

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

InDEED

Stiftung Umweltenergierecht
Friedrich-Ebert-Ring 9
97072 Würzburg

Telefon
+49 931 794077-0

Telefax
+49 931 7940 77-29

E-Mail
papke@stiftung-umweltenergierecht.de
hilpert@stiftung-umweltenergierecht.de

Internet
www.stiftung-umweltenergierecht.de

Inhaltsverzeichnis

Zusammenfassung 1

A. Einleitung und Grundlagen 2
I. Wesentliche Merkmale des Konzepts Asset Logging 2
1. Erhebung von Anlagen-Daten aus zuverlässigen Datenquellen 2
2. Datenbereitstellung und -verwendung auf Basis einer Internet-Plattform 3
II. Verknüpfung des Asset Logging mit der Blockchain-Technologie 3
1. Relevante Eigenschaften der Blockchain-Technologie für das Asset Logging 4
2. Grundsätzliche Funktionsweise der Blockchain-Technologie 5
a) Schnittstelle 5
b) Validierung 5
c) Konsensmechanismen 6
3. Matrix der Blockchain-Arten anhand der Zugangs- und Validierungsrechte 7
4. Speziell: Hashing und Merkle Trees 8
III. Zwischenergebnis 9

B. Ausgewählte Anwendungsfelder für das Bereitstellen von Anlagen-Daten 10
I. Regulatorisch vorgegebene Rechte und Pflichten im Bereich des Energiewirtschaftsrechts 10
1. Registrierungspflichten im Rahmen des Marktstammdatenregisters 10
a) Worum geht es? 10
b) Welche Daten werden umfasst? 11
c) Wie erfolgt die nähere Ausgestaltung? 11
2. Informationsplattform zu Strommarktdaten 12
a) Worum geht es? 12
b) Welche Daten werden umfasst? 12
c) Wie erfolgt die nähere Ausgestaltung? 13
3. Informationsansprüche und -pflichten der Netzbetreiber 13
a) Worum geht es? 13
b) Welche Daten werden umfasst? 14
c) Wie erfolgt die nähere Ausgestaltung? 15
4. Weitere Anwendungsbereiche für Asset Logging mittels Blockchain-Technologie 16
5. Exkurs: Die Rolle von Self-Sovereign Identities (SSI) für die beschriebenen Anwendungsfelder 16
6. Zwischenfazit 16

II. Zivilrechtliche Vertragsgestaltung 17
1. Anwendungsfelder im Rahmen des Zivilrechts 17
2. Zivilprozessuale Verwertbarkeit von Blockchain-Daten 17
a) Grundsätze der Beweisaufnahme am Zivilgericht 18
b) Die Bedeutung der Blockchain-Datenbank 18
III. Zwischenergebnis 19

C. Vereinbarkeit mit den Vorgaben des Datenschutzrechts 21
I. Verhältnis relevanter Gesetze und Verordnungen zueinander 21
II. Daten vs. personenbezogene Daten 22
1. Kriterien für die Abgrenzung von personenbezogenen und sonstigen Daten 23
2. Qualität der Daten im Kontext des Asset Logging-Konzepts 24
III. Zulässigkeit der Datenverarbeitung 25
1. Zulässigkeit der Datenverarbeitung im Rahmen der DS-GVO 25
2. Zulässigkeit der Datenverarbeitung im Rahmen des MsbG 25
a) Aufbau und Regelungsgehalt der §§ 49, 50 MsbG 25
b) Anwendbarkeit des § 50 MsbG auch auf nicht-personenbezogene Daten? 26
3. Zulässigkeit der Datenverarbeitung im Rahmen des BDSG 27
4. Besonderheiten bei der Einwilligung 27
a) Wirksamkeitsvoraussetzungen 27
b) Das Widerrufsrecht des Betroffenen 28
IV. Rechte und Pflichten bei der Datenverarbeitung 28
1. Zentraler Ansprechpartner beziehungsweise Verantwortlicher nach Art. 4 Nr. 7, Art. 5 Abs. 2 und Art. 24 ff. DS-GVO 28
2. Recht auf Löschung (Recht auf Vergessenwerden), Art. 17 DS-GVO 29
3. Weitere relevante Rechte und Pflichten 31
V. Zwischenergebnis 31

D. Gesamtergebnis 32

Zusammenfassung

Die Blockchain-Technologie, die zunächst durch die digitale Währung Bitcoin einen breiten Bekanntheitsgrad erlangt hat, bietet Anwendungsmöglichkeiten in den verschiedensten Lebensbereichen. In der Energiewirtschaft wird untersucht, inwieweit Blockchain-Lösungen bei der Transformation des Energiesystems hilfreich sein könnten.

Im Vorfeld des Forschungsprojektes „InDEED“ wurde herausgearbeitet, dass die Anwendungsfelder „Labeling von Energieflüssen“ sowie „Asset Logging“ die größten Potenziale aufweisen. Dementsprechend befasst sich das Projekt mit der Frage, welche konkreten Use Cases sich in diesen beiden Bereichen ergeben könnten. Die vorliegende Würzburger Studie bietet eine erste rechtliche Annäherung an das Thema „Asset Logging mittels Blockchain-Technologie“.

Inhaltlich geht es dabei um die technische Möglichkeit, den Austausch von Anlagen-Daten (etwa Betriebs-, Wartungs- und Instandhaltungsdaten) bzw. die darauf basierende Nachweiserbringung manipulationsresistenter zu gestalten. Dies betrifft sowohl den Austausch von Daten zwischen einzelnen Unternehmen – insbesondere Akteuren des Energiesektors – untereinander, als auch deren Übermittlung oder Nachweis an Behörden. Inhaltlich steht einerseits die Abwicklung regulatorischer Pflichten im Mittelpunkt, andererseits bestehen gerade auch umfangreiche Anwendungspotentiale im Bereich der zivilrechtlichen Vertragsgestaltung.

Asset Logging stellt ein technisches Werkzeug zur Bereitstellung und Verwendung von solchen Anlagen-Daten dar. Hierzu werden ausgewählte Anlagen-Daten aus vertrauenswürdigen Quellen erhoben und dann mittels einer Internet-Plattform im Rahmen verschiedener Use Cases verwendet. Die Blockchain-Technologie bietet dabei insbesondere Gewähr für die Integrität der hinterlegten Daten.

Allerdings ist bei der Konzipierung einer Asset Logging-Plattform zu beachten, dass die Vorgaben des Datenschutzrechts (DS-GVO, BDSG) sowie des Messstellenbetriebsgesetzes (MsbG) eingehalten werden. Gerade der Rückgriff auf die Blockchain-Technologie kann potenziell Probleme aufwerfen, soweit personenbezogene Daten verwendet werden. Hier ist insbesondere an das “Recht auf Löschung” zu denken.

Kernergebnisse

- Der Gesetzgeber sieht verschiedene Pflichten für Behörden im Energiesektor vor, Internet-Plattformen und Daten-Register zu betreiben, etwa im Bereich des Marktstammdatenregisters. Zudem bestehen Informationsansprüche Privater untereinander, etwa für Netzbetreiber. Hier bieten sich mögliche Anwendungsfelder für Blockchain-basiertes Asset Logging.
- Weitere Anwendungsfelder bestehen im Rahmen der zivilrechtlichen Vertragsgestaltung, etwa im Bereich Wartungs- oder Garantieverträge. Einen Mehrwert kann dies zumindest potenziell beim Beweis von Anlagen-Daten im Streitfall bieten. Allerdings kann die Blockchain aktuell die Anforderungen an förmliche Beweismittel nicht erfüllen.
- Die verarbeiteten Anlagen-Daten können zumindest im Einzelfall in den Anwendungsbereich von DS-GVO, MsbG und BDSG fallen. Durch eine entsprechende Plattform-Architektur in Verbindung mit geeigneten technischen Hilfsmitteln wie „Hashing“ bzw. „Merkle Trees“ kann ein Konflikt mit den Vorgaben des Datenschutzrechts aber vermieden werden.

A. Einleitung und Grundlagen

Im Januar 2021 veröffentlichte die Bundesregierung ihre Datenstrategie mit dem Ziel, die innovative und verantwortungsvolle Datenbereitstellung und Datennutzung zu erhöhen. Denn Daten, so die Bundesregierung, bilden die Grundlage der digitalen Gesellschaft.[1] Im Rahmen des Forschungsprojektes „InDEED“[2] befasst sich die Stiftung Umweltenergierecht aus rechtlicher Sicht mit dem Konzept „Asset Logging mittels Blockchain-Technologie“. Dabei geht es um die technische Möglichkeit, den Austausch von Anlagen-Daten (etwa Betriebs-, Wartungs- und Instandhaltungsdaten) bzw. die darauf basierende Nachweiserbringung manipulationsresistenter zu gestalten. Dies betrifft sowohl den Austausch von Daten zwischen einzelnen Unternehmen – insbesondere Akteuren des Energiesektors – untereinander, als auch deren Übermittlung oder Nachweis an Behörden.

Das vorliegende Papier nähert sich dem Konzept Asset Logging mittels Blockchain-Technologie zunächst aus technischer und energiewirtschaftlicher Sicht, beschäftigt sich also insbesondere mit den folgenden Fragen: Wie funktioniert das Konzept im Einzelnen? Und was hat es in diesem Zusammenhang mit der Nutzung der Blockchain-Technologie auf sich? Anschließend werden ausgewählte Anwendungsfelder des Konzepts aus Sicht des Energiewirtschaftsrechts sowie des allgemeinen Zivilrechts dargestellt (**Fehler! Verweisquelle konnte nicht gefunden werden.**). Schließlich wird aus datenschutzrechtlicher Sicht geprüft, inwiefern sich hier Hemmnisse ergeben (**Fehler! Verweisquelle konnte nicht gefunden werden.**)

I. Wesentliche Merkmale des Konzepts Asset Logging

Asset Logging stellt ein technisches Werkzeug zur Bereitstellung und Verwendung von Anlagen-Daten dar. Hierzu werden nach dem Konzept im Forschungsprojekt „InDEED“ ausgewählte Anlagen-Daten aus vertrauenswürdigen Quellen erhoben und dann mittels einer Internet-Plattform im Rahmen verschiedener Use Cases verwendet.

1. Erhebung von Anlagen-Daten aus zuverlässigen Datenquellen

Der Begriff der „Anlagen-Daten“, die potenziell im Rahmen des Asset Logging bereitgestellt werden können, umfasst alle anlagenbezogenen Daten. Dies sind Betriebs-, Wartungs- und Instandhaltungsdaten von Energieerzeugungs-, Speicher- und Verbrauchsanlagen, von Netzinfrastruktur-Anlagen sowie vergleichbare Daten von Anlagen außerhalb des Energiesektors.

Im Speziellen kann nochmal zwischen Initialdaten (Anschaffungskosten, technische Kennwerte laut Hersteller), Planungsdaten (zu erwartender Verbrauch, zu erwartende Erzeugung, geplante Wartungsmaßnahmen), Wartungs- und Verfügbarkeitsdaten (Anlagenunfälle, manuelle Eingriffe, Wartungsdaten, Wartungsberichte), Betriebsdaten (tatsächliche Erzeugung, tatsächlicher Verbrauch) und ökonomischen Daten (Anschaffungs-, Wartungs- und Betriebskosten) unterschieden werden. Abzugrenzen sind demgegenüber Daten, die gerade keinen Anlagenbezug haben, sondern sich ausschließlich auf natürliche und/oder

[1] Bundesregierung, Datenstrategie der Bundesregierung, 2021, S. 5, siehe https://www.bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632.

[2] „Verbundvorhaben: InDEED – Konzeption, Umsetzung und Evaluation einer auf Blockchain basierenden energiewirtschaftlichen Datenplattform für die Anwendungsfälle ‚Labeling‘ und ‚Asset Logging‘“, gefördert durch das Bundesministerium für Wirtschaft und Energie. Verbundpartner sind: Forschungsstelle für Energiewirtschaft e.V. (FfE e.V.), Forschungsgesellschaft für Energiewirtschaft mbH (FfE GmbH) und Universität Bayreuth (mit Fraunhofer Blockchain-Labor).

juristische Personen und ihr Handeln beziehen.

Die Erhebung der Daten kann automatisiert oder manuell stattfinden. Abhängig von der jeweils genutzten Technik stehen sie dann digital oder analog zur Verfügung. Analog erhobene Daten müssen allerdings digitalisiert werden, damit sie im Rahmen des Konzepts verarbeitet werden können. Nach Erhebung (und gegebenenfalls Digitalisierung) müssen sie mit einem digitalen Zeitstempel und einer digitalen Signatur oder ID gekennzeichnet werden, um später die Rückverfolgung zur Anlage und zum Erhebungszeitpunkt zu ermöglichen.

2. Datenbereitstellung und -verwendung auf Basis einer Internet-Plattform

Nach ihrer Erhebung werden die Daten im nächsten Schritt über eine Internet-Plattform bereitgestellt. Akteure sollen je nach Bedarf und Berechtigung im Rahmen der einzelnen Use Cases auf die Inhalte zugreifen und hinterlegte Daten einsehen können. Ein Vertragsschluss und eine Vertragsabwicklung auf Basis der bereitgestellten Datengrundlage soll potentiell auch im Rahmen einer solchen Plattform möglich sein, steht aber zunächst nicht im Mittelpunkt des Konzepts[3].

Der Begriff „Plattform“ ist dabei im Rechtskontext vielschichtig[4]: Es wird hier insbesondere zwischen „Aufmerksamkeitsplattformen“ und „Vermittlungsplattformen“ unterschieden. Erstere dienen vor allem dem Zweck, einer Nutzergruppe die Aufmerksamkeit der anderen Nutzergruppe zu ermöglichen (z.B. Werbeplattform), wohingegen Letztere die Vermittlung zwischen den Mitgliedern verschiedener Nutzergruppen ermöglichen[5]. Der Vorgang einer „Vermittlung“ ist dabei weit zu deuten, so dass auch die Möglichkeit des Ablegens von und Zugreifens auf Anlagen-Daten durch verschiedene Akteure – was das Konzept Asset Logging im Kern darstellt – als Vermittlungsleistung im Sinne einer „Nicht-Transaktions-Vermittlungsplattform“ bezeichnet werden kann.

Die Verwendung von Internet-Plattformen liefert verschiedene Vorteile. Diese bestehen vor allem in gesteigerter Standardisierung und der Möglichkeit zur Kollaboration über Organisationsgrenzen hinweg[6]. Die mittels Internet-Plattform bereitgestellten Daten können letztlich in verschiedenen Use Cases verwendet werden. Die adressierten Akteure können beispielsweise im Rahmen von Service- und Wartungsarbeiten, der Abwicklung von Garantie- und Versicherungsansprüchen, dem Verkauf von Anlagen, der Durchführung von Betriebs-Contracting und dem Erbringen von regulatorischen Nachweispflichten auf Plattformen zugreifen[7]. Jeweils vorausgesetzt, dass für den konkreten Use Case auch eine entsprechende Berechtigung des Akteurs vorliegt.

II. Verknüpfung des Asset Logging mit der Blockchain-Technologie

Angesicht aktueller und wiederkehrender Debatten um Datenschutz und Datensicherheit auf Internet-Plattformen[8], erfreut

[3] Als Zukunftsvision beschreibt *Strüker* unter dem Begriff „Asset Management“ wie Energiedienstleistungen für Gebäude und Industrieprozesse, zum Beispiel Wartungen, auf Basis von mittels Blockchain-basierten Plattformen bereitgestellten Daten direkt vertraglich abgewickelt werden könnten; vgl. *Strüker*, in: Strüker/Einhellig, Blockchain in der integrierten Energiewende, 2019, siehe: https://www.dena.de/newsroom/veranstaltungen/2019/blockchain-in-der-integrierten-energiewende/.

[4] *Schallbruch et. al*, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft. Bericht der Kommission Wettbewerbsrecht 4.0, 2019, S. 15 m.w.N., siehe: https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.html.

[5] *Schallbruch et. al*, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft. Bericht der Kommission Wettbewerbsrecht 4.0, 2019, S. 15, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.html.

[6] *Sedlmeir*, Von Bitcoin zu Libra und dem digitalen Euro: Technische Fortschritte von Blockchains und deren Implikationen auf digitale Währungen, RdZ 2020, S. 210; *Schallbruch et. al.*, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft. Bericht der Kommission Wettbewerbsrecht 4.0, 2019, S. 16.

[7] Zu den Use Cases siehe insbesondere: *Zeiselmair et al.*, Poster Abstract: Asset Logging – transparent documentation of asset data using a decentralized platform, S. 1, siehe https://www.ffe.de/attachments/article/970/Paper_Asset_Logging_Energyinformatics_AZeiselmair.pdf.

[8] „Daten im Internet sind nur schwer zu vertrauen“, so: *Socher*, Zeit Online. Alles gesagt, Podcast 2020, abrufbar unter: https://www.zeit.de/digital/2020-11/richard-

sich die mit besonderen Sicherheitseigenschaften ausgestattete Blockchain-Technologie als grundlegende Netzwerk-Technik für Datenspeicherung und Plattformfunktionen zunehmender Aufmerksamkeit[9]. Neben einem hohen Maß an Datenintegrität liefern Blockchain-basierte Plattformen die Vorteile von Standardisierungspotentialen, Kollaborationsmöglichkeiten über Organisationsgrenzen hinweg und Netzwerkeffekten – ohne, dass dabei zwangsläufig eine Aggregation von Marktmacht bei einem Betreiber befürchtet werden muss[10].

Der Begriff „Blockchain-Technologie" steht für ein bestimmtes elektronisches Datenregister, welches durch die Akteure – auch „Nodes" genannt – eines verteilten und verbundenen Computernetzes verwaltet wird. Sie ist eine Unterform sog. „Distributed Ledger Technologies", also solcher Systeme, die eine synchronisierte Verifizierung und Speicherung von Daten in Peer-to-Peer-Netzwerken als Infrastruktur ermöglichen[11]. Distributed-Ledger-Technologies werden ihrer Ursprungsidee nach nicht von einer bestimmten Instanz übergeordnet verwaltet und nutzen keinen zentralen Datenspeicher, wie das bei alternativen Techniken der Fall ist (z.B. Cloud-Lösungen)[12]. Sie weisen zudem keine traditionelle Client-Server-Netzwerkarchitektur auf. Stattdessen kommunizieren die vernetzten und grundsätzlich gleichrangigen Nodes miteinander und betreiben das System basierend auf der redundanten Speicherung der Daten im Kollektiv[13].

1. Relevante Eigenschaften der Blockchain-Technologie für das Asset Logging

Der Begriff „Blockchain" findet seinen Ursprung in der Tatsache, dass die abgebildeten Daten im Rahmen des „distributed ledgers" in Blöcken bei jedem Node lokal gespeichert („block") und kryptographisch verkettet („chain") werden. Aufgrund dieser besonderen Architektur weisen Blockchains[14] bestimmte Eigenschaften auf, welche für das Anwendungsfeld Asset Logging von besonderer Relevanz sind[15]:

Mithilfe entsprechender kryptographischer Verfahren können sie nämlich ein hohes Maß an *Daten-Vertraulichkeit* gewährleisten, weil durch die Anonymisierung von Daten die namentliche Identifizierung von Nutzern und der unbefugte Zugriff auf Daten verhindert werden kann. Durch die Verkettung von Informationen bieten Blockchains eine inhärente Manipulationsresistenz und damit *Daten-Integritätsbeweise*. Die verteilte Validierung der Daten-Zeitstempel kann daneben ein besonders hohes Maß an *Daten-Authentizität* sicherstellen. Besondere *Transparenz* wird durch die Nachvollziehbarkeit von Prozessen hergestellt. Einmal getätigte Dateneinträge können an sich nicht mehr verändert oder gelöscht werden. Eine dauerhafte *Verfügbarkeit* ergibt sich dadurch, dass die Blockchain als dezentrales Netzwerk nicht auf die Verfügbarkeit einzelner Nodes angewiesen ist, sondern auch im Falle des Ausfallens vieler Nodes weiter existiert.

Hinzuweisen ist jedoch darauf, dass es nicht „die eine" Blockchain-Technologie gibt. Vielmehr findet sich die Technik,

socher-kuenstliche-intelligenz-interviewpodcast-alles-gesagt.

[9] So zum Beispiel: *Sedlmeir*, Von Bitcoin zu Libra und dem digitalen Euro: Technische Fortschritte von Blockchains und deren Implikationen auf digitale Währungen, RdZ 2020, S. 210

[10] *Glaser/Hawlitschek/Notheisen*, in: Treiblmaier/Beck, Business Transformation through Blockchain, 2019, S. 121 ff.

[11] Zum Peer-to-Peer-Netzwerk von Computern als Infrastruktur des Programms „Blockchain": *Urbach/Völter*, Grundlagen und Potenziale der Distributed Ledger Technology, LR 2020, S. 119; BNetzA, Die Blockchain-Technologie – Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation, 2019, S. 5; *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 5; Joint Research Centre, Blockchain now and tomorrow, 2019, S. 18.

[12] BNetzA, Die Blockchain-Technologie - Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation, 2019, S. 5.

[13] BNetzA, Die Blockchain-Technologie - Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation, 2019, S. 5, 7, 17.

[14] Der Plural findet hier deshalb Verwendung, weil bei der Verwendung *einer* Blockchain-Datenbank *mehrere* voneinander getrennte Blockchains entstehen.

[15] *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 33; BNetzA, Die Blockchain-Technologie – Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation, 2019, S. 17.

welche 2008 als Grundlage der digitalen Währung Bitcoin Bekanntheit erlangte[16], mittlerweile in unterschiedlichen Ausgestaltungsmöglichkeiten wieder, wobei die soeben dargelegten vorteilhaften Eigenschaften in unterschiedlichem Ausmaß gewährleistet werden. Der Anspruch der folgenden Darstellung ist es demgemäß, die Blockchain-Technologie möglichst allgemein zu beschreiben, um ihre Eigenschaften, unabhängig von der konkreten Ausgestaltung, nachvollziehbar zu machen.

2. Grundsätzliche Funktionsweise der Blockchain-Technologie

Chronologisch betrachtet wird ein Datum beziehungsweise ein Datenpaket über eine Schnittstelle in das System eingebracht, anschließend validiert und daraufhin von den Nodes der Datenblock-Kette – unter Nutzung eines Konsensmechanismus – hinzugefügt.

a) Schnittstelle

Nach Erhebung gelangen die Datenpakete potenziell vollständig automatisiert und in zeitlichen Intervallen „gesammelt“ über eine Schnittstelle („Oracle“) in das Blockchain-System[17]. Auf die Erhebung selbst hat die Blockchain-Technologie als Datenbank keinen Einfluss. Dass Daten schon fehlerhaft und damit nicht authentisch erhoben werden, beispielsweise wegen beschädigter oder manipulierter Messeinrichtungen, kann durch Blockchains nicht verhindert werden[18]. Im Energiesektor stehen aber mit geeichten und zertifizierten Smart-Meter-Gateways vergleichsweise sichere und vertrauenswürdige Instrumente zur authentischen Datenerhebung zur Verfügung[19]. Vor der Speicherung auf der Blockchain werden die Daten durch die Messinfrastruktur mit einer digitalen Signatur versehen, welche eine Zurückverfolgbarkeit zu Anlage und Zeit der Erhebung ermöglicht.

b) Validierung

Anschließend werden die Daten validiert[20], also für authentisch befunden[21]. Dies geschieht typischerweise im Konsens aller Nodes. Handelt es sich bei den Daten um Überweisungswerte, etwa im Fall einer digitalen Währung, lässt sich diese Prüfung anhand der bislang der Blockchain hinzugefügten Daten und „Kontostände“ durchführen. Beispielsweise entspricht im Fall des öffentlichen Bitcoin-Netzwerks[22] die Validierung der Überprüfung, ob der die Überweisung anmeldende Node über ausreichende Mittel verfügt[23]. Die unverschlüsselten Daten und ein öffentlicher Schlüssel des anweisenden Nodes werden hierfür an alle direkt verbundenen Nodes versandt, welche diese dann eigenständig mittels der von ihnen verwalteten Blockchain auf Authentizität prüfen. Kommt ein Node zu einem positiven Ergebnis, wird dieses im Netzwerk weiter propagiert. So erhält das gesamte Netzwerk die Daten und den dazugehörigen öffentlichen Schlüssel.

Im Unterschied zum Blockchain-Anwendungsfall digitaler Währungen, werden beim Asset Logging im Rahmen des Forschungsprojektes „InDEED“ keine Kontostände und Überweisungen, sondern Anlagen-Daten abgebildet. Um diese zu validieren, also auf Authentizität hin zu prüfen, werden die den Daten unmittelbar nach Erhebung angehängten digitalen Signaturen

[16] *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, siehe: https://nakamotoinstitute.org/bitcoin/.

[17] *Urbach/Völter*, Grundlagen und Potenziale der Distributed Ledger Technology, LR 2020, S. 119 (123); BNetzA, Die Blockchain-Technologie - Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation, 2019, S. 16.

[18] Diese Problematik ist als „Oracle- oder Digitalisierungsproblem“ bekannt: *Mühlberger et al.*, Foundational Oracle Patterns: Connecting Blockchain to the Offchain World, 2020; *Urbach/Völter*, Grundlagen und Potenziale der Distributed Ledger Technology, LR 2020, S. 119 (123).

[19] Siehe hierzu: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/SmartMeterGateway/smartmetergateway_node.html. Auf die gerichtlichen und politischen Entwicklungen im Hinblick auf die Markterklärung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) nach § 30 MsbG sei an dieser Stelle hingewiesen.

[20] Es herrscht hier keine begriffliche Einigkeit, so wird in diesem Kontext sowohl von „validieren“ also auch von „verifizieren“ gesprochen. Die Begriffe werden synonym verwendet.

[21] *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 31.

[22] Siehe hierzu: *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, S. 2.

[23] *Urbach/Völter*, Grundlagen und Potenziale der Distributed Ledger Technology, LR 2020, S. 119 (122) m.w.N.

verwendet. Damit ist es für Nodes möglich, zu bestätigen, dass Daten von einer bestimmten Anlage (z.B. einer PV-Anlage) abgesendet und auf dem Übertragungsweg nicht manipuliert worden sind. So kann zwar nicht gänzlich ausgeschlossen werden, dass fehlerhafte Daten in die Blockchain übernommen werden (vgl.o.). Das Risiko dafür kann jedoch deutlich reduziert werden. Blockchains fungieren im Rahmen von Asset Logging demnach nicht als Validator der Überweisung von *Werteinheiten* zwischen Konten, sondern als Validator von *Daten-Authentizität* durch Nachvollziehung digitaler Signaturen.

c) Konsensmechanismen

Ein Node setzt im nächsten Schritt die validierten Daten zu Datenblöcken zusammen und hängt sie der durch ihn gespeicherten Blockchain an. Der neu erstellte Datenblock wird im Netzwerk propagiert, damit ihn die anderen Nodes des Netzwerks ihrer Blockchain anhängen. Dies tun sie, wenn sie von dessen Richtigkeit überzeugt sind, wodurch am Ende dieses Schrittes alle über dieselbe lokale Blockchain verfügen.

Da es sich um ein dezentrales System handelt, muss ein Node die Aufgabe übernehmen, die Daten-Blöcke zu verpacken und anschließend dem Netzwerk zum Anhängen zur Verfügung zu stellen, denn eine zentrale, das System betreibende Instanz existiert dem Grundgedanken nach gerade nicht. Der damit einhergehenden Frage, warum alle Systemnutzer einem anderen Akteur dahingehend vertrauen, dass dieser dem System nur validierte und damit authentische Daten hinzufügt, begegnen Blockchains mittels „Konsensmechanismen“, die unterschiedlich ausgestaltet sein können[24], aber stets dem gleichen Ziel dienen: Einer Konsensfindung innerhalb des Netzwerks über die der Blockchain neu anzuhängenden Datenblöcke[25].

Das Vertrauen der Systemnutzer dahingehend, dass der Blockchain nur validierte und damit authentische Daten hinzufügt werden, folgt (zumindest beim proof of work-Verfahren, dazu sogleich) daraus, dass die aufzubringende Rechenleistung für die Überprüfung eines erstellten Datenblocks durch die restlichen Nodes äußerst gering ist und ein nicht-authentischer Datenblock daher schnell erkannt und nicht weiter verwendet wird[26]. Wenn die Nodes untereinander einen Konsens für die Bildung eines einheitlichen Datenblocks in der Blockchain gefunden haben, wird der neue Block mit den vorherigen Blöcken verkettet. Die Manipulation eines Blocks hätte dann eine Änderung aller nachfolgenden Blöcke zur Folge, wodurch die Blöcke bei einem Node im Netzwerk nicht mehr mit den Blöcken der übrigen Nodes im Netzwerk übereinstimmen würden und dementsprechend als manipuliert erkannt werden könnten[27].

Konsensmechanismen variieren vor allem in Abhängigkeit von der Ausgestaltung des Zugangs zu einem Blockchain-System[28]. Ist beispielsweise eine Blockchain öffentlich zugänglich (public) und derart ausgestaltet, dass jeder Node am Konsensmechanismus teilnehmen kann (permissionless),[29] ist regelmäßig eine Form von digitaler Währung oder anderer Incentivierung erforderlich, um einen Anreiz zur Teilnahme zu bieten[30].

[24] Zu den verschiedenen Verfahren siehe: BNetzA, Die Blockchain-Technologie - Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation, 2019, S. 11 ff.; *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 32 ff.; *Schlatt et al.*, Blockchain: Grundlagen, Anwendungen und Potenziale, 2016, S. 14.

[25] *Schwintowski et al.,* Das Verhältnis von Blockchain-Governance und Gesellschaftsrecht, NJOZ 2018, S. 1401 (1403).

[26] *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 32; nur im Kollektiv, wenn eine Mehrheit unehrlich agieren würde, könnte das System ein invalides Ergebnis hervorbringen (sog. „51 Prozent-Attacke“), *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 97; Joint Research Centre, Blockchain now and tomorrwo, 2019, S. 16.

[27] *FfE*, Die Blockchain-Technologie: Chance zur Transformation der Energieversorgung?, Berichtsteil: Technologiebeschreibung, 2018, S. 32.

[28] Zu den verschiedenen Ausgestaltungsmöglichkeiten des Zugangs siehe: BNetzA, Die Blockchain-Technologie - Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation, 2019, S. 13 f.

[29] *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 34; *Bilski,* Blockchain-Technologie, Smart Contracts und selbstvollziehende Verträge, 2019, S. 4.

[30] Belohnt wird der Aufwand der Blockerstellung beispielsweise mit dem Erhalt digitaler Werteinheiten (Token), *Bilski,* Blockchain-Technologie, Smart Contracts und selbstvollziehende Verträge, 2019, S. 12; der BGH befasste sich bereits im Jahr 2017 mit der Frage, ob die Verwendung fremder Rechenleistung mittels Bots zum Mining von Bitcoins nach dem StGB, gem. §§ 202a, 263a, 269, 303a strafbar sein kann. Siehe hierzu auch

Die public und permissionless konzipierte Bitcoin-Blockchain nutzt dabei das sogenannte proof of work-Verfahren (PoW): Rechenleistung muss erbracht werden, um einen Datenblock erstellen zu dürfen, den die anderen Nodes dann ihrer Blockchain anhängen[31]. Im Gegensatz dazu wird im Rahmen des proof of stake-Verfahrens (PoS) nicht Rechenleistung, sondern die Verteilung der Systemanteile unter den Nodes als Bezugspunkt dafür verwendet, welchem Node das Recht zugesprochen werden soll, einen Datenblock erzeugen zu können[32]. Es handelt sich also um ein Verfahren, das im Gegensatz zum PoW nicht auf dem Verbrauch realer Ressourcen beruht und somit grundsätzlich auch weniger Rechenleistung verbraucht[33].

Neben dem PoW- und dem PoS-Verfahren gibt es noch weitere Konsensmenchanismen, wie das proof of authority-Verfahren, das sich für bestimmte Formen von Blockchain-Systemen anbietet (insbesondere für die private permissioned Blockchain; Erläuterung und Abgrenzung im folgenden Abschnitt)[34]. In dessen Rahmen erhalten diejenigen Nodes das Recht zur Blockerzeugung, die zuvor als Berechtigte festgelegt worden sind, eine unmittelbare Belohnung gibt es nicht. Der Anreiz zur Teilnahme ergibt sich dann beispielsweise schon durch die Vorteile der Anwendungsfälle an sich.

3. Matrix der Blockchain-Arten anhand der Zugangs- und Validierungsrechte

Mit Blick auf den Zugang zu einer Blockchain im Sinne der Teilnahme an sich, existieren zum einen öffentlich (public) organisierte Blockchain-Systeme, zum anderen aber auch solche, deren Zugang beschränkt ist (private). Bezüglich der Genehmigung zur Blockerzeugung besteht die Möglichkeit der unbeschränkten (permissionless) und der beschränkten Genehmigung (permissioned).

Es ergibt sich also Folgendes[35]:

- Public permissionless: Jeder kann das Protokoll herunterladen, am Netzwerk teilnehmen und Transaktionen validieren.
- Public permissioned: Jeder kann das Protokoll herunterladen und am Netzwerk teilnehmen, aber nur unter gewissen Bedingungen Transaktionen validieren.
- Private permissioned: Nur ausgewählte Akteure können am Netzwerk teilnehmen und nur ausgewählte Teilnehmer im Netzwerk dürfen Transaktionen validieren.
- Private permissionless: Nur ausgewählte Akteure können am Netzwerk teilnehmen, aber alle Teilnehmer im Netzwerk dürfen Transaktionen validieren.

Je privater und beschränkter eine Blockchain ausgestaltet ist, desto mehr verliert sie zwar an Dezentralität und Anonymität, eröffnet dafür aber andere Möglichkeiten. So können dann beispielsweise Teilnehmer auch anhand ihrer Vertrauenswürdigkeit ausgewählt[36] und Konsensmechanismen einfacher gestaltet werden.

Im Kontext von Asset Logging mittels Blockchain-Technologie ist zu beachten, dass die Menge an potentiellen Teilnehmern um ein Vielfaches geringer sein wird als beispielsweise im Falle einer weltweit verfügbaren digitalen Währung. Die Plattform hier muss also nicht für das Zusammentreffen einer sehr großen Anzahl an Netzwerkmitgliedern konzipiert werden. Zudem findet Asset Logging mittels

die Anmerkung von *Safferling*, in: NStZ 2018, S. 401 (403).

[31] *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 32.

[32] Beim PoS-Verfahren investieren die Stakeholder Geld statt Hardware und Ressourcen in den Konsensprozess, d.h., es kann Krypto-Währung gekauft werden und als „Stake" (also Einlage) genutzt werden, um dadurch abhängig von der Einlage proportional höhere Chancen zu haben, als Validator für einen Block ausgewählt zu werden, *FfE*, Die Blockchain-Technologie: Chance zur Transformation der Energieversorgung?, Berichtsteil: Technologiebeschreibung, 2018, S. 39.

[33] *Bonneau et al.,* Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, S. 116 f; *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 35.

[34] *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 34; *Schlatt at al.*, Blockchain: Grundlagen, Anwendungen und Potenziale, 2016, S. 14.

[35] *FfE*, Die Blockchain-Technologie – Chance zur Transformation der Energieversorgung? Berichtsteil: Technologiebeschreibung, S. 13.

[36] *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 34.

Blockchain-Technologie in einem grundsätzlich anderen, „vertrauenswürdigeren“ Kontext statt, weshalb ohne weiteres eine private permissioned Blockchain-Technologie zur Anwendung kommen kann, ohne dass damit ein faktischer Verlust an Sicherheitseigenschaften einher ginge.

4. Speziell: Hashing und Merkle Trees

Im Rahmen von Asset Logging mittels Blockchain-Technologie ist sogenanntes „Hashing“ notwendig, wenn es sich bei den verarbeiteten Daten um besonders sensible Daten oder solche mit konkretem Personenbezug handelt. Um lediglich Prüfsummen, nicht aber das vollständige Datum auf einer Blockchain abzulegen, kann mittels Hashing dafür gesorgt werden, dass nur eine Art „digitaler Fingerabdruck“ im Rahmen der Blockchain-Transaktion verwendet wird. Im Ergebnis ist bei der Nutzung von Hashing zur Datenintegration dann nicht das Datum selbst auf der Blockchain öffentlich einsehbar, sondern nur eine Zahlenfolge (sogenannter Hashwert) [37].

Es handelt sich dabei um ein kryptographisches Verfahren, mit dem jedem Datum ein bestimmter Zahlenwert (Hash) zugeteilt wird. Dieser Hash ist so ermittelt, dass er ausschließlich zu diesem einen Datum passt, ohne dass ein Rückschluss auf das Ausgangsdatum möglich ist[38]. Unter Nutzung des Hashes ist das Datum abhängig von der Länge des Werts nahezu unauflösbar, da für eine Entschlüsselung jede einzelne Kombination des Datums aus Buchstaben und Zahlen geprüft werden müsste und eine solche Rechenleistung aktuell nicht darstellbar ist[39].

Sollen größere Datenmengen gehashed werden, kommen sogenannte „Merkle Trees“ zum Einsatz[40]. Ein Merkle Tree ist eine Baumstruktur, die insbesondere dazu verwendet wird, die Integrität von Daten in einem Satz effizient zu überprüfen. Das Kernstück eines Merkle-Tree ist dessen mathematisch strukturierte Verbindung von sämtlichen Hashwerten in den Blättern und der übergeordneten Wurzel, die in einer Hauptwurzel zusammenlaufen. Es können so Hashes einzelner Transaktionen eines Blocks sukzessive zu einem einzigen Hash kombiniert werden, um die zu versendende Datenmenge so gering wie möglich zu halten. So kann eine Blockchain beibehalten werden, obwohl nicht in jedem Knoten alle Daten aller vergangenen Transaktionen vorgehalten werden müssen[41]. Im Ergebnis müssen dann nur die „Archival Nodes“ (große Teilnehmer mit ausreichend Speicherplatz) sämtliche vergangenen Transaktionen der vorherigen Blöcke speichern. Die „Lightweight Nodes“ (kleine Teilnehmer mit wenig Speicherplatz) können dagegen die vergangenen Transaktionen eines jeweiligen vorherigen Blocks mit Hilfe des Merkle Trees in einem einzigen Hashwert zusammenfassen („Block Header“)[42].

Obwohl Daten, die durch Hashing anonymisiert wurden, nicht mit vertretbarem Aufwand wiederherstellt werden können, ist ihre Kontrolle mit Hilfe der in der Blockchain liegenden Hashwerte möglich. Jeder im Netzwerk beteiligte Akteur kann die Validität der Daten z.B. von Archival Nodes bewerten[43]. Jeder Eingabewert führt

[37] Vgl. *Fridgen et al.*, Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 36.

[38] *Fridgen et al.*, Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 36; *Bilski,* Blockchain-Technologie, Smart Contracts und selbstvollziehende Verträge, 2019, S. 8; *Schlatt et al.*, Blockchain: Grundlagen, Anwendungen und Potenziale, 2016, S. 8.

[39] Auch wenn sich das mit der Verwendung sogenannter Quantenrechner entsprechender Größe in der Zukunft ändern könnte, lässt sich dennoch sagen, dass das Verfahren aktuell sehr sicher ist und bestimmten Gefahren wiederum technisch begegnet werden kann, *Erbguth*, Datenschutzkonforme Verwendung von Hashwerten auf Blockchains – Wann sind kryptographische Hashwerte von personenbezogenen Daten selbst wieder personenbezogene Daten?, MMR 2019, S. 654 (655).

[40] *FfE*, Die Blockchain-Technologie – Chance zur Transformation der Energieversorgung? Berichtsteil: Technologiebeschreibung, S. 18; https://academy.binance.com/de/articles/merkle-trees-and-merkle-roots-explained.

[41] *FfE*, Die Blockchain-Technologie – Chance zur Transformation der Energieversorgung? Berichtsteil: Technologiebeschreibung, S. 19.

[42] *FfE*, Die Blockchain-Technologie: Chance zur Transformation der Energieversorgung?, Berichtsteil: Technologiebeschreibung, 2018, S. 19; näher zu den Bestandteilen eines Block Headers *Ertel/Löhmann*, Angewandte Kryptographie, 6. Aufl. 2019, S. 158.

[43] *FfE*, Die Blockchain-Technologie – Chance zur Transformation der Energieversorgung? Berichtsteil: Technologiebeschreibung, S. 19.

deterministisch zu immer dem gleichen Hashwert und jeder Hashwert ist in einen (binären) Merkle Tree eingebunden. Dass das Ursprungsdatum ein Teil der gehashten Datenstruktur ist, kann ohne Kenntnis des Klardatums bewiesen werden. Hierzu muss einerseits der fragliche Hashwert des Merkle Tree dem Hashwert des Eingabewerts entsprechen und andererseits der fragliche Hashwert des Merkle Tree zusammen mit dem benachbarten Hashwert des Merkle Tree den übergeordneten Wurzel-Hash auswerfen[44].

Die Anwendung von Hashing und Merkle-Trees sorgt im Konzept Asset Logging mittels Blockchain-Technologie im Ergebnis also dafür, dass einerseits ursprünglich große Datensätze durch bloße Speicherung der entsprechenden Hashwerte bei Bedarf überprüft werden können. Andererseits sorgt sie dafür, dass auch solche Daten, die ursprünglich Personenbezug aufweisen, beim Speichern auf der Blockchain nicht mehr als personenbezogen anzusehen sind. Im Ergebnis enthält die Blockchain dann nur anonymisierte Daten, was insbesondere mit Blick auf die Vorgaben des Datenschutzrechts vorteilhaft ist (siehe unter **Fehler! Verweisquelle konnte nicht gefunden werden.**).

III. Zwischenergebnis

Beim Konzept des Asset Logging mittels Blockchain-Technologie handelt es sich um ein als Internet-Plattform konzipiertes technisches Konzept, welches Hashes von Anlagen-Daten aus vertrauenswürdigen Quellen nach deren Erhebung mittels Blockchain-Technologie speichert und bereitstellt. Das Plattformmodell bietet einen Mehrwert durch Standardisierung, die Förderung von Kollaboration über Organisationsgrenzen hinweg und durch Skalierbarkeit. Die Nutzung der Blockchain-Technologie gewährleistet besondere Sicherheitseigenschaften, wie etwa Daten-Vertraulichkeit, Daten-Integrität sowie Daten-Authentizität, Transparenz und Verfügbarkeit. Unter Einsatz von Hashing und Merkle Trees können Daten anonymisiert und die auf der Blockchain gespeicherten Datenmengen zugleich gering gehalten werden.

[44] *Fill/Meier*, Blockchain kompakt, S. 11; *Ertel/Löhmann*, Angewandte Kryptographie, 6. Aufl. 2019, S. 102 ff.

B. Ausgewählte Anwendungsfelder für das Bereitstellen von Anlagen-Daten

Nachdem die Grundlagen des Konzepts Asset Logging mittels Blockchain-Technologie dargestellt wurden, sollen im Folgenden ausgewählte Anwendungsfelder für das Bereitstellen von Anlagen-Daten beschrieben werden. Diese betreffen einerseits den Bereich bestimmter, regulatorisch vorgegebener Rechte und Pflichten im Bereich des Energiewirtschaftsrechts (behördliche Registrierungs- und Meldepflichten beziehungsweise Informationsansprüche von Akteuren der Energiewirtschaft untereinander), zum anderen aber auch die freie zivilrechtliche Vertragsgestaltung (etwa Wartungs- oder Garantieverträge).

I. Regulatorisch vorgegebene Rechte und Pflichten im Bereich des Energiewirtschaftsrechts

Im Folgenden wird anhand von drei Beispielen herausgearbeitet, in welchen Zusammenhängen Asset Logging auf Basis der Blockchain-Technologie im Bereich des Energiewirtschaftsrechts eingesetzt werden kann. Dabei werden zuerst zwei Anwendungsfälle dargestellt, die Registrierungs- und Meldepflichten privater Akteure gegenüber Behörden betreffen. Der dritte Anwendungsfall betrifft das Verhältnis privater energiewirtschaftlicher Akteure untereinander, nämlich die gesetzlich vorgesehenen Informationsansprüche zwischen Netzbetreibern. Im Anschluss wird ein kurzer Überblick über weitere mögliche Anwendungsbereiche gegeben.

1. Registrierungspflichten im Rahmen des Marktstammdatenregisters

Gegenüber staatlichen Stellen bestehen für die Akteure des Energiesektors verschiedene Registrierungs- und Meldepflichten. Eine zentrale Registrierungspflicht folgt aus den gesetzlichen Regelungen zum Marktstammdatenregister[45]. Ein Anwendungsfeld für das Asset Logging mittels Blockchain-Technologie könnte darin liegen, dass die Bundesnetzagentur (BNetzA) das Marktstammdatenregister als Internet-Plattform auf Basis der Blockchain-Technologie betreibt[46].

a) Worum geht es?

Der deutsche Gesetzgeber legte im Jahr 2016 fest, dass die BNetzA mit dem Marktstammdatenregister (www.marktstammdatenregister.de) künftig ein elektronisches Verzeichnis mit bestimmten energiewirtschaftlichen Daten errichtet und betreibt (§ 111e EnWG). Das Register übernimmt eine Zentralisierungsfunktion, auch, indem es verschiedene andere schon bestehende Datenbanken, beispielsweise das EEG-Anlagenregister oder das PV-Meldeportal, zusammenführt[47]. Ausdrücklich nennt der Gesetzgeber die Zielsetzung, die Verfügbarkeit und Qualität energiewirtschaftlicher Daten für die im Energieversorgungssystem handelnden Akteure sowie für die zuständigen Behörden zur Wahrnehmung ihrer gesetzlichen Aufgaben zu verbessern, den Aufwand zur Erfüllung energierechtlicher Meldepflichten zu verringern und die Transformation des Energieversorgungssystems gegenüber der Öffentlichkeit transparent darzustellen (§ 111e Abs. 1 S. 2 EnWG).

[45] Ausführlich zum Marktstammdatenregister: *Bartsch/Wagner/Hartmann*, Das Marktstammdatenregister nach §§ 111e/f EnWG – Ziele, Inhalte und betroffene Marktakteure, in: IR 2016, S. 197-201.

[46] An sich wäre zudem denkbar, dass Dritte als Dienstleistung ein konkurrierendes Register auf Basis der Blockchain-Technologie betreiben.

[47] *Winkler*, in: Kment, Energiewirtschaftsgesetz, 2. Aufl. 2019, EnWG § 111e, Rn. 5; *Säcker*, in: Säcker, Berliner Kommentar zum Energierecht. 4. Aufl. 2019, § 111e EnWG Rn. 1.

§ 111e EnWG enthält eine Verordnungsermächtigung, weshalb Einzelheiten materiellrechtlich in der Marktstammdatenregisterverordnung[48] (MaStRV) geregelt sind. Die in dem Register abgelegten Daten sind teilweise für Dritte im Rahmen gesetzlicher Bestimmungen zugänglich, teilweise werden diese auch durch die BNetzA veröffentlicht. Die BNetzA muss anderen Behörden den Zugang zum Marktstammdatenregister eröffnen, soweit diese die darin gespeicherten Daten zur Erfüllung ihrer jeweiligen Aufgaben benötigen (§ 111e Abs. 4 EnWG). Damit sollen redundante Datenmeldungen vermieden und dadurch die meldepflichtigen Akteure entlastet werden. Denn Daten, die bereits im Register erfasst sind, sollen nicht erneut von Behörden, die für die Überwachung und den Vollzug energierechtlicher Bestimmungen zuständig sind, erhoben werden müssen[49].

Es werden nur bestimmte Daten, die nicht als personenbezogene Daten[50] beziehungsweise vertrauliche Daten besonders geschützt sind[51], durch die BNetzA veröffentlicht. Allerdings ist materiellrechtlich geregelt, dass die BNetzA Netzbetreibern in bestimmten Fällen Zugang zu solchen Daten zu gewähren hat, die nicht im Rahmen von § 15 MaStRV veröffentlicht werden. Auch personenbezogene Daten können von dieser Pflicht betroffen sein. Das ist dann der Fall, wenn es sich bei den Daten um für die Erfüllung der gesetzlichen Aufgaben der Netzbetreiber erforderliche Daten handelt (§ 17 Abs. 1 S. 1 Nr. 1 MaStRV). Dabei müssen die Netzbetreiber solche Daten, zu denen ihnen entsprechend Zugang gewährt wurde, unverzüglich löschen, sobald sie die Daten nicht mehr zur Erfüllung benötigen (§ 17 Abs. 3 S. 1 MaStRV)[52].

Der BNetzA stehen Registerberichtigungsmöglichkeiten zu (§ 10 MaStRV). Hierfür kann sie registrierte Marktakteure (§ 10 Abs. 2 MaStRV), insbesondere Netzbetreiber, auffordern, die im Marktstammdatenregister eingetragenen Daten zu prüfen (§ 13 Abs. 1 MaStRV). Im Falle eines Datenfehlers übermittelt ein Netzbetreiber der BNetzA als Prüfergebnis einen Hinweis auf einen möglichen Datenfehler oder von den eingetragenen Daten abweichende Daten. Die erfolgte Überprüfung der Daten durch den Netzbetreiber ist im Marktstammdatenregister zu kennzeichnen.

b) Welche Daten werden umfasst?

Das Marktstammdatenregister ist – schon dem Namen nach – auf die Sammlung von Stammdaten angelegt[53]. Darüber hinausgehende „Bewegungsdaten“, also etwa Produktionsmengen, Lastflussdaten und Speicherfüllstände, werden dementsprechend nicht erfasst. Dabei ist formell-gesetzlich in § 111e Abs. 2 Nr. 1 EnWG bestimmt, dass die als Stammdaten zu erfassenden Daten der Elektrizitätswirtschaft Daten über Anlagen zur Erzeugung und Speicherung von elektrischer Energie sowie deren Betreiber, Betreiber von Elektrizitätsversorgungsnetzen und Bilanzkreisverantwortliche umfassen. Der Verordnungsgeber hat die Regelungen näher ausgestaltet, indem er in § 6 MaStRV bestimmt, dass die in der Anlage 1 der Verordnung genannten konkreten Daten zur Registrierung erforderlich sind[54]. Je nach Ereignis und Art des zu meldenden Akteurs oder Objekts unterscheiden sich diese erforderlichen Angaben.

c) Wie erfolgt die nähere Ausgestaltung?

Das Register ist so organisiert, dass sich die gesetzlich bestimmten Akteure (Marktakteure und Behörden) bei der Vornahme bestimmter Handlungen aktiv zu registrieren haben (vgl. §§ 3 ff. MaStRV). Eine solche Registrierung muss mittels Webportal erfolgen können; in bestimmten Fällen muss aber auch eine schriftliche Registrierung möglich sein (§ 8 Abs. 1 MaStRV).

Wollen andere Behörden auf das Register zugreifen, ist die Grundlage hierfür, dass die organisatorischen und technischen Voraussetzungen für einen solchen Zugriff gewährleistet sind, keine eigenständige Datenerhebung zur Umsetzung europäischen

[48] Vom 10. April 2017 (BGBl. I S. 842), zuletzt durch Artikel 4 des Gesetzes vom 21. Dezember 2020 (BGBl. I S. 3138) geändert.

[49] *Winkler*, in: Kment, Energiewirtschaftsgesetz, 2. Aufl. 2019, EnWG § 111e, Rn. 15.

[50] Zum Personenbezug von Daten siehe später **Fehler! Verweisquelle konnte nicht gefunden werden.**.

[51] *Lietz*, in: Theobald/Kühling, Energierecht, 2020, MaStRV § 15, Rn. 1.

[52] Vgl. zu den sich aus der DS-GVO ergebenden Löschungspflichten C. IV. 2. .

[53] BT-Drs. 18/7317, S. 129; BR-Drs. 542/15, S. 152.

[54] Abrufbar etwa unter https://www.gesetze-im-internet.de/mastrv/anlage.html.

Rechts erforderlich ist und die jeweils benötigten Daten vollständig und richtig übermittelt worden sind (§ 111e Abs. 4 Nr. 1-4 EnWG). Der Gesetzgeber spricht vom Marktstammdatenregister als einem „elektronischen Verzeichnis“ (§ 111e Abs. 1 S. 1 EnWG). Die Daten sollen über das Internet eingegeben, gepflegt und jederzeit verfügbar gemacht werden können[55].

Weiterhin legt der Gesetzgeber fest, dass die Prozesse der Energieversorgung mittels des Verzeichnisses durchgängig digitalisiert und auf eine einheitliche Datenbasis gestellt werden sollen (§ 111e Abs. 1 S. 1 Nr. 2a EnWG). Außerdem hat die BNetzA durch fortlaufende Weiterentwicklung sicherzustellen, dass das Verzeichnis jederzeit dem *Stand der digitalen Technik* und den Nutzungsgewohnheiten in Onlinesystemen entspricht (§ 111e Abs. 1 S. 2 EnWG). Diese Vorgaben richten sich zunächst unmittelbar an das Behördenhandeln.

Vorgaben gegenüber privaten Akteuren hinsichtlich der zu nutzenden Technik werden nicht gemacht. Die Handlungsmöglichkeiten privater Akteure sollen ersichtlich nicht eingeschränkt werden. Der Wortlaut des Rechts[56] lässt aber den Willen erkennen, digitale Innovationen insoweit zu forcieren, als deren Nutzung für Behörden vorausgesetzt wird. Der Gesetzgeber arbeitet hinsichtlich konkreter technischer Anforderungen vermehrt mit unbestimmten Rechtsbegriffen, so dass diesen ein großer Spielraum hinsichtlich der einzusetzenden Technik zukommt.

Würde die BNetzA das Marktstammdatenregister als Internet-Plattform auf Basis der Blockchain-Technologie betreiben, dann könnten den sich registrierenden Akteuren entsprechende Lese- und Schreiberechte eröffnet werden. Faktisch würden dann die Regulierungsbehörde und die privaten Akteure dieselbe Internet-Plattform bespielen. Durch entsprechende Ausgestaltung der Lese- und Schreiberechte könnte ein technisches Äquivalent zu dem schon heute bestehenden Marktstammdatenregister geschaffen werden. Neu wäre dann vor allem, dass das System von den besonderen Sicherheitseigenschaften der Blockchain-Technologie profitiert und damit an realer Wertigkeit und Manipulationsresistenz gewinnt. Die Manipulationsresistenz betrifft allerdings nur die im System abgelegten Daten. Ob die dort abgelegten Daten hingegen inhaltlich richtig sind, kann die Blockchain nicht garantieren. Vor einer konkreten Umsetzung dürfte somit zu klären sein, ob die Vorteile einer Blockchain-Lösung den technischen Mehraufwand rechtfertigen.

2. Informationsplattform zu Strommarktdaten

Zur Steigerung der Transparenz des Strommarktes betreibt die BNetzA neben dem Marktstammdatenregister eine nationale Informationsplattform zu Strommarktdaten. Es erscheint denkbar, auch die hier in Frage stehenden Strommarktdaten mittels einer Asset Logging-Plattform im Wege der Blockchain-Technologie zu verarbeiten.

a) Worum geht es?

§ 111d Abs. 1 S. 1 EnWG verpflichtet die BNetzA zur Errichtung und zum Betrieb einer nationalen Informationsplattform, um der Öffentlichkeit jederzeit die aktuellen Informationen zu den Strommärkten zur Verfügung zu stellen[57]. Das soll der Schaffung von Transparenz und damit Akzeptanz in der Bevölkerung dienen. Eine entsprechende Website ist unter www.smard.de aufrufbar.

b) Welche Daten werden umfasst?

Während das Marktstammdatenregister für die Erfassung von Stammdaten betrieben wird, hat die BNetzA über die Informationsplattform zu den Strommarktdaten die Basis zur Veröffentlichung relevanter Strommarktdaten zu schaffen (§ 111d Abs. 1 S. 1 EnWG). Solche umfassen zunächst Informationen insbesondere zu Stromerzeugung, -last, der Menge, der Ex- und Importe von Elektrizität, der Verfügbarkeit von Netzen und Energieerzeugungsanlagen sowie zu Kapazitäten und der Verfügbarkeit von grenzüberschreitenden

[55] *Lietz*, in: Theobald/Kühling, Energierecht, 107. EL 2020, MaStRV § 1, Rn. 5.

[56] So auch *Lietz*, in: Theobald/Kühling, Energierecht, 107. EL Juli 2020, MaStRV § 1, Rn. 5.

[57] BT-Drs. 18/7317, S. 59; *Winkler*, in: Kment, Energiewirtschaftsgesetz, 2019, EnWG § 111d Rn. 5.

Verbindungsleitungen sowie mittelfristig als auch perspektivisch weitere bei der BNetzA verfügbare Daten (§ 111d Abs. 1 EnWG).

Die BNetzA greift für die Informationsplattform auf Daten der Europäischen Informationsplattform „ENTSO-E Transparency Plattform“ zurück[58]. Die rechtliche Grundlage für die Einrichtung dieser europäischen Plattform bildet Art. 3 Abs. 1 TransparenzVO[59]. Bei den dort verarbeiteten Daten handelt es sich um solche, die von den Primäreigentümern, also den Stellen, die Daten generieren (vgl. Art. 2 Nr. 23 TransparenzVO), an die Betreiber von Übertragungsnetzen (ÜNB) übermittelt werden müssen. Die ÜNB sind dann dazu verpflichtet, diese Daten zu verarbeiten und anschließend an die ENTSO-E zu übermitteln[60]. Die Datenübermittlungspflicht der ÜNB und der Primäreigentümer betrifft vor allem Informationen über Gesamtlast, Übertragungsinfrastruktur sowie tatsächliche Erzeugung.

Die BNetzA soll die erlangten Daten in einer für die Gebotszone der Bundesrepublik Deutschland aggregierten Form veröffentlichen, wobei die Art der Veröffentlichung der Daten „in einer für die Öffentlichkeit verständlichen Darstellung und in leicht zugänglichen Formaten erfolgen [soll], um die Öffentlichkeit besser in die Lage zu versetzen, die Informationen des Strommarktes und die Wirkungszusammenhänge nachvollziehen zu können“ (§ 111d Abs. 3 EnWG).

c) Wie erfolgt die nähere Ausgestaltung?

Die BNetzA hat die Website zu den Strommarktdaten als „elektronische Plattform“ zu betreiben (§ 111d Abs. 1 S. 1 EnWG). Anders als bei einem „elektronischen Verzeichnis“ wie dem Marktstammdatenregister, scheint der Gesetzgeber hier die Plattformkomponente, also die Zugriffsmöglichkeit anderer, mit der Nutzung des Begriffs hervorheben zu wollen. Der BNetzA sind die entsprechenden Daten auf ihr Verlangen auf einer nationalen Internetplattform zur Verfügung zu stellen. Ihr steht also insoweit unmittelbares Datenzugriffsrecht zu[61]. Insbesondere müssen die ÜNB sowie die Primäreigentümer auf Verlangen der BNetzA die Daten über eine zum automatisierten Datenaustausch eingerichtete Schnittstelle zur Verfügung stellen (§ 111d Abs. 2 S. 2 EnWG)[62].

Dieser Vorgabe könnte eine Blockchain-basierte Internet-Plattform aufgrund ihrer technischen Ausgestaltung gerecht werden. Bei der Entscheidung für oder gegen den Einsatz der Blockchain-Technik ist allerdings immer zu bedenken, dass sie lediglich die Manipulationssicherheit der abgelegten Daten sicherstellt, nicht aber die Richtigkeit der Daten selbst. Vor einer konkreten Umsetzung dürfte allerdings abschließend zu klären sein, ob die Vorteile einer Blockchain-Lösung den technischen Mehraufwand rechtfertigen können. Aus rechtlicher Sicht steht es der BNetzA jedenfalls grundsätzlich offen, auf eine Blockchain-Konzeption zurückzugreifen, da der Gesetzgeber hierzu keine konkreten beziehungsweise gegenteiligen Vorgaben macht.

3. Informationsansprüche und -pflichten der Netzbetreiber

Weitere Anwendungsfelder für das Asset Logging auf Blockchain-Basis ergeben sich überdies mit Blick auf regulatorisch bestimmte Informationsansprüche beziehungsweise -pflichten der Akteure des Energiesektors *untereinander*. Die den Netzbetreibern bereitzustellenden Informationen im Rahmen von § 12 EnWG könnten hier ein Anwendungsfeld eröffnen. Betroffen ist das Verhältnis der Netzbetreiber zueinander und zu den sonstigen Akteuren der Energiewirtschaft.

a) Worum geht es?

Der Gesetzgeber sieht verbindliche Verpflichtungen zur wechselseitigen

[58] Vgl. www.transparency.entsoe.eu.

[59] VO (EU) Nr. 543/2013 der Europäischen Kommission über die Übermittlung und die Veröffentlichung von Daten in Strommärkten und zur Änderung des Anhangs I der VO (EG) Nr. 714/2009 des Europäischen Parlaments und des Rates (Transparenzverordnung) v. 14.6.2013 (ABl. L 163 S. 1). Die amtliche Bezeichnung lautet jedoch „EU-Strommärkte-Daten-Übermittlungs-VO“.

[60] *Ahnis*, in: Theobald/Kühling, Energierecht, 2020, EnWG § 111d Rn. 8.

[61] *Winkler*, in: Kment, Energiewirtschaftsgesetz, 2019, EnWG § 111d Rn. 7; BT-Drs. 18/7317, S. 127.

[62] BT-Drs. 18/7317, S. 128.

Informationsbereitstellung zwischen Netzbetreibern vor (§ 12 Abs. 2 EnWG). Für Übertragungs- und Verteilnetzbetreiber bedeutet das, dass diese den Betreibern anderer Netze, die mit dem eigenen Netz technisch verbunden sind, die notwendigen Informationen bereitstellen müssen, um einen sicheren und effizienten Netzbetrieb, den koordinierten Netzausbau und den Netzregelverbund sicherzustellen (§ 12 Abs. 2 EnWG, i.V.m. § 14 Abs. 1 S. 1 EnWG). Nach der Systematik und dem Sinn und Zweck der Norm sind alle Informationen notwendig i.S.v. § 12 Abs. 2 EnWG, die für die Erfüllung der jeweiligen Betreiberpflichten nach § 11 Abs. 1 S. 1, Abs. 1a und Abs. 1 S. 2 EnWG i.V.m. §§ 12 bis 16a EnWG erforderlich sind[63]. Das Informationsrecht kann vor den Zivilgerichten eingeklagt werden[64].

Darüber hinaus folgt aus § 12 Abs. 4 EnWG ein genereller Informationsanspruch der Netzbetreiber auch gegenüber weiteren natürlichen und juristischen Personen: Bestimmte, für ein Funktionieren des Systems maßgebliche Akteure des Sektors müssen diesen auf deren Verlangen hin unverzüglich bestimmte Informationen bereitstellen (§ 12 Abs. 4 und 5 EnWG). Als Adressaten benannt werden Betreiber von Erzeugungsanlagen, Betreiber von Anlagen zur Speicherung von elektrischer Energie, Betreiber von Elektrizitätsverteilernetzen, Betreiber von Gasversorgungsnetzen, industrielle und gewerbliche Letztverbraucher, Anbieter von Lastmanagement und Großhändler oder Lieferanten von Elektrizität (§ 12 Abs. 4 S. 1 Nr. 1-7 EnWG). Die Regelung hat zum Ziel, die zwischen den Netzbetreibern und anderen Marktakteuren oftmals bestehenden Informationsasymmetrien abzubauen[65].

Mit der Inanspruchnahme Ihres Informationsrechts kommen auch Pflichten auf die Netzbetreiber zu. Der Gesetzgeber verpflichtet diese insbesondere dazu, sicherzustellen, dass die Betriebs- und Geschäftsgeheimnisse, die ihnen im Rahmen der Informationsweitergabe zur Kenntnis gelangen, ausschließlich zu den dort genannten Zwecken genutzt werden und dass deren unbefugte Offenbarung ausgeschlossen ist (§ 12 Abs. 5 Nr. 1 EnWG). Auch müssen die erhaltenen Informationen in anonymisierter Form – zusammen mit bestimmten weiteren, auf diesen Informationen basierenden Analysen und Erkenntnissen – auf deren Verlangen hin an die BNetzA übermittelt werden (§ 12 Abs. 5 Nr. 2 bis 5 EnWG).

Aus § 12 Abs. 7 EnWG ergibt sich, dass es sich bei dem in § 12 Abs. 4 EnWG geregelten Informationsrecht für Netzbetreiber und den damit einhergehenden Verpflichtungen gegenüber der Regulierungsbehörde (mittlerweile) um eine Art Auffanganspruch handelt. Denn die BNetzA, das BMWi sowie die Netzbetreiber sollen vorrangig eine Abfrage des Marktstammdatenregisters nutzen (vgl. hierzu bereits 1. a)). Dies deckt freilich nur den Bereich der Stammdaten ab.

b) Welche Daten werden umfasst?

In den Anwendungsbereich der Regelung fallen solche Informationen, die notwendig sind, damit die Elektrizitätsversorgungsnetze sicher betrieben, gewartet und ausgebaut werden können (§ 12 Abs. 4 S. 1 EnWG). Ausdrücklich durch den Gesetzgeber benannt werden dabei Stammdaten (hierzu ist auf das Marktstammdatenregister zu verweisen, vgl.o.), Planungsdaten und Echtzeitdaten (§ 12 Abs. 4 S. 2 EnWG), einschließlich etwaiger Betriebs- und Geschäftsgeheimnisse.

Die Daten, die von dem unbestimmten Rechtsbegriff der „notwenigen Informationen“ umfasst sind, unterscheiden sich aber im Detail und in Abhängigkeit von dem in die Pflicht genommen Akteur. Von Betreibern von Erzeugungsanlagen (§ 12 Abs. 4 S. 1 Nr. 1 EnWG) können die Elektrizitätsversorgungsnetzbetreiber beispielsweise Informationen über Wartungsarbeiten oder die Verfügbarkeit von Erzeugungskapazitäten verlangen[66]. Von den Betreibern von Anlagen zur Speicherung elektrischer Energie (§ 12 Abs. 4 S. 1 Nr. 2 EnWG) können vor allem

[63] *Sötebier*, in: Britz/Hellermann/Hermes, EnWG, 2015, § 12 Rn. 38.

[64] *König*, in: Säcker, Berliner Kommentar zum Energierecht. 2019, § 12 EnWG Rn. 76; *Brucker/Günther*, in: Elpas/Graßmann/Rasbach, Energiewirtschaftsgesetz Kommentar, 2018, § 12 EnWG Rn. 7.

[65] *König*, in: Säcker, Berliner Kommentar zum Energierecht. 2019, § 12 EnWG Rn. 64.

[66] BT-Drs. 15/3917, S. 56.

Informationen über die Ein- und Ausspeisefähigkeit ihrer Anlagen eingeholt werden[67].

Industrielle und gewerbliche Letztverbraucher (§ 12 Abs. 4 S. 1 Nr. 5 EnWG) können verpflichtet werden, über ihr gegenwärtiges und geplantes eigenes Verbrauchsverhalten Auskunft zu geben[68]. Umfasst sind deshalb insbesondere Stillstandzeiten, etwa durch Wartungsarbeiten, und Erweiterungsprojekte, die sich spürbar auf die Stromabnahme durch Letztverbraucher auswirken können. Die Einzelheiten zum Inhalt der Datenaustauschpflicht zwischen den zahlreichen Marktakteuren und den Netzbetreibern werden durch eine Festlegung der BNetzA vom 16. April 2014 konkretisiert[69].

c) Wie erfolgt die nähere Ausgestaltung?

Zwar enthalten § 12 Abs. 2, 4 und 5 EnWG keine expliziten Vorgaben dazu, auf welchem Wege die benannten Informationen bereitzustellen sind,[70] es wird aber unter Verweis auf die Forderungen nach einem diskriminierungsfreien Betrieb (§ 12 Abs. 1 EnWG) argumentiert, dass eine praxisgerechte Umsetzung durch elektronische Übermittlung der Informationen oder durch Bereitstellung in einem geschützten Bereich der Internetseiten der ÜNB erfolgen soll[71].

Die Frage der Informationsübermittlung ist auch im Zusammenhang mit der allgemeinen Pflicht der Netzbetreiber zu sehen, Energieversorgungsnetze sicher, zuverlässig und leistungsfähig zu betreiben (§ 11 Abs. 1 S. 1 EnWG). Denn diese umfasst gem. § 11 Abs. 1a EnWG auch Pflichten für die Art und Weise des Umgangs mit elektronischen Daten. Die Norm versteht hierunter den angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme. Die gesetzliche Formulierung zielt darauf ab, dass die Sicherheit und Zuverlässigkeit des Gesamtsystems gegen IT-Gefahren geschützt werden muss[72]. Auch wenn hieraus nicht folgt, dass jedes einzelne Betriebselement gegen solche Gefahren abzusichern ist, wird angenommen, dass die Vorsorge der Netzbetreiber vor allem sicherzustellen hat, dass die Funktionsfähigkeit der für die Sicherheit und Zuverlässigkeit des Energieversorgungssystems (vgl. § 13 Abs. 4 EnWG) wesentlichen Bestandteile ihrer Netze nicht durch IT-Gefahren unterlaufen wird[73].

Ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes liegt vor, wenn der Katalog[74] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eingehalten wird und dies vom Betreiber dokumentiert worden ist (§ 11 Abs. 1a S. 4 EnWG). Die Einhaltung kann von der Regulierungsbehörde überprüft werden. Daneben ergeben sich auch aus der Einstufung des Netzbetriebs als kritische Infrastruktur im Sinne des § 11 Abs. 1b und 1c EnWG in Verbindung mit dem BSI-G[75] ein umfangreiches Pflichtenprogramm, das die Betreiber einzuhalten haben.[76]

Sollte die wechselseitige Informationsbereitstellung im Rahmen des Netzbetriebs über die Blockchain-Technologie ausgestaltet werden, sind – wie auch bei allen sonstigen Gestaltungsformen – die rechtlichen Vorgaben zum Schutz vor IT-Gefahren bei der technischen Umsetzung vollumfänglich zu beachten. Sofern die Ausgestaltung des Systems zur wechselseitigen Informationsbereitstellung den Anforderungen gerecht werden kann, spricht aber aus rechtlicher Sicht zunächst nichts gegen eine Einbindung der Blockchain-Technologie, da die entsprechenden Vorgaben im EnWG technologieoffen gestaltet sind. Für die

[67] *König*, in: Säcker, Berliner Kommentar zum Energierecht. 4. Aufl. 2019, § 12 EnWG Rn. 69.

[68] *König*, in: Säcker, Berliner Kommentar zum Energierecht, 4. Aufl. 2019, § 12 EnWG Rn. 71.

[69] BNetzA, Beschl. v. 16.4.2014, BK6-13-200 – Festlegung zu Datenaustauschprozessen im Rahmen eines Energieinformationsnetzes (Strom).

[70] Vgl. zum Umfang der Informationspflichten aus § 12 Abs. 4 EnWG auch die BNetzA-Festlegung BK6-13-200.

[71] *Theobald*, in: Theobald/Kühling, Energierecht, 2020, EnWG § 11, Rn. 88.

[72] *König*, in: Säcker, Berliner Kommentar zum Energierecht, 2019, § 12 EnWG Rn. 71.

[73] *König*, in: Säcker, Berliner Kommentar zum Energierecht, 2019, § 12 EnWG Rn. 71.

[74] BNetzA, IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz, 2015, siehe: http://www.bundesnetzagentur.de/DE/Sachgebiete/Elektrizitaetund-Gas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheit.html.

[75] BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist.

[76] Vgl. dazu ausführlicher und m.w.N.: *Guckelberger*, Rechtsfragen kritischer Infrastrukturen, DVBl 2019, S. 525.

Ausgestaltung im Detail müssten allerdings auch die Regularien des Katalogs des BSI im Einzelnen eingehalten werden.

4. Weitere Anwendungsbereiche für Asset Logging mittels Blockchain-Technologie

Das Energierecht sieht noch zahlreiche weitere Konstellationen vor, in denen privaten Akteuren oder öffentlichen Stellen die Pflicht zur Meldung von Daten oder Vorgängen oder die Information über bestimmte Sachverhalte vorgegeben wird. So sieht das EnWG – regelmäßig in Verbindung mit näher ausführenden Rechtsverordnungen beziehungsweise Festlegungen der BNetzA – zum Beispiel umfangreiche Meldepflichten im Rahmen des Redispatch (vgl. § 13a EnWG) oder zur Abwicklung von Regelenergie (vgl. §§ 6 ff. StromNZV) vor. Das EEG enthält für die Durchführung der Erneuerbaren-Förderung zahlreiche Melde- und Nachweispflichten, um den Anspruch beziehungsweise die Höhe der konkret zustehenden Förderung korrekt ermitteln zu können, vgl. § 32 beziehungsweise §§ 70, 74 f. EEG 2021. Die obige Darstellung von drei möglichen Anwendungsfällen des Asset Logging mittels Blockchain-Technologie zur Erfüllung energierechtlicher Pflichten ist daher nur beispielhaft zu verstehen.

5. Exkurs: Die Rolle von Self-Sovereign Identities (SSI) für die beschriebenen Anwendungsfelder

Im Rahmen der Kombination kryptographischer Verfahren und unter Einbezug der Blockchain wurde das Konzept von portablen, selbstsouverän kontrollierten Identitäten (Self-Sovereign Identities; kurz: SSI) entwickelt. Da SSI überprüfbare Nachweise über Eigenschaften und Berechtigungen erhalten und mittels interoperabler Standards domänenübergreifend in unterschiedlichen Interaktionen nutzen können, ist dieses Konzept potentiell auch für die Anwendung am Energiemarkt geeignet[77].

Grundsätzlich beschreibt SSI eine Abwandlung des zentralen, von einem Dienstleistungsanbieter kontrollierten, Identitätsmanagementsystems hin zu einem Nutzerzentrierten System. Im Gegensatz zu anderen Identitätsmanagementsystemen verwaltet hier nicht etwa ein Dienstleister, sondern der Nutzer selbst seine Daten. Er kann dadurch jeweils nur diejenigen Informationen preisgeben, die im entsprechenden Fall erforderlich sind[78]. Eine Blockchain kann im Rahmen der SSI als vertrauenswürdige Datenbank dienen und entsprechende Zertifikate bereithalten und die Echtheit dieser Nachweise überprüfbar machen.

Im Energiesektor steigt das Bedürfnis nach gegenseitigem Austausch von Informationen insbesondere aufgrund der vielen kleinteiligen Akteure und der zunehmenden Vernetzung von Erzeugern, Aggregatoren, Speichern und Verbrauchern. Hier kann SSI eine sinnvolle Grundlage darstellen, um die einzelnen Akteure miteinander zu verbinden und gleichzeitig dafür sorgen, dass nur diejenigen Informationen weitergegeben werden müssen, welche im Einzelfall notwendig sind.

Denkbar ist SSI insbesondere als Alternative zum – zentral organisierten – Marktstammdatenregister (vgl. B. I. 1. , weil sich die Möglichkeit bietet, dezentral und unabhängig vom Anwendungsfall notwendige Stammdaten von einzelnen Instanzen zu zertifizieren und bei Bedarf von berechtigten Anwendern zu verifizieren. Anlagenbetreiber oder auch weitere Marktteilnehmer wären dadurch in der Lage, ihre Daten selbstbestimmt auf einer Blockchain abzulegen und so der BNetzA bzw. weiteren Strommarktakteuren erforderliche Informationen zukommen zu lassen.

6. Zwischenfazit

Der Einsatz von Asset Logging mittels Blockchain-Technologie ist in verschiedenen Konstellationen vorstellbar. Vorliegend wurde ein Einsatz zur Erfüllung der Meldepflichten an das Marktstammdatenregister

[77] Vgl. *Strüker* et al., Self-Sovereign Identity. Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten, S. 3, abrufbar unter: https://www.fim-rc.de/wp-content/uploads/2021/06/Fraunhofer-FIT_SSI_Whitepaper.pdf.

[78] Vgl. *Strüker et al.*, Self-Sovereign Identity. Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten, S. 11 f., abrufbar unter: https://www.fim-rc.de/wp-content/uploads/2021/06/Fraunhofer-FIT_SSI_Whitepaper.pdf.

geprüft, welches von der BNetzA als elektronisches Verzeichnis energiewirtschaftlicher Daten geführt wird. Einen weiteren Anwendungsfall stellt die ebenfalls von der BNetzA betriebene Informationsplattform zu Strommarktdaten dar. Hier handelt es sich jeweils um Meldepflichten Privater gegenüber einer Behörde. Etwas anders gelagert ist der dritte dargestellte Fall, die aus § 12 EnWG herrührenden Informationspflichten der Netzbetreiber untereinander beziehungsweise gegenüber anderen energiewirtschaftlichen Akteuren. Diese betreffen vor allem das Verhältnis Privater zueinander.

In allen drei Fällen deutet sich an, dass die in Frage stehenden Melde- und Informationspflichten aus rein rechtlicher Perspektive mittels Asset Logging unter Einsatz der Blockchain-Technologie erbracht werden könnten, da das Gesetz hier keine bestimmte Form zur Erfüllung der jeweiligen Pflichten vorschreibt. Sollte sich die Blockchain-Technologie also zu einem technischen Standard entwickeln, wäre hier ein Einsatz aus rechtlicher Sicht denkbar.

II. Zivilrechtliche Vertragsgestaltung

Nachdem gezeigt wurde, inwieweit ein Blockchain-basiertes Plattform-Konzept für das Asset Logging im Bereich von energiewirtschaftlichen Rechten und Pflichten Relevanz entfalten könnte, sollen im Folgenden die Anwendungsfelder im Bereich der zivilrechtlichen Vertragsgestaltung näher betrachtet werden.

1. Anwendungsfelder im Rahmen des Zivilrechts

Gemeint sind hier bestimmte anlagenbezogene Verträge zwischen privaten Akteuren, beispielsweise hinsichtlich des Kaufs oder der Miete von Anlagen sowie im Bereich des Contracting. Ebenfalls kommen Werkverträge, etwa hinsichtlich der Anlagenwartung oder solche Verträge, die den Anlagenbetrieb durch ein Dienstleistungsunternehmen für den Eigentümer regeln beziehungsweise Garantien und Versicherungen zum Inhalt haben, als Anwendungsfelder für das Asset Logging mittels Blockchain-Technologie in Betracht.

Teil von solchen vertraglichen Vereinbarungen können nach Einschätzung des Forschungsprojektes „InDEED“ unter anderem auch Anlagen-Daten sein. So können entsprechende Daten im Rahmen eines Anlagen-Kaufs wesentlicher Vertragsbestandteil sein. Genauso könnte ein Werkvertrag bezüglich einer Wartungsleistung ein bestimmtes Ergebnis – ausgedrückt als Anlagen-Datum – zum Inhalt haben. Es geht dabei regelmäßig um das Einhalten von Vertragsbedingungen beziehungsweise das Einhalten oder Auslösen bestimmter sonstiger Bedingungen, Vorgaben oder Sachverhalte, was durch die Nutzung von Asset Logging mittels Blockchain-Technologie transparent oder jedenfalls überprüfbar gemacht werden kann.

Die Nutzung einer Blockchain-basierten Internet-Plattform kann bestimmte Vorteile hinsichtlich der Darstellung solcher Daten bieten, die möglicherweise einen Streitgegenstand zwischen den Parteien darstellen. Das folgt aus den besonderen Sicherheitseigenschaften der Blockchain-Technologie (siehe oben A. II. 1.). Es könnte dann beispielsweise die Integrität von mittels Blockchain-Technologie gespeicherten Anlagen-Daten als Vertragsgegenstand garantiert werden. Dies ist durch die mittels Blockchain-Technologie manipulationsresistent gespeicherten Hashes (vgl. oben A. II. 2.) der Daten möglich. Die Vereinbarung, dass bestimmte Daten im Rahmen der Durchführung eines Vertrags mittels Blockchain-basierter Internet-Plattform abgebildet werden, ist vertragsrechtlich jedenfalls ohne weiteres zulässig (Privatautonomie[79]).

2. Zivilprozessuale Verwertbarkeit von Blockchain-Daten

Fraglich ist allerdings, inwieweit sich ein technischer Mehrwert des Rückgriffs auf die Blockchain-Technologie auch im Prozessrecht perpetuiert. Dies würde jedenfalls das Anwendungspotential des

[79] Hierzu z.B. *di Fabio*, in: Maunz/Dürig, Grundgesetz-Kommentar, 2020, GG Art. 2 Abs. 1.

untersuchten Konzeptes erhöhen und könnte sich im gegenteiligen Fall als Hemmnis darstellen.

a) Grundsätze der Beweisaufnahme am Zivilgericht

Findet sich eine zivilrechtliche Unstimmigkeit zwecks ihrer Klärung vor Gericht wieder, so kommt es bei sich widersprechenden Sachverhaltsinformationen der Prozessparteien insbesondere darauf an, zu klären, welche Darstellung der Wahrheit entspricht. Hierzu dient unter anderem die Beweisaufnahme im Rahmen des Erkenntnisverfahrens[80] (§ 276 Abs. 2 ZPO). Der Gegenstand von dort eingebrachten Beweisen sind Tatsachen[81], die innere und äußere Vorgänge umfassen, die einer sinnlichen Wahrnehmung durch Dritte zugänglich sind[82]. Vor einem Zivilgericht sind nur solche Tatsachen zu beweisen, die umstritten und erheblich sind[83]. Umstritten sind Tatsachen dann nicht, wenn beispielsweise beide Parteien übereinstimmend vortragen, dass Tatsachen nicht ausdrücklich bestritten werden (§ 138 Abs. 3 ZPO), oder wenn es um offenkundige (§ 291 ZPO) und gerichtsbekannte Tatsachen geht.

Es kann zwischen drei Arten des Beweises unterschieden werden: Der Strengbeweis (als Regelfall), die Glaubhaftmachung und der Freibeweis (als Ausnahmen). Sie unterscheiden sich vor allem darin, dass je nach Art ein unterschiedlich weites Spektrum an Beweismitteln möglich ist. Während eine Glaubhaftmachung mittels sämtlicher Beweismittel möglich ist (§ 294 Abs. 1 ZPO), kann ein Strengbeweis nur im Rahmen eines förmlichen Verfahrens und ausschließlich durch fünf Beweismittel erbracht werden (§ 284 S. 1 i.V.m. §§ 355 bis 484 ZPO). Förmliche Beweismittel im Rahmen des Strengbeweises sind Zeugen (§§ 373 bis 401 ZPO), Urkunden (§§ 415 bis 444 ZPO), Sachverständige (§§ 402 bis 414 ZPO), Augenschein (§§ 371 bis 372a ZPO) und die Parteivernehmung (§§ 445 bis 455 ZPO).

b) Die Bedeutung der Blockchain-Datenbank

Es gibt im Rahmen der Beweiserhebung im Zivilprozess zwei denkbare Anknüpfungspunkte für Daten, die mittels Blockchain-Technologie gespeichert sind: Sie könnten offenkundige Tatsachen darstellen oder im Beweisverfahren wie eine Urkunde behandelt werden. Hilfsweise könnte eine Wirkung als Beweismittel auch über die Hinzuziehung eines Sachverständigen konstruiert werden.

Offenkundig sind nach § 291 ZPO solche Tatsachen, die in einem größeren oder kleineren Bezirk einer beliebig großen Menge von Personen bekannt sind oder wahrnehmbar waren und über die man sich aus zuverlässigen Quellen ohne besondere Fachkunde unterrichten kann[84]. Bezogen auf eine Blockchain könnte man daher (unter Bezugnahme auf die eingangs dargestellten Wesensmerkmale und Vorteile) annehmen, die mittels Blockchain-Technologie gespeicherten Daten seien garantiert integer, entstammten daher einer zuverlässigen Quelle und seien deshalb offenkundige Tatsachen.

Doch auch wenn die Blockchain-Technologie es ermöglicht, manipulationsresistente Netzwerke aufzubauen, kann sie ebenso durch schlechte Implementierung zum Aufbau unsicherer Netzwerke führen. Eine Garantiefunktion kann die Blockchain-Technologie also aus technischer Sicht nicht übernehmen. Ginge man hingegen von einer Garantiefunktion aus, so würden die in Frage stehenden Daten allein durch die Nutzung der Blockchain-Speichertechnik bereits aufgrund des Grundsatzes der Offenkundigkeit ohne förmlichen Beweis als erwiesen angesehen werden (bei Nutzung der Blockchain-Technologie könnte dies freilich nur dann zutreffen, wenn man von der Prämisse ausgeht, die in ihr gespeicherten Daten seien garantiert integer, vgl. A. II. 1. .). Folge der Beurteilung von Blockchain-Daten als nicht garantiert integer ist, dass auch für die Einführung von Inhalten in den Zivilprozess, die mittels Blockchain-Technologie gesichert wurden, ein Beweisverfahren durchzuführen ist.

[80] Mit Ausnahme des selbständigen Beweisverfahrens (§ 485 bis 494a ZPO).

[81] *Paulus*, Zivilprozessrecht, 2016, S. 142.

[82] vgl. BGHG NJW-RR 1990, 1276.

[83] *Paulus*, Zivilprozessrecht, 2016, S. 144.

[84] *Huber*, in: Musielak/Voit, ZPO, 2020, § 291 Rn. 1. m.w.N.

Im Rahmen des Beweisverfahrens kommt am ehesten der *Urkundenbeweis* in Betracht: Eine Urkunde (§§ 415 bis 444 ZPO) ist jede verkörperte Gedankenäußerung in Schriftzeichen, die für die Beweiserbringung geeignet ist[85]. Eine echte Urkunde gilt in der Praxis als vergleichsweise zuverlässiges Beweismittel[86]. Allerdings wird die Zuverlässigkeit von Urkunden aufgrund der „Computerisierung" und dem damit einhergehenden Verlust „der Unterscheidbarkeit zwischen Original und Kopie" in gewissem Umfang eingeschränkt[87]. Gerade dieser Schwäche könnte aber mit dem sogenannten „Internet der Werte", basierend auf der Blockchain-Technologie[88], ein Stück weit begegnet werden.

Der Gesetzgeber unterscheidet zwischen öffentlichen und privaten Urkunden (vgl. § 415 Abs. 1 und § 416 ZPO). Erstere beweisen einen vollständigen Vorgang, letztere beschränkten sich nur auf den Beweis der Erklärungsabgabe des Ausstellers. Für die Blockchain kommt im Verhältnis zwischen Privaten – also auch in Bezug auf die zivilrechtliche Vertragsgestaltung im Rahmen des Asset Logging – nur die Einstufung als private Urkunde in Frage, da die öffentliche Urkunde auf behördliche Vorgänge beschränkt ist (§ 415 Abs. 1 ZPO). Eine private Urkunde steht aber schon generell nicht für die Richtigkeit der durch sie transportierten Daten, sondern nur – aber immerhin – für deren korrekte Wiedergabe ein.

In der rechtswissenschaftlichen Literatur wird die Einordnung einer Blockchain als Urkunde (soweit ersichtlich) jedoch überwiegend verneint. *Bilski* schreibt insoweit, ohne genauere Begründung, dass Einträgen in Distributed Ledgers, also auch Blockchains, gegenwärtig nicht die Qualität einer öffentlichen oder privaten Urkunde zugesprochen wird[89]. Die Beweiskraft von solchen Einträgen müsse daher bislang im Verfahren gegebenenfalls kostenintensiv gutachterlich dargelegt werden. Dem ist zuzustimmen, fehlt es Einträgen in Blockchain-Datenbanken wohl schon am Erfordernis der Unterschrift des Ausstellers oder des notariell beglaubigten Handzeichens[90]. *Möllenkamp/Shmatenko* sprechen insoweit richtigerweise von dem Fehlen einer qualifizierten elektronischen Signatur[91].

Trotz der Tatsache, dass mittels Blockchain-Technologie abgelegte Daten derzeit weder als offenkundige Tatsachen noch als Urkunde verwendet werden können, sind diese doch keineswegs wertlos, da sie zumindest *mittelbar* in den Prozess eingeführt werden können. Eine erhöhte Beweiswirkung könnte unter Umständen auf dem Wege erreicht werden, dass von den Parteien ein Sachverständiger aus dem IT-Bereich benannt wird, welcher individuell für den vorliegenden Fall die Beweisqualität der Blockchain-Daten erläutert. Festzuhalten bleibt in jedem Fall, dass die Sicherheitseigenschaften der Blockchain-Technologie im Rahmen des Prozessrechts bislang nicht institutionalisiert wurden, so dass ihre Beweiskraft nur für jeden Fall individuell im Prozess festgestellt werden kann. Angesichts der Unterschiedlichkeit der möglichen Blockchain-Ausgestaltungsformen ist dies aber womöglich ohnehin alternativlos.

III. Zwischenergebnis

Es hat sich nach dem Vorstehenden gezeigt, dass es zum einen im Bereich energiewirtschaftlicher Rechte und Pflichten zu Behörden und bezüglich der Akteure der Energiewirtschaft untereinander, aber auch im Bereich der rein zivilrechtlichen Vertragsgestaltung bereits Anwendungsfelder für das Asset Logging mittels Blockchain-Technologie gibt. Im Falle einer Umsetzung sind die Vorteile der besonderen Vertrauenswürdigkeit und Manipulationsresistenz eines Blockchain-Systems den Nachteilen im Bereich des erhöhten Strombedarfs

[85] *Paulus*, Zivilprozessrecht, 2016, S. 151.

[86] Vgl. *Paulus*, Zivilprozessrecht, 2016, S. 151.

[87] *Paulus*, Zivilprozessrecht, 2016, S. 152.

[88] vgl. *Fridgen et al.,* Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, 2019, S. 70.

[89] *Bilski,* Blockchain-Technologie, Smart Contracts und selbstvollziehende Verträge, 2019, S. 79. Wobei der einfache Ausdruck von auf einem elektronischen Datenträger gespeicherten Dokumenten freilich nicht von vornherein aus dem Kreis der Urkunden ausgenommen ist.

[90] Vgl. *Schreiber*, in: Münchener Kommentar zur ZPO, 2020, ZPO § 41, Rn. 2.

[91] *Möllenkamp/Shmatenko*, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 2020, Teil 13.6 Blockchain und Kryptowährungen, Rn. 87; a.A. scheinbar *Kaulartz/Matzke,* Die Tokenisierung des Rechts, NJW 2018, S. 3278 (3281).

gegenüberzustellen. Grundsätzliche rechtliche Umsetzungshindernisse bestehen zumeist aber nicht – die Vereinbarkeit der Datennutzung mit den Vorgaben des Datenschutzrechts vorausgesetzt (dazu sogleich).

Im Zivilprozess ist die Einführung einer Blockchain-Datenbank wohl nur über die Einbeziehung von Sachverständigen möglich, da sie nicht als Urkunde betrachtet werden kann.

C. Vereinbarkeit mit den Vorgaben des Datenschutzrechts

Abschließend ist zu prüfen, ob und inwiefern aus Sicht des Datenschutzes rechtliche Hemmnisse oder Hindernisgründe für den praktischen Einsatz, insbesondere mit Blick auf den Einsatz der Blockchain-Technologie, bestehen[92].

Sowohl auf nationaler als auch auf europäischer Ebene existieren Regelungen, die vorgeben, unter welchen Voraussetzungen und in welcher Art und Weise Daten verarbeitet werden dürfen. Auf nationaler Ebene regelt das Messstellenbetriebsgesetz (MsbG)[93] die Datenverarbeitung vor allem in Zusammenhang mit intelligenten Messsystemen (Smart Meter). Das Bundesdatenschutzgesetz (BDSG)[94] umfasst den Schutz von personenbezogenen Daten insbesondere im Bereich der Datenverarbeitung durch öffentliche Stellen (hier beispielsweise die Speicherung oder die Weitergabe an andere Behörden), sieht aber auch Sonderregelungen für die Verarbeitung durch nicht-öffentliche Stellen vor.

Auf europäischer Ebene dient die Datenschutzgrundverordnung (DS-GVO)[95] dem Datenschutz. Sie ist immer dann zwingend zu berücksichtigen, wenn die Verarbeitung personenbezogener Daten im Raum steht. Neben den Voraussetzungen für die Verarbeitung enthält die DS-GVO auch ein Pflichtenprogramm, dass bei jeder Verarbeitung personenbezogener Daten eingehalten werden muss.

I. Verhältnis relevanter Gesetze und Verordnungen zueinander

Die DS-GVO regelt die Verarbeitung von personenbezogenen Daten durch Einzelpersonen, Unternehmen und Verbände innerhalb der EU. Sie findet nur Anwendung auf Daten von natürlichen Personen (Art. 2 Abs. 1 DS-GVO). Daten juristischer Personen sind nicht umfasst[96]. Die Verordnung dient dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere dem Schutz personenbezogener Daten und dem Schutz des freien Datenverkehrs[97]. Aufgrund des Vorrangs des europäischen Unionsrechts gegenüber dem nationalen Recht kommt der DS-GVO als europarechtlicher Verordnung grundsätzlich ein Anwendungsvorrang gegenüber nationalen Gesetzen (in diesem Fall MsbG und BDSG) zu[98].

Dass das MsbG dennoch seinen eigenen Regelungsgehalt behält, folgt aus den in der DS-GVO vorgesehenen Öffnungsklauseln. Nach Art. 6 Abs. 2 DS-GVO können Mitgliedsstaaten im Anwendungsbereich von Art. 6 Abs. 1 lit. c) DS-GVO spezifischere Bestimmungen beibehalten oder einführen. Hierzu müssen sie spezifische

[92] Siehe für eine ausführliche Darstellung der Grundlagen von Datenschutz und Datensicherheit im Kontext von Blockhain und insbesondere Energieplattformen: *Fietze/Papke/Wimmer/Antoni/Hilpert*, Der Rechtsrahmen für regionale Peer to Peer-Energieplattformen unter Einbindung von Blockchains, Würzburger Studien zum Umweltenergierecht Nr. 16, September 2020, https://stiftung-umweltenergierecht.de/wp-content/uploads/2020/10/Stiftung_Umweltenergierecht_WueStudien_16_Rechtsrahmen_Energieplattformen_pebbles_2.pdf, S. 71 ff.

[93] Messstellenbetriebsgesetz vom 29. August 2016 (BGBl. I S. 2034), das zuletzt durch Artikel 10 des Gesetzes

vom 16. Juli 2021 (BGBl. I S. 3026) geändert worden ist.

[94] Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das durch Artikel 10 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist.

[95] 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).

[96] *Bretthauer*, Smart Meter im Spannungsfeld zwischen Europäischer Datenschutzgrundverordnung und Messstellenbetriebsgesetz, EnWZ 2017, S. 56 (57).

[97] *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 1 Rn. 1.

[98] *Bretthauer*, Smart Meter im Spannungsfeld zwischen Europäischer Datenschutzgrundverordnung und Messstellenbetriebsgesetz, EnWZ 2017, S. 56 (57); die Verordnung ist unmittelbar anwendbar und bedarf keines Umsetzungsaktes.

Anforderungen für die Verarbeitung „präziser“ bestimmen (Art. 6 Abs. 2 DS-GVO). Dies gilt jedoch nur für solche Bereiche/Materien, die ohnehin bereits regulativ durch die DS-GVO umfasst sind. Das heißt, die Regelungsdichte der nationalen Gesetzgebungsakte richtet sich maßgeblich nach der Regelungsdichte der DS-GVO[99]. Des Weiteren müssen die nationalstaatlichen Regelungen die Anforderungen des Art. 6 Abs. 3 und 4 DS-GVO erfüllen[100]. Das Regelungskonzept der §§ 49 ff. MsbG (auf das noch einzugehen sein wird) erfüllt diese Anforderungen, weshalb die hier relevanten Normen des MsbG als spezifischere Bestimmungen von der DS-GVO unangetastet bleiben und weiterhin ohne Einschränkung gelten[101].

Für das BDSG, welches wie schon die DS-GVO nur bei personenbezogenen Daten Anwendung findet (§ 1 Abs. 1 BDSG), ergibt sich ebenfalls eine Geltung neben der DS-GVO. Während die Regelungen im BDSG für öffentliche Stellen umfassend sind, beinhaltet es nur einzelne spezifische Regelungen, die von privaten Unternehmen zu beachten sind[102]. Durch die Neufassung des BDSG vom 25. Mai 2018 wurde auf das gleichzeitige Inkrafttreten der DS-GVO reagiert, die zwar einige mitgliedstaatliche Gestaltungsspielräume enthält, gegenüber der vergangenen Fassung des BDSG dennoch an etlichen Stellen vorrangig anzuwenden gewesen wäre[103].

Im Bereich des Messstellbetriebes ist das BDSG allerdings nicht anwendbar, da das MsbG insoweit als spezielleres Gesetz vorgeht. Dieser aus dem Grundsatz „lex specialis derogat legi generali“ (das speziellere Gesetz geht dem allgemeineren Gesetz vor) folgende Vorrang ist zudem in § 49 Abs. 1 S. 2 MsbG ausdrücklich normiert[104].

II. Daten vs. personenbezogene Daten

Die Anwendbarkeit datenschutzrechtlicher Regelungen beruht häufig auf dem Vorliegen personenbezogener Daten. Im Folgenden wird daher eine Abgrenzung von Daten und personenbezogenen Daten vorgenommen.

Da das Datenschutzrecht Ausfluss der informationellen Selbstbestimmung des Einzelnen ist, soll es seinem Sinn und Zweck nach gerade solche Daten schützen, die einen gewissen Personenbezug aufweisen[105]. Daher ist der Anwendungsbereich der DS-GVO auf den Bereich der personenbezogenen Daten beschränkt, weshalb das umfassende Pflichtenprogramm der DS-GVO auf nicht-personenbezogene Daten keine Anwendung findet[106]. Auch das BDSG findet nur bei personenbezogenen Daten Anwendung. Das MsbG bezieht sich in vielen Bereichen speziell auf personenbezogene Daten, kennt aber auch Vorschriften, die für andere, nicht-personenbezogene Daten gelten (insbesondere § 50 MsbG). Insgesamt kann konstatiert werden, dass bei der Verarbeitung von personenbezogenen Daten ein höheres Schutzniveau gilt als bei der Verarbeitung von sonstigen Daten.

[99] *Benecke/Wagner*, Öffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG, DVBl. 2016, S. 600 (601).

[100] Demnach muss die jeweilige Norm Bestimmungen beispielsweise darüber enthalten, welche allgemeinen Bedingungen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, usw.

[101] *Bretthauer*, Smart Meter im Spannungsfeld zwischen Europäischer Datenschutzgrundverordnung und Messstellenbetriebsgesetz, EnWZ 2017, S. 56 (60 f.).

[102] https://www2.deloitte.com/dl/de/pages/legal/articles/neues-bundesdatenschutzgesetz.html.

[103] *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Einleitung Rn. 274; *Benecke/Wagner*, Öffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG, DVBl. 2016, S. 600 (608).

[104] Vgl. *Kelly*, Akzeptanzfähigkeit der digitalisierten Energiewende nach dem Messstellenbetriebsgesetz, EurUP 2018, S. 449 (459); *Raabe/Lorenz*, in: Säcker, Berliner Kommentar zum Energierecht, 4. Aufl. 2017, § 49 MsbG Rn. 1.

[105] Es findet keine Unterscheidung danach statt, ob es sich um ein Datum, eine Information oder Wissen handelt, https://www.datenschutzbeauftragter-info.de/definition-und-unterscheidung-der-begriffe-daten-informationen-wissen/.

[106] Vgl. *Metzger*, Digitale Mobilität – Verträge über Nutzerdaten, GRUR 2019, 129 (135).

1. Kriterien für die Abgrenzung von personenbezogenen und sonstigen Daten

Anhand der DS-GVO können einige allgemeine Grundlagen erarbeitet werden, die bei der Einordnung helfen, wann es sich um personenbezogene Daten handelt. Art. 4 Nr. 1 DSG-VO definiert den Begriff der personenbezogenen Daten. Dies sind demnach Angaben jeglicher Art, die sich auf eine unmittelbar identifizierte oder zumindest mittelbar identifizierbare natürliche Person beziehen. Es stellt sich hier zunächst die Frage, wie eng oder weit die Grenzen der unmittelbaren und vor allem der mittelbaren Identifizierung zu ziehen sind.

Jedenfalls unverschlüsselte Profildaten wie Verbrauchs-, Erzeugungsdaten und gewohnheitsbezogene Daten (Komfortanforderungen) oder Informationen zur Zahlungsbereitschaft, sofern sie bestimmten natürlichen Personen zugeordnet sind, können wegen ihrer direkten Identifikation den personenbezogenen Daten zugeordnet werden[107]. Über den Anwendungsbereich der mittelbaren Identifizierbarkeit sind zudem verschlüsselte oder in gewissem Maße entpersonalisierte Daten als personenbezogene Daten im Sinne der DS-GVO anzusehen, wenn durch sie unter Zuhilfenahme sonstiger Informationen beziehungsweise technischer Mittel auf die Identität der Person geschlossen werden kann, sofern der erforderliche Aufwand zur Identifizierung nicht unangemessenen hoch ist[108]. Nicht mehr um personenbezogene Daten handelt es sich erst dann, wenn eine vollständige irreversible Anonymisierung vorgenommen wurde. Irreversible Anonymisierung setzt allerdings voraus, dass die Entschlüsselung entweder tatsächlich (technisch) unmöglich ist, oder der (zeitliche) Aufwand jedenfalls als so hoch anzusehen ist, dass die Identifizierung unwahrscheinlich erscheint. Wann dies der der Fall ist, muss in jedem Einzelfall gesondert geprüft werden[109]. Sollen also oben genannte Daten verarbeitet werden, so handelt es sich nur dann um nicht-personenbezogene Daten, wenn diese derart anonymisiert sind, dass eine rückwirkende Entschlüsselung nicht möglich ist und die hinter den Daten stehende Person auch nicht anderweitig zugeordnet werden kann.

Auch bei Daten, die im Rahmen einer Blockchain gespeichert werden, kann es sich um personenbezogene Daten handeln[110]. Selbst wenn diese nur in pseudonymisierter Form vorliegen[111], wird der Personenbezug nicht ausgeschlossen, wenn es Dritten durch Analysetools theoretisch mit vertretbarem Aufwand möglich ist, die Teilnehmer hinter einer Blockchain-ID zu

[107] *Glattfeld/Keller-Herder*, Die Datenschutz Grundverordnung und ihre Umsetzung durch EVU, ER 2018, S. 135 m.w.N.; hierbei sind alle Mittel zu berücksichtigen, die vernünftigerweise eingesetzt werden könnten, um die betreffende Person zu bestimmen, *Köhler/Müller-Boysen*, Blockchain und smart contracts – Energieversorgung ohne Energieversorger?, ZNER 2018, S. 203 (207).

[108] Erwägungsgrund 26 der DS-GVO weist darauf hin, dass pseudonymisierte personenbezogene Daten, die mithilfe zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, als personenbezogene Daten gelten. Um festzustellen, ob eine natürliche Person identifizierbar ist, sind alle Mittel 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. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden, sollen alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden. Hierbei ist die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklung zu berücksichtigen.

[109] Entschieden ist dies beispielsweise für pseudonymisierte Werbe-Cookies. Diese sind personenbezogen, da der Nutzer anhand der vielen zu ihm gespeicherten Verhaltensmerkmale und spätestens anhand der IP-Adresse unter zumutbarem Aufwand identifizierbar ist, https://t3n.de/news/dsgvo-daten-personenbezogen-841433/.

[110] *Köhler/Müller-Boysen*, Blockchain und smart contracts – Energieversorgung ohne Energieversorger?, ZNER 2108, 203 (207) m.w.N.; *Eperiesi-Beck*, Pseudonymisierung von Daten in der Cloud, ew Spezial 1/2019, 40 (40 f.); siehe auch das Dokument des Bundesverbands IT-Sicherheit (Teletrust) und der Europäischen Agentur für Netz und Informationssicherheit (Enisa), https://www.teletrust.de/uploads/media/PM-190207-ENISA-TeleTrusT-Handreichung_Stand_der_Technik_DEU.pdf.

[111] *Bitkom e.V.*, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Blockchain und Datenschutz, Faktenpapier, 2017, S. 22 m.w.N., https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf; *Schawe*, Blockchain und Smart Contracts in der Kreativwirtschaft, MMR 2019, 218 (221), verweist darauf, dass insbesondere mit Big-Data-Analysen der Personenbezug von pseudonymisierten Daten hergestellt werden kann.

identifizieren[112]. Zwar ist eine dauerhafte Verschlüsselung im Rahmen einer Blockchain grundsätzlich denkbar, muss dann aber konsequent durchgeführt werden und die entsprechenden Hürden nehmen[113]. Dies bestätigt Art. 25 DS-GVO durch den sogenannten Privacy by Design-Grundsatz, der gerade auf den Datenschutz durch entsprechende Technikgestaltung Bezug nimmt[114]. Im Rahmen von Asset Logging mittels Blockchain-Technologie kann diese irreversible Anonymisierung wie bereits dargestellt durch Verwendung von Hashing und Merkle-Trees erfolgen (siehe dazu bereits unter A. II. 4. .).

2. Qualität der Daten im Kontext des Asset Logging-Konzepts

Es kann also festgehalten werden, dass dem Begriff der personenbezogenen Daten ein umfassender Anwendungsbereich zugeschrieben wird und Daten schon immer dann personenbezogen sind, wenn aufgrund einer Kombination an Informationen beziehungsweise mit Hilfe technischer Mittel ein Rückschluss auf die dahinterstehende Person ermöglicht wird[115].

Für den Energiesektor im Allgemeinen gilt, dass jedenfalls Stammdaten bei natürlichen Personen (z.B. Name, Anschrift, Bankverbindung, Kundennummer, Mess- sowie Marktlokation) und damit Informationen über Art und technische Ausstattung, Ort und Spannungsebene sowie Art der kommunikativen Anbindung von an Smart-Meter-Gateways angeschlossenen Anlagen als unmittelbar personenbezogene Daten in den Anwendungsbereich von Art. 6 Abs. 1 DS-GVO und §§ 49, 50 MsbG fallen (vgl. § 2 Nr. 22 MsbG)[116].

Bewegungsdaten (Verbrauchs- und Erzeugungsdaten) und gewohnheitsbezogene Daten wie Komfortanforderungen oder Informationen zur Zahlungsbereitschaft sind mittelbar als personenbezogene Daten anzusehen, wenn sie bestimmten natürlichen Personen wie einem Letztverbraucher beziehungsweise einem Anschlussnutzer zugeordnet werden können[117]. Eine solche Zuordnung der Daten zu natürlichen Personen kann beispielsweise über die Zählpunktbezeichnung auf den Anschlussnutzer erfolgen[118]. Es handelt es sich aber dann nicht um personenbezogene Daten, wenn ohne Möglichkeit der Identifizierbarkeit einer einzelnen Person nur auf eine Personenmehrheit rückgeschlossen werden kann, beispielsweise bei aggregierten Messdaten mehrerer Haushalte[119].

Bei Anlagen-Daten im Kontext von Asset Logging mittels Blockchain-Technologie handelt es sich vorrangig um solche ohne unmittelbaren Personenbezug. Schon die Bezeichnung als „Anlagen-Daten“ macht deutlich, dass in der Regel kein unmittelbarer Bezugspunkt zu natürlichen Personen besteht. Auch eine mittelbare Zuordnung durch die Anlagen-Daten, die im Fokus des Konzepts stehen, ist jedenfalls auszuschließen, soweit es sich bei den im Rahmen des Asset Logging verarbeiteten Daten um Wartungs- und Instandhaltungsdaten oder vergleichbare Daten handelt, die in keinerlei Zusammenhang mit natürlichen Personen stehen.

Trotz dieser übergreifenden Einordnung besteht abhängig von der Ausgestaltung eines Use Cases im Einzelfall doch die Möglichkeit, dass es sich bei Daten, die im Rahmen des Asset Logging verarbeitet werden, um personenbezogene Daten handelt. Dies ist insbesondere bei Daten zu Planung (zu erwartender Verbrauch, zu erwartende Erzeugung, geplante Wartungsmaßnahmen) und Betrieb (tatsächliche Erzeugung, tatsächlicher Verbrauch) denkbar, wenn natürliche Personen dahinter stehen. Es soll daher im Folgenden dargestellt werden,

[112] Es genügt bereits, wenn nur der Organisator in einer zulassungsbeschränkten Blockchain die Schlüssel bestimmten Personen zuordnen kann.

[113] *Gödeke/Jördening*, Blockchain-Lösungen für die Versorgungswirtschaft, VersorgW 2019, 5 (7), die auch die Möglichkeit der vollständigen Anonymisierung im Rahmen einer Blockchain annehmen.

[114] *Schawe*, Blockchain und Smart Contracts in der Kreativwirtschaft, MMR 2019, 218 (221).

[115] https://www.dr-datenschutz.de/personenbezogene-daten-nach-dsgvo-einfach-erklaert/.

[116] *Raabe/Lorenz*, in: Säcker, Berliner Kommentar zum Energierecht, 4. Aufl. 2017, § 50 MsbG Rn. 6.

[117] *Wimmer*, Smart Meter, Plattform und Blockchain, EnWZ 2020, S. 387 (388) m.w.N.; *Bartsch*, in: Theobald/Kühling, Energierecht, 2020, 230, Datenschutz in Energieversorgungsunternehmen, Rn. 8.

[118] *Drozella*, in: Säcker, Berliner Kommentar zum Energierecht, 4. Aufl. 2017 § 5 MsbG Rn. 14.

[119] *Raabe/Lorenz*, in: Säcker, Berliner Kommentar zum Energierecht, 4. Aufl. 2017, § 49 MsbG Rn. 13 m.w.N.

welche grundlegenden Rechte und Pflichten für die Verarbeitung von personenbezogenen Daten gelten.

III. Zulässigkeit der Datenverarbeitung

Mit Blick auf die Datenverarbeitung geht es im Rahmen des Datenschutzes typischerweise um die Frage, unter welchen Voraussetzungen die Verarbeitung erlaubt ist und welche Pflichten hierbei zu beachten sind. Der Definitionsbereich der Verarbeitung ist sehr weit zu verstehen und umfasst nahezu jede Aktivität die mit Daten in Zusammenhang zu bringen ist[120].

Die Zulässigkeit der Datenverarbeitung wird durch ein sogenanntes Verbot mit Erlaubnisvorbehalt geregelt. Das heißt, die Verarbeitung von Daten ist grundsätzlich verboten und nur ausnahmsweise zulässig, wenn ein sogenannter Erlaubnistatbestand vorliegt[121]. Dies kann entweder eine Einwilligung oder ein im Gesetz explizit vorgesehener anderer Grund (Katalogtatbestand) sein. Zwischen DS-GVO und MsbG ergeben sich hier gewisse Unterschiede.

1. Zulässigkeit der Datenverarbeitung im Rahmen der DS-GVO

Die Verarbeitung personenbezogener Daten ist nach der DS-GVO entweder aufgrund einer Einwilligung oder eines der sonstigen Erlaubnistatbestände aus Art. 6 Abs. 1 lit. b) bis f) DS-GVO zulässig. Als Erlaubnistatbestände werden beispielsweise die Erfüllung eines Vertrags, einer rechtlichen Verpflichtung oder aber die Wahrung berechtigter Interessen genannt.

2. Zulässigkeit der Datenverarbeitung im Rahmen des MsbG

Grundnormen für die Datenverarbeitung sind § 49 MsbG, der festlegt, welche Stellen zur Datenverarbeitung berechtigt sind (numerus clausus)[122], und § 50 MsbG, der sich mit zulässigen Zwecken und dem Umfang der Datenverarbeitung befasst[123].

Bezugspunkt der §§ 49, 50 MsbG sind nicht nur intelligente Messsysteme (iMSys), sondern auch Messeinrichtungen, moderne Messeinrichtungen (mME) und sonstige Messsysteme[124]. Ein iMSys besteht aus einer sogenannten modernen Messeinrichtung, also einer Messeinrichtung, die den tatsächlichen Verbrauch und die tatsächliche Nutzungszeit erfassen und darstellen kann (§ 2 Nr. 15 MsbG), und einem Smart Meter Gateway (SMG) als Kommunikationseinheit (§ 2 Nr. 19 MsbG). An das SMG können gemäß der im MsbG vorgenommenen Legaldefinition etwa auch EE- und KWK-Anlagen angeschlossen werden; es muss zudem über die Möglichkeit zur Erfassung, Verarbeitung und Versendung von Daten verfügen. Aus den §§ 19 ff. MsbG ergeben sich technische Vorgaben zur Gewährleistung von Datenschutz und Datensicherheit beim Einsatz von Smart Meter Gateways[125].

a) Aufbau und Regelungsgehalt der §§ 49, 50 MsbG

§ 50 MsbG regelt in Zusammenhang mit § 49 MsbG, wer Daten unter welchen Voraussetzungen verarbeiten darf. § 49 MsbG definiert hierbei zunächst den Kreis der berechtigten Stellen, das heißt, diejenigen,

[120] Siehe hierzu insbesondere auch Art. 4 Nr. 2 DS-GVO, wonach die Datenverarbeitung definiert ist als jeder Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

[121] *Lüdemann/Pokrant/Ortmann*, in: Rohrer/Karsten/Leonhardt, MsbG, 2018, § 50 Rn. 1 f.

[122] Erweiterbar durch Einwilligung des Anschlussnutzers, *Lüdemann/Pokrant/Ortmann*, in: Rohrer/Karsten/Leonhardt, MsbG, 2018, § 50 Rn. 6.

[123] *Lüdemann/Pokrant/Ortmann*, in: Rohrer/Karsten/Leonhardt, MsbG, 2018, § 49 Rn. 1 f., § 50 Rn. 1.

[124] BT-Drs. 18/7555, S. 105; *Lüdemann/Pokrant/Ortmann*, in: Rohrer/Karsten/Leonhardt, MsbG, 2018, § 49 Rn. 2, § 50 Rn. 4.

[125] *Hilpert/Antoni*, Rechtsrahmen für netzdienliche Flexibilitätsplattformen, Würzburger Studien zum Umweltenergierecht Nr. 14, Dezember 2019, https://stiftung-umweltenergierecht.de/wp-content/uploads/2019/12/Stiftung_Umweltenergierecht_Wuestudien_14_Rechtsrahmen-f%C3%BCr-netzdienliche-Flexibilit%C3%A4tsplattformen.pdf, S. 16 f.

die überhaupt für die Verarbeitung personenbezogener Daten in Frage kommen (personeller Anwendungsbereich). Berechtigte Stellen sind nach § 49 Abs. 2 MsbG Messstellenbetreiber, Netzbetreiber, Bilanzkoordinatoren, Bilanzkreisverantwortliche, Direktvermarktungsunternehmer nach dem EEG, Energielieferanten sowie jede Stelle, die über eine Einwilligung des Anschlussnutzers verfügt, die den Anforderungen des Art. 7 DS-GVO genügt. Über § 49 Abs. 3 MsbG ist es zudem zulässig, dass die nach § 49 Abs. 2 MsbG berechtigten Stellen die Verarbeitung durch einen Auftragsverarbeiter (Art. 28 DS-GVO) durchführen lassen.

§ 50 MsbG befasst sich mit zulässigen Zwecken und dem Umfang der Datenverarbeitung (sachlicher Anwendungsbereich). Die Verarbeitung von Daten ist dann zulässig, wenn eine der Voraussetzungen des § 50 MsbG vorliegt[126]. Diese Voraussetzungen sind:

- die Einwilligung des Anschlussnutzers (§ 50 Abs. 1 Alt. 1 MsbG),
- die Erforderlichkeit zur Erfüllung eines der in § 50 Abs. 1 Nr. 1-4 MsbG genannten Zwecke (beispielsweise die die Erfüllung von Verträgen, die Erfüllung rechtlicher Verpflichtungen oder die Aufgabenwahrnehmung des Netzbetreibers, § 50 Abs. 1 Alt. 2 MsbG[127]) oder
- das Vorliegen von einem der 13 explizit genannten Sonderfälle in § 50 Abs. 2 MsbG.

b) Anwendbarkeit des § 50 MsbG auch auf nicht-personenbezogene Daten?

Im Rahmen des Messstellenbetriebsgesetzes ist in Hinblick auf den Datenbegriff zudem Folgendes zu beachten: Während § 49 MsbG („Verarbeitung personenbezogener Daten“) ausdrücklich auf „personenbezogene Daten“ abstellt, ist § 50 MsbG („Zulässigkeit und Umfang der Verarbeitung von Daten“) unspezifischer formuliert und spricht von „Daten“ im Allgemeinen[128]. Es stellt sich daher die Frage, ob, und wenn ja, inwiefern, sich hierdurch Unterschiede ergeben. Aufgrund des engen sachlichen Zusammenhangs von § 49 und § 50 MsbG[129] und ausweislich der Gesetzesbegründung ist jedenfalls davon auszugehen, dass Daten im Sinne des MsbG auch personenbezogene Daten umfasst. Das heißt, immer wenn im MsbG schlicht die Rede von Daten ist, so sind hierunter mindestens auch personenbezogene Daten zu verstehen[130].

Umgekehrt ist aber zu klären, ob § 50 MsbG neben personenbezogenen Daten auch die sonstigen Daten umfasst, oder aber mit Blick auf die DS-GVO auf personenbezogene Daten zu beschränken ist. Wenn auch sonstige Daten umfasst sind, dann folgt daraus, dass auch anonymisierte, nicht-personenbezogene Daten nur unter den genannten Voraussetzungen des § 50 MsbG verarbeitet werden dürfen. Dies würde gerade im Rahmen des Asset Logging dazu führen, dass diese Voraussetzungen auch dort zu beachten sind, selbst wenn regelmäßig kein Personenzug der dort Verarbeiteten Daten anzunehmen ist (siehe unter C. II. 2. .).

Mit Blick auf die Grundprinzipien der DS-GVO und deren Vorgaben für den Schutz personenbezogener Daten wird teilweise angenommen, dass auch im Bereich des MsbG eine entsprechende Einschränkung bezüglich der Datenverarbeitung vorzunehmen ist, um die Parallelität des Schutzbereichs beider Rechtsordnungen sicherzustellen[131]. Andererseits legen insbesondere die bereits genannte Verschiedenheit der Formulierung zu § 49 MsbG, die Gesetzesbegründung sowie die Tatsache, dass das MsbG auch an anderen Stellen den Schutz von nicht-personenbezogenen Daten kennt (beispielsweise bei der Erhebung nach § 59 MsbG), nahe, dass eine derart pauschale

[126] *Lüdemann/Pokrant/Ortmann*, in: Rohrer/Karsten/Leonhardt, MsbG, 2018, § 50 Rn. 1 f.

[127] *Lüdemann/Pokrant/Ortmann* in: Rohrer/Karsten/Leonhardt, MsbG, 2018, § 50 Rn. 11 ff.

[128] *Lüdemann/Pokrant/Ortmann* in: Rohrer/Karsten/Leonhardt, MsbG, 2018, § 49 Rn. 2.

[129] Namentlich der Konkretisierung von § 49 MsbG durch § 50 MsbG, siehe BT-Drs. 18/7555, S. 105.

[130] BT-Drs. 18/7555, S. 105; *Bretthauer*, Smart Meter im Spannungsfeld zwischen Europäischer Datenschutzgrundverordnung und Messstellenbetriebsgesetz, EnWZ 2017, S. 56 (59).

[131] *Bremen/Börkey*, in: Steinbach/Weise, Messstellenbetriebsgesetz, 2. Aufl. 2018, § 50 Rn. 4, insbesondere mit Blick auf Art. 6 I f) DS-GVO und einen möglicherweise weitergehenden Schutzbereich von sonstigen Daten gegenüber personenbezogenen Daten, wodurch ein Wertungswiderspruch entstünde.

Verkürzung des Schutzbereichs nicht vorgesehen ist[132].

Übergeordnet ist jedenfalls zu berücksichtigen, dass sich § 50 MsbG schon grundsätzlich nur auf solche Daten bezieht, die beim Einsatz von Messsystemen anfallen. Es ist anzunehmen, dass der allgemeine Datenbegriff in § 50 MsbG gewählt wurde, um solche Messdaten unabhängig von ihrem Personenbezug vollumfänglich erfassen zu können. Inwieweit die Vorschrift dann aber beispielsweise auch auf derartige Daten Anwendung findet, die ursprünglich personenbezogen waren, aber irreversibel anonymisiert wurden, gerade um die freie Verarbeitung in Zusammenhang mit neuen Konzepten zu ermöglichen, ist fraglich. Auch wenn nicht davon auszugehen ist, dass das MsbG die Möglichkeit der Datenverarbeitung im Rahmen der technischen Fortentwicklung der irreversiblen Datenverschlüsselung erschweren soll, wäre es aber denkbar, neue Katalogtatbestände in § 50 Abs. 2 MsbG einzufügen, um derartige Konflikte zu lösen und die Datenverarbeitung für solche Konzepte unproblematischer zu gestalten.

3. Zulässigkeit der Datenverarbeitung im Rahmen des BDSG

Soweit der Anwendungsbereich des BDSG für die Datenverarbeitung eröffnet ist (also nicht der Vorrang des MsbG die Verarbeitung nach anderen Vorschriften ausschließt[133]), so ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle nach § 3 BDSG immer dann zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist. Weitere Erlaubnistatbestände finden sich zudem in den § 22 ff. BDSG.

4. Besonderheiten bei der Einwilligung

Beim Einholen einer Einwilligung ist darauf zu achten, dass alle Wirksamkeitskriterien erfüllt sind. Zur genaueren Bestimmung dieser Kriterien kann wiederum die DS-GVO herangezogen werden (hier insbesondere Art. 4 Nr. 11 und Art. 7 DS-GVO)[134]. Es besteht ein gewisser Gleichlauf der Einwilligungsvoraussetzungen im Rahmen der DS-GVO und des MsbG, weshalb die Thematik übergeordnet zu den Besonderheiten der speziellen Regelwerke erläutert wird.

a) Wirksamkeitsvoraussetzungen

Eine wirksame Einwilligung muss demnach durch eine Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Erteilung von der betroffenen Person, *vor* Verarbeitung und *höchstpersönlich*[135] erteilt werden. Zudem sind auf Seiten des Einwilligenden *Freiwilligkeit*, *Informiertheit* und *hinreichende Bestimmtheit* erforderlich.

Bezüglich der *Freiwilligkeit* ist zu beachten, dass insbesondere die Erfüllung eines Vertrags nicht von der Einwilligung abhängig gemacht werden darf, wenn die Einwilligung des Betroffenen per se nicht zur Vertragserfüllung erforderlich ist. Es ist also unzulässig, einen Vertrag abzuschließen, dem Vertragspartner die Erbringung der Leistung dann aber vorzuenthalten, um diesen zur Abgabe einer Einwilligung zu bewegen (sog. vertikales Kopplungsverbot)[136].

Das Kriterium der *Informiertheit* erfordert es, dass der Betroffene eine Einwilligung in Kenntnis der Sachlage abgibt. Nach Erwägungsgrund 42 der DS-GVO sollte die betroffene Person hierfür mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen.[137] Diese Vorgaben der DS-GVO sind auch bei einer Einwilligung im Rahmen des MsbG zu

[132] BT-Drs. 18/7555, S. 105; *Lüdemann/Pokrant/Ortmann*, in: Rohrer/Karsten/Leonhardt, MsbG, 2018, § 49 Rn. 2, § 50 Rn. 4.

[133] *Raabe/Lorenz* in: Säcker, Berliner Kommentar zum Energierecht, 4. Aufl. 2017, § 49MsbG Rn. 1.

[134] *Lüdemann/Pokran*t, Die Einwilligung beim Smart Metering, DuD 6/2019, 365 (366 ff.).

[135] Siehe auch Art. 4 Nr. 1 DS-GVO, der die betroffene Person als die natürliche Person bezeichnet, die durch Informationen identifiziert oder identifizierbar ist.; *Lüdemann/Pokrant*, Die Einwilligung beim Smart Metering, DuD 6/2019, 365 (369 f.).

[136] *Gola*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 85; *Steege*, Ist die DS-GVO zeitgemäß für das autonome Fahren?, MMR 2019, S. 509 (511).

[137] *Lüdemann/Pokrant*, Die Einwilligung beim Smart Metering, DuD 6/2019, 365 (366).

beachten.[138] Laut Erwägungsgrund 32 der DS-GVO soll die Einwilligung durch eine eindeutige bestätigende Handlung erfolgen, mit der unter anderem unmissverständlich das Einverständnis bekundet wird. Dies lässt auf das Erfordernis eines „Opt-ins“ schließen[139].

Das Erfordernis der *Bestimmtheit* stellt sicher, dass der Betroffene im Zeitpunkt der Einwilligung auch weiß, für welchen jeweiligen Fall seine Daten verarbeitet werden. Dies umfasst beispielsweise auch die Kenntnis über den Kreis der Datenempfänger oder die Weitergabe der Daten in andere Länder und ähnliche Einzelheiten[140]. Eine Einwilligung darf demnach nicht zu allgemein formuliert oder als Blanko-Erklärung ausgestaltet sein. Dem Einwilligenden müssen zum Zeitpunkt der Einwilligung auch dann alle Verarbeitungsvorgänge bekannt sein, wenn die Daten faktisch beliebig nutzbar sind. Jede nachträgliche Änderung oder Erweiterung bedarf einer neuen Einwilligung, sofern kein gesetzlicher Erlaubnistatbestand einschlägig ist, der mit den ursprünglichen Erhebungszwecken vereinbar ist. Einzig die anfängliche Festlegung von Zwecken, über deren tatsächlichen Einsatz erst später entschieden wird, schon bei Einholung der Einwilligung ist in diesem Zusammenhang denkbar[141].

Nur unter Beachtung der dargelegten Voraussetzungen ist eine Einwilligung auch als wirksam anzusehen. Dies ist zu beachten, wenn im Rahmen von Asset Logging-Anwendungsfällen auf das Instrument der Einwilligung zur Datenverarbeitung zurückgegriffen werden soll.

b) Das Widerrufsrecht des Betroffenen

Zu bedenken ist überdies, dass eine Einwilligung nur begrenzt „zukunftssicher“ ist, da Art. 7 Abs. 3 DS-GVO regelt, dass eine solche jederzeit vom Betroffenen widerrufen werden kann. Die Verarbeitung ist dann mit Wirkung für die Zukunft nicht mehr zulässig ist und der Betroffene kann eine Löschung der erhobenen Daten (auch bei Dritten) verlangen. Dies kann beim Verantwortlichen zu logistischem und technischem Aufwand führen und sollte daher bedacht werden, wenn sich für den Weg der Datenverarbeitung über die Einwilligung entschieden wird. Eine Belehrung über diese Widerrufsmöglichkeit muss bei Abgabe der Einwilligung erfolgen.

Insbesondere bei der Verknüpfung von Verarbeitung personenbezogener Daten und Blockchain-Technologie ergeben sich Schwierigkeiten, die nicht ohne weiteres zu lösen sind, weil das Grundprinzip der Blockchain gerade keine nachträgliche Löschung zulässt (dazu sogleich mehr).

IV. Rechte und Pflichten bei der Datenverarbeitung

Neben der Frage der Zulässigkeit der Datenverarbeitung an sich, ergeben sich aus der DS-GVO eine Reihe von Rechten beziehungsweise Pflichten, die bei der Verarbeitung personenbezogener Daten stets zu beachten sind. Im Folgenden sollen insbesondere das Erfordernis eines zentralen Ansprechpartners sowie das Recht auf Löschung thematisiert werden, da sie vorliegend die größte Relevanz aufweisen.

1. Zentraler Ansprechpartner beziehungsweise Verantwortlicher nach Art. 4 Nr. 7, Art. 5 Abs. 2 und Art. 24 ff. DS-GVO

Das System der DS-GVO sieht zunächst vor, dass es stets einen oder mehrere Verantwortliche gibt (Art. 4 Nr. 7 DS-GVO), die sicherstellen, dass die in der Verordnung angeführten Pflichten auch tatsächlich erfüllt werden. Nach Art. 5 Abs. 2 DS-GVO ist dieser/sind diese zur Rechenschaft über die Einhaltung der Pflichten der DS-GVO verpflichtet. In Art. 24 DS-GVO heißt es, dass der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen

[138] *Bitkom e.V.*, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Blockchain und Datenschutz, Faktenpapier, S. 31.

[139] Beim Opt-in-Verfahren muss der Betreffende aktiv seine Zustimmung bekunden, z.B. durch einen Haken beim Feld „Ja, ich stimme der Verarbeitung zu ..." in einem Web-Formular.

[140] *Klement*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 7 Rn. 68.

[141] *Lüdemann/Pokrant*, Die Einwilligung beim Smart Metering, DuD 6/2019, 365 (367) m.w.N.

Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umsetzt, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

Gibt es mehrere Verantwortliche, so regelt Art. 26 DS-GVO, dass sie in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht. Es ist in diesem Zusammenhang auch zu beachten, dass der Einfluss der Verantwortlichen nicht gleich groß sein muss, solange jeder Verantwortliche einen adäquat-kausalen Beitrag zur Datenverarbeitung leistet (es ist insbesondere ausreichend, dass eine natürliche oder juristische Person aus Eigeninteresse Einfluss auf die Verarbeitung der Daten nimmt). Dies gilt unabhängig von Eigentum oder Herrschaftssphäre der Infrastruktur zur Datenverarbeitung, Aufteilung der Integrität des Prozesses oder der Funktionsherrschaft[142].

Soweit personenbezogene Daten verarbeitet werden, kann das bereits dargestellte Prinzip der Verantwortlichkeit nach Art. 4 Nr. 7 DS-GVO vor allem bei der Verwendung einer öffentlichen (public) Blockchain einen hohen technischen Aufwand erfordern und zu Konflikten führen. Die Einrichtung einer zentralen Stelle, die Transaktionen und Vertragsdurchführung überwacht, widerspricht dem Grundgedanken der Öffentlichkeit, denn typischerweise kennen sich die Parteien nicht und es sorgt erst die Mehrheit der im P2P-Netzwerk beteiligten Rechner dafür, dass alle Transaktionen ordnungsgemäß durchgeführt werden[143].

Für das Konzept Asset Logging kann diese Problematik durch Verwendung einer privaten Blockchain (siehe unter A. II. 3. .) gelöst werden. Schwierigkeiten bezüglich der Zuordnung der Verantwortlichkeit sieht sich die private Blockchain nicht ausgesetzt, da es regelmäßig einen Organisator geben wird, der dann als Verantwortlicher i.S.d. DS-GVO anzusehen ist und im Zweifel für die Einhaltung entsprechender Pflichten haften muss.

2. Recht auf Löschung (Recht auf Vergessenwerden), Art. 17 DS-GVO

Wenn der Grund für die Datenverarbeitung wegfällt (Widerruf der Einwilligung oder Wegfall des Katalogtatbestands) und der Betroffene dies verlangt, ist der Verantwortliche gemäß Art. 17 DS-GVO zur Löschung verpflichtet und muss unter Berücksichtigung von verfügbaren Technologien auch bei Dritten, die diese Daten beziehungsweise Kopien der Daten, Links etc. verwenden, eine Löschung herbeiführen.[144] Die Arbeitsschritte zur Berücksichtigung dieser Rechte und Pflichten können bei großer Verbreitung von Daten mit einigem logistischen Aufwand verbunden sein und auch eine entsprechend hohe Serverleistung erfordern[145].

Problematisch ist mit Blick auf die Verwendung einer Blockchain (soweit es nach dem bereits Dargestellten um die Verarbeitung personenbezogener Daten geht), dass sich diese und das Recht auf Löschung grundsätzlich widersprechen[146]. Die grundlegende Idee der Blockchain, Daten lückenlos, nachvollziehbar und für die „Ewigkeit“ zu speichern, widerspricht der in Art. 17 DS-GVO vorgesehenen Pflicht, Daten unwiederbringlich zu löschen[147]. In diesem Zusammenhang sind zudem die Rechte auf Korrektur (Art. 16 DS-GVO) und auf Sperrung (Art. 18 DS-GVO) zu erwähnen, auch dort weist die Blockchain-Technologie aufgrund ihrer Unveränderlichkeit erhöhtes Konfliktpotenzial auf[148]. Überdies stellt sich

[142] *Specht-Riemenschneider/Schneider*, Die gemeinsame Verantwortlichkeit im Datenschutzrecht, MMR 2019, S. 503 (504 f.).

[143] *Kaularz/Heckmann*, Smart Contracts–Anwendungen der Blockchain-Technologie, CR 2016, 618 (620).

[144] *Dena-ANALYSE*, Datenschutz und Datensicherheit, 2018, S. 8; *Belz*, Wie Energieunternehmen die Datenmengen aus dem Digitalisierungsnetz meistern können, et 5/2019, S 60 (60 f.).

[145] *Belz*, Wie Energieunternehmen die Datenmengen aus dem Digitalisierungsnetz meistern können, et 5/2019, S. 60 (61).

[146] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1258).

[147] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1252).

[148] *Schawe*, Blockchain und Smart Contracts in der Kreativwirtschaft, MMR 2019, 218 (221), *Scholtka/Kneuper*, Lokale Energiemärkte auf Basis der Blockchain-Technologie, IR 2019, 17 (21); *Funke*,

erneut das Problem der dezentralen Verantwortlichkeit und damit einer möglicherweise mangelnden Durchsetzbarkeit der Löschungsrechte[149]. Insofern führt die Einhaltung des Rechts auf Löschung beim momentanen Entwicklungsstand der Gesetzeslage, Rechtsprechung und Technologie stets dazu, dass sich das Grundprinzip der Blockchain zu einem gewissen Grad erforderlichen Kompromissen ausgesetzt sieht[150].

Da die Datenlöschung nicht mit Vernichtung der Daten gleichzusetzen ist, dürfen keine zu hohen Anforderungen an die Löschung gestellt werden[151]. Für die bloße Löschung wird daher das Unkenntlichmachen der gespeicherten personenbezogenen Daten genügen, das heißt, die Daten müssen für den Verantwortlichen unlesbar werden, beziehungsweise dürfen für ihn nicht mehr zur Verfügung stehen[152]. Gleichzeitig muss der Verantwortliche aber sicherzustellen, dass der Zugriff auf die Daten durch Dritte nicht mehr oder nur noch mit unverhältnismäßig hohem Aufwand möglich ist[153].

Sofern das BDSG Anwendung bezüglich der Datenverarbeitung findet, ergibt sich aus § 35 Abs. 1 BDSG, dass ein geringerer Maßstab anzusetzen ist. Die Pflicht zur Löschung besteht nicht, wenn bei nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung eine Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen ist. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Art. 18 DS-GVO.

Anknüpfend an diese bestehenden Einschränkungen des Rechts auf Löschung könnte sich grundsätzlich bei Verwendung einer Blockchain als milderes Mittel zur Löschung im eigentlichen Sinne die Chance bieten, dieser in der Form nachzukommen, dass nur der Zugriff auf den Personenbezug der jeweiligen Daten oder auf den Schlüssel zur Aufhebung der Entpersonalisierung verweigert wird, ohne dass das System der Blockchain zu viel seines Charakters verliert[154].

Insbesondere durch eine entsprechende technische Ausgestaltung, die eine Verwendung der oben dargestellten Mechanismen Hashing und Merkle-Trees vorsieht (siehe A. II. 4. .), kann jedenfalls im Rahmen des Konzepts Asset Logging mittels Blockchain-Technologie dafür gesorgt werden, dass ursprünglich personenbezogene Daten nur irreversibel anonymisiert auf einer Blockchain gespeichert werden[155]. Diese Daten sind dann als nicht-personenbezogene Daten anzusehen. Da infolgedessen schon die Anwendbarkeit der DS-GVO entfällt, muss auch das Recht auf Löschung nicht berücksichtigt werden.

Rechtliche Aspekte der Blockchain und ihrer virtuellen Währungen, et 4/2018, 27 (29).

[149] *Köhler/Müller-Boysen*, Blockchain und smart contracts – Energieversorgung ohne Energieversorger?, ZNER 2018, 203 (207).

[150] *Gödeke/Jördening*, Blockchain-Lösungen für die Versorgungswirtschaft, VersorgW 2019, 5 (11) m.w.N., verweisen auf das Fehlen einer gefestigten Rechtsprechung im Bereich der Blockchain-Technologie; *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1254 ff.) m.w.N., die zum damaligen Zeitpunkt wohl nicht davon ausgingen, dass eine Erfüllung der Pflicht auf Löschung mit der Verwendung der Blockchain-Technologie vereinbar ist und deshalb auf eine mögliche Ausgestaltung beziehungsweise Anpassung der Rechtslage verweisen.

[151] *Bartsch*, in: Theobald/Kühling, Energierecht, 2020, 230, Datenschutz in Energieversorgungsunternehmen, Rn. 66; so auch *Bartsch/Rieke,* Das neue Datenschutzrecht mit Auswirkungen auch auf Energieversorger, EnWZ 2017, S. 435 (439).

[152] *Bartsch/Rieke*, Das neue Datenschutzrecht mit Auswirkungen auch auf Energieversorger, EnWZ 2017, 435 (439).

[153] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ, S. 1251 (1255).

[154] Vgl. *Funke*, et 4/2018, 27 (29); auch eine solche Vorgehensweise setzt eine technische Ausgestaltung voraus, die je nach Art des Use Cases mit mehr oder weniger Aufwand verbunden sein wird, weshalb als Lösung teilweise eine gesetzgeberische Abwandlung des Rechts auf Löschung in ein Recht auf Pseudonymisierung für komplexe dezentral organisierte IT-Architekturen vorgeschlagen wird, vgl. *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ S. 1251 (1258); diese zitierend auch: *Scholtka/Kneuper,* Lokale Energiemärkte auf Basis der Blockchain-Technologie, IR 2019, S. 17 (20).

[155] Vgl. so auch BNetzA, Die Blockchain-Technologie – Grundlagen, Potenziale und Herausforderungen, 2021, S. 22.

3. Weitere relevante Rechte und Pflichten

Neben dem Erfordernis eines zentralen Ansprechpartners und dem Recht auf Löschung sieht die DS-GVO weitere relevante Rechte und Pflichten vor. Insbesondere relevant sind Zweckbindung und Datenminimierung nach Art. 5 Abs. 1 DS-GVO, die Beweislastumkehr nach Art. 5 Abs. 2 DS-GVO[156] sowie die ausreichende Information durch den Verantwortlichen nach Art. 13 DS-GVO. Dieser hat hier ganz grundlegende Informationen, wie beispielsweise Name und Kontaktdaten, die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung, weiterzugeben. Daneben muss er über die Dauer, für die die personenbezogenen Daten gespeichert werden, das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen sowie auf Berichtigung oder Löschung und das Bestehen eines Rechts, eine Einwilligung jederzeit zu widerrufen, informieren.

Auch diese Rechte/Pflichten greifen jedoch dann nicht, wenn etwa durch technische Gestaltung der Personenbezug der Daten aufgehoben wird.

V. Zwischenergebnis

Zumeist stellen Anlagen-Daten im Kontext des Asset Logging Daten ohne Personenbezug dar und fallen dann jedenfalls nicht in den Anwendungsbereich der DS-GVO (möglicherweise aber dennoch teilweise in den Anwendungsbereich des MsbG, vgl.o.), weshalb auch die dort genannten Pflichten in diesen Fällen nicht beachtet werden müssen.

Handelt es sich in Einzelfällen doch um Daten mit Personenbezug, so ist das Pflichtenprogramm der DS-GVO und des MsbG dagegen vollumfänglich zu beachten. Das heißt, es muss eine wirksame Einwilligung eingeholt werden oder ein sonstiger Erlaubnistatbestand vorliegen und im Rahmen der DS-GVO insbesondere das Recht auf Löschung im Blick behalten werden. Dieses erfordert bei der Verwendung einer Blockchain sinnvollerweise die irreversible Anonymisierung der Daten und somit den Ausschluss des Personenbezugs bereits vor Speicherung auf der Blockchain. Es können dazu entsprechende technische Möglichkeiten wie Hashing beziehungsweise Merkle-Trees genutzt werden, um die Vorzüge der Blockchain-Technologie für das Asset Logging aufrechtzuerhalten, ohne personenbezogene Daten auf ihr zu speichern.

[156] Aufgrund dieses Prinzips ist beim Einholen einer Einwilligung trotz nicht bestehendem Formerfordernis die schriftliche Einwilligung aufgrund der Rechenschaftspflichten des Verantwortlichen zu empfehlen.

D. Gesamtergebnis

Als Gesamtergebnis zum Thema „Asset Logging mittels Blockchain-Technologie“, wie es im Rahmen des Forschungsprojektes „InDEED“ verstanden und untersucht wird, können folgende Thesen festgehalten werden:

1. Asset Logging mittels Blockchain-Technologie meint, dass Anlagen-Daten (etwa Betriebs-, Wartungs- und Instandhaltungsdaten) aus vertrauenswürdigen Quellen nach deren Erhebung mittels Blockchain-Technologie gespeichert werden. Als Internet-Plattform konzipiert, werden die Daten bestimmten Akteuren im Rahmen bestimmter Use Cases bereitgestellt. Die Nutzung der Blockchain-Technologie gewährleistet dabei besondere Sicherheitseigenschaften wie insbesondere Daten-Integrität.
2. Der Gesetzgeber sieht verschiedene Pflichten für Behörden im Energiesektor vor, Internet-Plattformen und Daten-Register zu betreiben, etwa im Bereich des Marktstammdatenregisters sowie bezüglich der Informationsplattform zu Strommarktdaten. Private Akteure sind hier verpflichtet, bestimmte Daten bereitzustellen. Zudem bestehen Informationsansprüche Privater untereinander, etwa für Netzbetreiber. Asset Logging mittels Blockchain-Technologie bietet hier – aber auch darüber hinaus – mögliche Anwendungsfelder.
3. Weitere Anwendungsfelder bestehen im Rahmen der zivilrechtlichen Vertragsgestaltung, etwa im Bereich Wartungs- oder Garantieverträge. Die Nutzung von Blockchain-basierten Internet-Plattformen kann hier Relevanz entfalten. Einen Mehrwert kann dies zumindest potenziell beim Beweis von Anlagen-Daten im Streitfall bieten. Allerdings kann die Blockchain zumindest aktuell die Anforderungen an förmliche Beweismittel nicht erfüllen.
4. Die verarbeiteten Anlagen-Daten können zumindest im Einzelfall in den Anwendungsbereich von DS-GVO, MsbG und BDSG fallen. Das Einholen einer Einwilligung beziehungsweise das Vorliegen eines sonstigen Erlaubnistatbestands ist dann erforderlich. Auch ist im Falle personenbezogener Daten den datenschutzrechtlichen Verpflichtungen, insbesondere der Pflicht zur nachträglichen Löschung, grundsätzlich nachzukommen. Durch eine entsprechende Plattform-Architektur in Verbindung mit geeigneten technischen Hilfsmitteln wie Hashing beziehungsweise Merkle Trees kann ein Konflikt zwischen Asset Logging mittels Blockchain-Technologie und den Vorgaben des Datenschutzrechts vermieden werden.

Kontakt
Stiftung Umweltenergierecht
Friedrich-Ebert-Ring 9
97072 Würzburg

T: +49 931 794077-0
F: +49 931 7940 77-29

info@stiftung-umweltenergierecht.de
www.stiftung-umweltenergierecht.de

Entstanden im Rahmen des Vorhabens:
InDEED – Konzeption, Umsetzung und Evaluation einer auf Blockchain basierenden energiewirtschaftlichen Datenplattform für die Anwendungsfälle ‚Labeling' und ‚Asset Logging'

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

InDEED