> ARGJENTA VESELI / MARIE-THERES HOLZLEITNER / STEPHAN CEJKA

D.S.G.V.O.: Datenverwendung Smart Gemacht und Verbraucherfreundlich Organisiert

Ein wichtiger Baustein der Energiewende wird in immer größer werdendem Ausmaß die Verfügbarkeit von Daten. Dieser Artikel geht daher der Frage nach, wie große Mengen an Energie(verbrauchs)daten, die für smarte Lösungsansätze und Technologien erforderlich sind, datenschutzrechtlich zu qualifizieren sind, welche Rechte und Pflichten sich daraus ergeben und präsentiert, wie etwaige Problemstellungen neuer Technologien mit diesen Vorschriften in Einklang zu bringen sind.

I. Einleitung

Die Energiewende ist stark von neuen Technologien, Geschäftsmodellen und Akteuren geprägt. Zukünftig sollen Verbraucher vermehrt in den Fokus rücken und von „einfachen" Verbrauchern zu sog Prosumern[1] (also auch Erzeugern) werden. Auch viele weitere Akteure wie bspw Energiespeicher, Aggregatoren etc werden Teil des neuen Energiesystems sein.

Um eine effiziente Interaktion all dieser (neuen) Marktrollen und eine höchstmögliche Integration erneuerbarer Energien insb in Anbetracht des zunehmend dezentralen und volatilen Strommarktes zu ermöglichen, ist ein intelligentes Stromversorgungsnetz sog Smart Grid erforderlich. Mithilfe eines Smart Grids werden ua Informationen von Verbrauchern im Netz derart kombiniert, dass eine wirksamere und wirtschaftlichere Planung der Stromversorgung erzielt wird.[2] Smart Grids ermöglichen eine Interaktion aller Akteure des Energiesystems über ein Kommunikationsnetzwerk.[3] Basis eines intelligenten Stromnetzes sind intelligente Verbrauchsmessgeräte (sog Smart Meter).[4] Smart Meter sind digitale Verbrauchszähler, die eine Zweiwege-Kommunikationskapazität aufweisen und Informationen von der gemessenen Einheit in nahezu Echtzeit und mit einer sehr hoher Granularität der Daten übertragen. Mit intelligenten Zählern erhöht sich die Menge an verfügbaren Energieverbrauchs-Daten enorm. Dieser Artikel beleuchtet daher zunächst die energierechtlichen Grundlagen von Smart Metern und iwF ob der EU-Datenschutzrahmen idZ einschlägig ist und wenn ja, welche Rechtsfolgen daran knüpfen.

Ebenfalls Teil des zukünftigen Energiesystems werden Energiegemeinschaften sein.[5] Innerhalb dieser soll bspw Strom erzeugt, verbraucht und gespeichert werden können. Für die technische Implementierung einer Energiegemeinschaft kann der Einsatz der Blockchain-Technologie angedacht werden. Blockchain ist eine dezentrale Datenbank, die von beteiligten Servern (sog Nodes) des Blockchain-Netzwerkes geführt wird und bei der jeder Teilnehmer seine eigene Kopie speichert und verarbeitet.[6] Da in der Blockchain ebenfalls große Mengen an Daten verarbeitet werden und die Blockchain durch Unveränderlichkeit gekennzeichnet ist, werden in diesem Artikel deren Vereinbarkeit mit dem Datenschutz analysiert und mögliche Lösungsansätze präsentiert.

II. Energierechtliche Aspekte von Smart Metern

§ 7 Abs 1 Z 31 ElWOG 2010[7] definiert ein intelligentes Messgerät als „eine technische Einrichtung die den tatsächlichen Energieverbrauch und Nutzungszeitraum zeitnah misst und die über eine fernauslesbare, bidirektionale Datenübertragung verfügt." Basierend

1 Dieser Begriff setzt sich aus „Producer" und „Consumer" zusammen.

2 Vgl *Artikel 29 Datenschutzgruppe*, Stellungnahme 12/2011 zur intelligenten Verbrauchsmessung („Smart Metering") (2011) 5.

3 Zur Definition von Smart Grids siehe die Homepage der Technologieplattform Smart Grids Austria abrufbar unter: <https://www.smartgrids.at/smart-grids.html> (Stand 30.11.2020).

4 Vgl *Artikel 29 Datenschutzgruppe*, Verbrauchsmessung (FN 2) 5.

5 Vgl *Cejka*, Energiegemeinschaften im Clean Energy Package der EU, ecolex 2020, 338.

6 Vgl *Nascimento* et al, Blockchain now and tomorrow (2019), 13 ff.

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

auf § 83 Abs 1 ElWOG 2010 wurde in § 1 Abs 1 IME-VO8 festgelegt, dass jeder Netzbetreiber:[9]

- bis Ende 2015 einen Projektplan über die stufenweise Einführung von intelligenten Messgeräten samt Angabe eines Zielerreichungspfades vorzulegen hat,
- bis Ende 2020 min 80 vH und
- im Rahmen der technischen Machbarkeit bis Ende 2022 min 95 vH der an sein Netz angeschlossenen Zählpunkte mit intelligenten Messgeräten auszustatten hat.[10]

Der Netzbetreiber hat (ungeachtet des Projektplans über die eben genannte stufenweise Einführung) Endverbraucher auf Wunsch mit einem intelligenten Messgerät auszustatten, wobei die Installation in diesem Fall ehestmöglich, höchstens binnen sechs Monaten zu erfolgen hat.[11]

Die Mindestfunktionsanforderungen, denen intelligente Messgeräte zu entsprechen haben, sind durch die Intelligente Messgeräte-AnforderungsVO 2011 (IMA-VO 2011)[12] festgelegt. In der Datenformat- und VerbrauchsinformationsdarstellungsVO 2012 (DAVID-VO 2012)[13] werden die Anforderungen an die Datenübermittlung von Netzbetreiber zu Lieferant und die Verbrauchsinformationen an die Endkunden festgelegt.

Gemäß § 84 Abs 1 ElWOG 2010 hat der Netzbetreiber spätestens sechs Monate ab dem Zeitpunkt der Installation des intelligenten Messgerätes beim jeweiligen Endverbraucher einmal täglich einen Verbrauchswert sowie sämtliche Viertelstundenwerte im intelligenten Messgerät zu erfassen und für 60 Kalendertage zu Zwecken der Verrechnung, Kundeninformation,[14] Energieeffizienz, Energiestatistik und Aufrechterhaltung eines sicheren und effizienten Netzbetriebs im intelligenten Messgerät zu speichern.

Weiters ist der Netzbetreiber gem Art 84 Abs 2 ElWOG 2010 verpflichtet, die täglichen Verbrauchswerte sowie auf ausdrücklichen Wunsch je nach vertraglicher Vereinbarung oder Zustimmung Viertelstundenwerte auszulesen und spätestens zwölf Stunden nach der Auslesung dem Endverbraucher über ein kundenfreundliches Web-Portal kostenlos zur Verfügung zu stellen. Spätestens am Fünften des jeweils darauffolgenden Kalendermonats hat der Netzbetreiber alle täglich erhobenen Verbrauchswerte an die jeweiligen Lieferanten zum Zweck der Verbrauchs- und Stromkosteninformation sowie zu Zwecken der Verrechnung zu übermitteln. Viertelstundenwerte dürfen nur nach ausdrücklicher Zustimmung des Endverbrauchers oder zur Erfüllung vertraglicher Pflichten an den Lieferanten übermittelt werden.[15]

III. Smart Meter und Datenschutz

Smart Meter bieten eine Menge an Vorteilen. Neben regelmäßigen Informationen zu Kosten und Verbrauch, wird die Legung transparenter und nachvollziehbarer Rechnungen ermöglicht sowie Klarheit bei Verbrauchsabgrenzungen etc geschaffen.[16] Mithilfe von Smart Metern können Daten über Verbraucher in großem Umfang erstellt, übermittelt und ausgewertet werden. Viele Akteure am Energiemarkt erhalten so detaillierte Informationen über den Energieverbrauch von Verbrauchern.[17] Dies ist auch durchaus vorteilhaft, da basierend auf diesen Informationen das Verbrauchsverhalten geändert und Energieeinsparungen erzielt werden können; jedoch können auch genaue Rückschlüsse auf das Verbrauchsverhalten (wie bspw, wann jemand zu Hause ist und dgl) getroffen werden. Es sind daher Aspekte des Datenschutzes zu berücksichtigen.[18] In Europa ist das Datenschutzrecht eines der wichtigsten Rechtsinstrumente, wenn Informationen über Personen verarbeitet und genutzt werden.[19] Das Recht auf Schutz personenbezogener Daten ist ein Grundrecht in der EU[20] und gem Art 16 Abs 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)[21] hat jeder das Recht auf Schutz der ihn betreffenden personenbezogenen Daten. Zentrale Rechtsgrundlage zum Schutz natürlicher Personen bei der

8 Verordnung des Bundesministeriums für Wirtschaft, Familie und Jugend, mit der die Eiführung intelligenter Messgeräte festgelegt wird (Intelligente Messgeräte-Einführungsverordnung – IME-VO), BGBl II 138/2012 idF BGBl II 383/2017.

9 § 7 Abs 1 Z 51 ElWOG 2010 (Grundsatzbestimmung).

10 Von dieser Verpflichtung sind solche Endverbraucher ausgenommen, deren Verbrauch über einen Lastprofilzähler gemessen werden (vgl § 1 Abs 3 IME-VO).

11 Vgl § 1 Abs 5 IME-VO.

12 Verordnung der E-Control, mit der die Anforderungen an intelligente Messgeräte bestimmt werden (Intelligente Messgeräte-AnforderungsVO 2011 – IMA-VO 2011), BGBl II 339/2011.

13 Verordnung des Vorstands der E-Control, mit der die Anforderungen an die Datenübermittlung von Netzbetreiber zu Lieferant und die Verbrauchsinformation an die Endkunden festgelegt werden (Datenformat- und VerbrauchsinformationsdarstellungsVO 2012 – DAVID-VO 2012), BGBl II 313/2012 idF BGBl II 468/2013.

14 Vgl § 81a ElWOG 2010.

15 Vgl § 84a Abs 2 ElWOG 2010.

16 Vgl *E-Control*, Smart Meter unterliegen strengen Datenschutzbestimmungen (2014) 3.

17 Vgl *Artikel 29 Datenschutzgruppe*, Verbrauchsmessung (FN 2) 2.

18 Vgl *Schrott*, Einführung intelligenter Messgeräte („Smart Meter") iZm Datenschutz und Datensicherheit, in Jahnel (Hg), Datenschutzrecht Jahrbuch 2014, 163 (163 f).

19 Vgl Art 1 und 6 sowie ErwGr 1, 13 und 14 DSGVO.

20 Vgl Art 8 Abs 1 GRC (Charta der Grundrechte der Europäischen Union, ABl 2012 C 326/391).

21 Vertrag über die Arbeitsweise der Europäischen Union, ABl 2012 C 326/47.

Verarbeitung personenbezogener Daten ist die europäische Datenschutzgrundverordnung (DSGVO).[22] Die DSGVO ist ein wesentlicher Schritt zur Stärkung der Grundrechte der Bürger im digitalen Zeitalter. Die Besonderheiten der Smart Meter werfen einige wichtige spezifische Fragen in Bezug auf die Anwendung der DSGVO (wie bspw die Qualifizierung von „Energiedaten") auf. Dieses Kapitel eruiert daher, welche Daten in den Anwendungsbereich der DSGVO fallen und insb ob dies bei Energie(verbrauchs)daten der Fall ist, welche Rechte und Pflichten aus der Anwendbarkeit der DSGVO resultieren und wer für die Einhaltung dieser Rechte verantwortlich ist.

A. Personenbezogene Daten

1. Allgemeines zu personenbezogenen Daten iSd DSGVO

Gem Art 2 DSGVO ist der Anknüpfungspunkt der DSGVO die „Verarbeitung[23] personenbezogener Daten", die sowohl die ganz oder tlw automatisierte Verarbeitung als auch die nicht-automatisierte Verarbeitung personenbezogener Daten (die in einem Dateisystem gespeichert sind oder gespeichert werden sollen) umfasst.[24] Der Kernbereich der DSGVO ist der Schutz „natürlicher Personen" (während die Verarbeitung personenbezogener Daten, die juristische Personen [und insb als juristische Personen gegründete Unternehmen betrifft] nicht unter die DSGVO fällt),[25] wobei es nicht auf das Bestehen eines Vertragsverhältnisses, sondern auf die faktische Datenverarbeitung ankommt.[26] Es werden somit nur Daten erfasst, die einer natürlichen Person zugeordnet sind.[27]

Art 4 Z 1 DSGVO definiert „personenbezogene Daten" als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person" (betroffene Person) beziehen. Eine natürliche Person gilt als identifiziert, wenn sie mit den verfügbaren Informationen und Mitteln eindeutig identifiziert werden kann.[28] Derselben Bestimmung zufolge wird eine natürliche Person als identifizierbar angesehen, wenn sie direkt oder indirekt, insb mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten udgl identifiziert werden kann. Sie ist auch identifizierbar, wenn sich die betreffenden Daten auf Aspekte ihres Privatlebens beziehen; Faktoren etwa, die spezifisch für die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität dieser natürlichen Person sind.

Zur Feststellung der Identifizierbarkeit einer natürlichen Person sollten alle Mittel, „die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren,"[29] berücksichtigt werden. Für die Beurteilung, ob Mittel nach allgemeinem Ermessen wahrscheinlich genutzt werden, sollten alle objektiven Faktoren (Kosten der Identifizierung, erforderlicher Zeitaufwand) herangezogen und dabei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen berücksichtigt werden.[30] Der EuGH hat sich mit der Frage befasst, aus welcher Perspektive die Identifizierbarkeit gegeben sein muss. Insb hat er geprüft, ob ein Personenbezug vorliegt, wenn sich die Daten, die eine Identifizierung einer Person ermöglichen, nicht am Speicherort des für die Verarbeitung Verantwortlichen selbst befinden.[31] Der relativen Theorie zufolge, ist nur die Perspektive des für die Datenverarbeitung Verantwortlichen zu berücksichtigen, während nach der absoluten Theorie jeder Dritte, der in der Lage sein könnte, eine Identifizierung vorzunehmen, zu berücksichtigen ist.[32]

Der EuGH folgte der relativen Theorie und stellte fest, dass ein Bezug zu einer Person gegeben ist, wenn die betroffene Person vom für die Verarbeitung Verantwortlichen durch zusätzliches Wissen (auch von Dritten) und durch vernünftige Mittel identifiziert werden kann. Er führte aus, es sei für eine Einstufung als „personenbezogenes Datum" nicht erforderlich, „dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden."[33]

22 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), ABl 2016 L 119/1.

23 Der Begriff „Verarbeitung" bezeichnet gem Art 4 Z 2 DSGVO „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe iZm 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".

24 Vgl *Fritz*, Anwendungsbereich und Rechtfertigung – Alles neu macht die DS-GVO? in Jahnel (Hg), Datenschutzrecht Jahrbuch 2016, 9 (18).

25 Vgl Art 1 Abs 1 und ErwGr 14 DSGVO.

26 Vgl *Gabauer/Knyrim*, Checkliste Prüfschema zur datenschutzrechtlichen Rollenverteilung, Dako 2019, 14.

27 Vgl ErwGr 14 DSGVO.

28 Vgl *Finck/Pallas*, They who must not be identified, Max Planck Institute for Innovation and Competition Research Paper Series 2020, 1 (13).

29 ErwGr 26 DSGVO.

30 Vgl ErwGr 26 DSGVO.

31 Vgl EuGH 19.10.2016, C-582/14, *Breyer/DE*, ECLI:EU:C:2016:779.

32 Vgl *Finck*, Blockchain and the General Data Protection Regulation (2019) 24.

33 EuGH 19.10.2016, C-582/14, *Breyer/DE*, ECLI:EU:C:2016:779, Rz 43.

Die DSGVO verwendet auch den Begriff der Pseudonymisierung, der in Art 4 Z 5 DSGVO als „Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können" definiert wird. Personenbezogene Daten werden bei der Pseudonymisierung so bearbeitet (dh verändert/verschlüsselt), dass die Daten nicht mehr ohne Weiteres einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Es ist jedoch möglich die Verschlüsselung bei Bedarf aufzuheben und so den Bezug zur Person wiederherzustellen. Um diese Entschlüsselung durch Unbefugte zu erschweren, müssen die notwendigen Zusatzinformationen getrennt von den personenbezogenen Daten gespeichert werden. Zudem müssen technische und organisatorische Vorkehrungen getroffen werden, um den Zugriff zu verhindern. Im Gegensatz zu den identifizierbaren Personendaten ist die reine Zuordnungsmöglichkeit durch den Datennutzer durch Pseudonymisierung weitestgehend zu verhindern.[34] Die Grundsätze der DSGVO gelten nicht für anonyme Informationen. Solche Informationen beziehen sich entweder nicht auf eine identifizierte oder identifizierbare natürliche Person oder es wurden personenbezogene Daten in einer Weise anonymisiert, die eine Identifizierung der betroffenen Person unmöglich macht.[35]

2. Energiedaten personenbezogene Daten?

Zunächst scheint es, dass durch Smart Meter erfasste Verbrauchsdaten rein technischer Natur sind; jedoch zeigen die gesammelten Daten detaillierte Informationen über das Energieverhalten eines Verbrauchers und spiegeln ua sein Privatleben wider.[36] Die Verbrauchswerte sind einem Zählpunkt zugeordnet und es werden Informationen über das Energieprofil eines Verbrauchers gesammelt. Diese Stromverbrauchsdaten geben zB Einblicke in das tägliche Leben der natürlichen Personen und so Aufschluss über die spezifischen Eigenschaften des Individuums.[37] Die betroffene Person ist identifiziert oder zumindest über den Zählpunkt identifizierbar. Es handelt sich somit um personenbezogene Daten, weshalb die Bestimmungen der DSGVO zur Anwendung gelangen.[38]

B. Recht auf Löschung

Art 5 DSGVO schreibt sieben Grundsätze vor, die bei der Verarbeitung personenbezogener Daten eingehalten werden müssen.[39] Weiters enthält sie umfangreiche Informationspflichten bei der Datenerhebung, Auskunftsrechte, Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit, Widerspruchsrechte sowie das Recht nicht einer automatisierten Einzelentscheidung unterworfen zu sein. Aus Gründen der Einschlägigkeit wird im Folgenden lediglich auf das Recht auf Löschung eingegangen.

Der Verarbeiter personenbezogener Daten ist gem Art 17 Abs 1 DSGVO verpflichtet diese zu löschen, wenn eine betroffene Person nicht mehr möchte, dass ihre Daten verarbeitet werden und sofern kein legitimer Grund zur Behaltung dieser gegeben ist. Mithilfe dieses „Rechts auf Vergessenwerden", soll die Privatsphäre von Individuen geschützt und nicht etwa die Pressefreiheit eingeschränkt werden. Bei Vorliegen einer der in Art 17 Abs 1 DSGVO angeführten Gründe, hat die betroffene Person das Recht vom Verantwortlichen zu verlangen, jene Daten unverzüglich zu löschen, die die Person selbst betreffen. Beispielhaft sei der Grund angeführt, dass personenbezogene Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Die Löschungsverpflichtung besteht jedoch nicht, sofern die Verarbeitung für einen der in Art 17 Abs 3 DSGVO angeführten Gründe erforderlich ist (dazu gehört bspw, dass die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist).

C. Verantwortlicher

Die DSGVO gesteht „betroffenen Personen", wie soeben dargelegt, eine Reihe an Rechten zu. Für die Einhaltung und Gewährleistung dieser Rechte ist der „Verantwortliche" zuständig. In diesem Kapitel wird erläutert, wem unter allgemeinen Grundsätzen die Rolle des Verantwortlichen zukommt und wer konkret beim Einsatz von Smart Metern sowie damit verbundener Verarbeitung von personenbezogenen Daten als Verantwortlicher zu qualifizieren ist.

1. Allgemeines zum Verantwortlichen iSd DSGVO

Gem Art 4 Z 7 DSGVO ist der Verantwortliche jene „natürliche oder juristische Person, Behörde, Einrich-

34 Vgl *Finck/Pallas*, Identified (FN 28), 21 f; *Artikel 29 Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken (2014) 24.

35 Vgl ErwGr 26 DSGVO.

36 Vgl *Smart grids task force*, Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection (2011) 4; verfügbar unter: <https://ec.europa.eu/energy/sites/ener/files/documents/Recommendations%20regulatory%20requirements%20v1_0_clean%20%282%29.pdf> (Stand 01.12.2020).

37 Vgl *Artikel 29 Datenschutzgruppe*, Verbrauchsmessung (FN 2) 8.

38 Vgl *Schrott*, Messgeräte (FN 18) 170.

39 „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz", „Zweckbindung", „Datenminimierung", „Richtigkeit", „Speicherbegrenzung", „Integrität und Vertraulichkeit" und „Rechenschaftspflicht".

tung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Die Hauptaufgabe des Verantwortlichen besteht darin, denjenigen zu ermitteln, der für die Einhaltung der DSGVO verantwortlich ist.[40] Der Verantwortliche ist daher derjenige, der über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet und nicht jener der „rechtmäßig entscheidet." Wichtig ist hier zu betonen, dass es in diesem Kontext nicht um Rechtmäßigkeit iSe rechtlichen Befugnis der entscheidenden Organisation oder dergleichen geht, sondern um die Möglichkeit der einfachen Ermittlung eines für die Verarbeitung Verantwortlichen bei dem tatsächlich die Verantwortung für die Verarbeitung liegt und der (auch im Falle einer unrechtmäßigen Datenverarbeitung) zur Verantwortung gezogen werden kann.[41] Gem Art 26 DSGVO können zwei oder mehrere Verantwortliche gemeinsam Zweck und Mittel zur Verarbeitung festlegen und so als gemeinsame Verantwortliche agieren.

2. Verantwortlicher bei Einsatz von Smart Metern

Im Rahmen von Smart Metering besteht eine Vielzahl von Verarbeitungen personenbezogener Daten durch den Netzbetreiber einerseits und den Lieferanten andererseits. Es ist daher wichtig zu ermitteln, wer idZ als Datenverantwortlicher zu betrachten ist.

Netzbetreiber haben ua die Messung der Bezüge, Leistungen und Lastprofile der Netzbenutzer vorzunehmen[42] und sind gem § 84a Abs 2 ElWOG 2010 zur Übermittlung der Verbrauchswerte der Endverbraucher an die jeweiligen Lieferanten zum Zweck der Verbrauchs- und Stromkosteninformation sowie zu Zwecken der Verrechnung verpflichtet. Da sie die tatsächliche Verfügungsgewalt über die Daten haben, sind Netzbetreiber jedenfalls Verantwortliche iSd DSGVO.[43] Hinsichtlich der vom Netzbetreiber an die Lieferanten übermittelten Verbrauchsdaten für Verrechnungszwecke sowie zum Zweck der Stromverbrauchsinformation sind die Lieferanten betreffend dieser Verarbeitungen Verantwortliche.[44]

IV. Blockchain

Das EU-Legislativpaket „Saubere Energie für alle Europäer" zielt ua darauf ab, Verbraucher in den Mittelpunkt der Energiewende zu stellen und eine aktive Teilnahme an der Umstellung auf erneuerbare Energien zu ermöglichen. Zugang zu Informationen über Energieverbrauch und -kosten, sowie eine verstärkte Digitalisierung, mehr Flexibilität und Auswahl, sind ein wichtiger Baustein zur Erreichung dieses Ziels. Bürgern wird es außerdem ermöglicht sich zu Energiegemeinschaften[45] zusammenzuschließen und innerhalb dieser Energie ua zu erzeugen, zu verbrauchen und zu speichern.[46] Für die technische Implementierung von Energiegemeinschaften wird oftmals der Einsatz der Blockchain-Technologie angedacht. Dabei wird innerhalb der Energiegemeinschaft durch die Teilnehmer Energie erzeugt, gemessen und verkauft, wobei mithilfe der Blockchain ua die Abrechnung in automatisierter Weise durchgeführt wird.

Die Blockchain-Technologie hat sich aus ihrem ursprünglichen Anwendungsbereich (den Kryptowährungen) emanzipiert und wird laufend in anderen Bereichen[47] ua auch der Energiewirtschaft[48] angedacht und auch bereits tlw eingeführt[49]. Die Blockchain bietet einige Vorteile und es ist zurzeit ein Hype iHa diese Technologie festzustellen; jedoch muss in jedem Anwendungsfall im Vorhinein überprüft werden, ob der Einsatz einer Blockchain in concreto hilfreich und notwendig ist. Gerade wenn es (wie zuvor beschrieben) um die Verarbeitung von für die Abrechnung relevante Daten geht, ist jedenfalls der Datenschutz zu berücksichtigten. Denn wie bereits festgestellt, handelt es sich bei Energie(verbrauchs)daten um personenbezogene Daten. Es wird daher zunächst die Funktionsweise der Blockchain beleuchtet und iwF die Vereinbarkeit dieser mit den Vorgaben der DSGVO analysiert und Lösungsansätze präsentiert.

40 Vgl *Artikel 29 Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" (2010) 4.

41 Vgl *Artikel 29 Datenschutzgruppe*, Verarbeitung (FN 40) 11 f.

42 Vgl § 45 Z 10 ElWOG 2010.

43 Vgl *Markl*, Smart Metering und Datenschutz in Österreich, in Steinmüller/Hauer/Schneider (Hg), Jahrbuch Energiewirtschaft 2011, 35 (40 f); *Schrott*, Messgeräte (FN 18) 171 f.

44 Vgl *Trieb*, Smart-Metering-Komponenten – Datenschutzrechtliche Anforderungen an Ausschreibungsbedingungen, Magazin für Energiewirtschaft 2016, 18.

45 Erneuerbare-Energie-Gemeinschaften gem Art 22 EE-RL 2018 (Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Förderung der Nutzung von Energie aus erneuerbaren Quelle, ABl 2018 L 328/82) und Bürgerenergiegemeinschaften gem Art 16 EBM-RL 2019 (Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU, ABl 2019 L 158/125).

46 Vgl *Generaldirektion Energie (Europäische Kommission)*, Saubere Energie für alle Europäer (2019) 14 f; *Cejka*, Energiegemeinschaften (FN 5) 338.

47 Vgl *Casino* et al, A systematic literature review of blockchain-based applications, Telematics and Informatics (2019) 55.

48 Vgl *Mika/Goudz*, Blockchain-Technologie in der Energiewirtschaft (2020); *Andoni* et al, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, Renewable and Sustainable Energy Reviews 2019, 143; *Brilliantova/Thurner*, Blockchain and the future of energy, Technology in Society 2019, 38.

49 Siehe dazu die Forschungsprojekte „SonnWende+" (Projektnummer: 861621) und „Blockchain Grid" (Projektnummer: 868656).

A. Funktionsweise der Blockchain

Technisch gesehen ist die Blockchain eine dezentrale Ledger-Technologie, dh ein verteiltes Register, bei der jeder Teilnehmer seine eigene Kopie speichert und verarbeitet. Da es im System keine zentrale koordinierende Stelle gibt, muss dezentral Konsens zwischen den einzelnen Teilnehmern (genannt Nodes) bezüglich des gültigen Stands der Blockchain hergestellt werden (in der Bitcoin-Blockchain zB mit dem „Proof of Work"-Konsensalgorithmus). In regelmäßigen Zeitintervallen werden Transaktionen mithilfe eines Miners in Blöcke zusammengefasst und diese dann an die derzeitige Blockchain angekettet (**Fehler! Verweisquelle konnte nicht gefunden werden.**) – daher der Name: Blockchain.

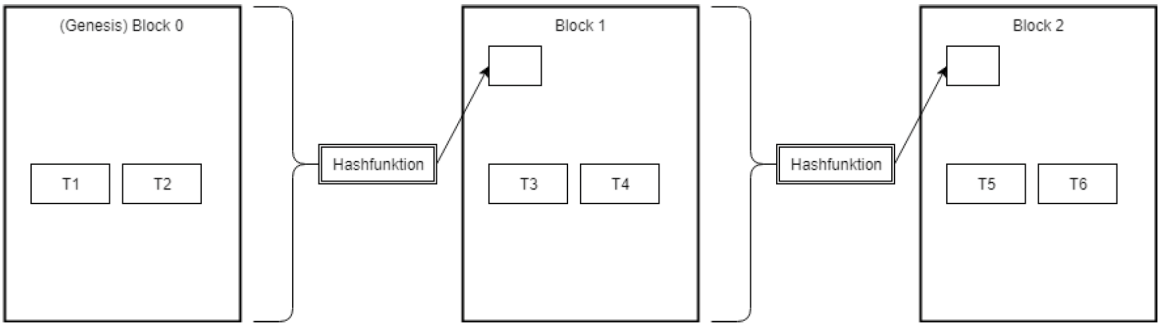

Abbildung 1 Funktionsweise der Blockchain

Zur Verknüpfung der Blöcke werden geeignete Hashing-Algorithmen[50] (zB SHA-256, SHA-512) verwendet, welche für beinahe beliebige Werte eine Zeichenfolge mit festgelegter Länge erzeugen und diversen Eigenschaften genügen müssen: So zeichnet diese Algorithmen insb aus, dass es einfach ist aus einem Wert seinen Hashwert zu erzeugen, die Umkehrfunktion ist aber praktisch unmöglich. Außerdem ist es praktisch unmöglich zwei Werte zu finden, die denselben Hashwert erzeugen. Selbst kleinste Änderungen des Ausgangswertes führen zu völlig anderen Hashwerten. Der berechnete Hashwert wird im Header des nachfolgenden Blocks gespeichert. Somit zieht jede nachträgliche Änderung (auch Löschung) einer Transaktion die Berechnung aller nachfolgenden Blöcke nach sich. Das Erzeugen neuer Blöcke (Mining) ist jedoch rechenintensiv, sodass eine Neuberechnung insb bei steigender Anzahl der nachfolgenden Transaktionen, aber auch bei steigender Anzahl an beteiligten Nodes immer schwerer durchführbar wird. Jede Transaktion ist damit dauerhaft nachvollziehbar und unveränderbar auf der Blockchain gespeichert; eine Manipulation von Daten durch Dritte ist praktisch ausgeschlossen.[51] Dies schafft Vertrauen in die Authentizität und Vollständigkeit der Daten.[52]

Blockchains können zunächst hinsichtlich der Verwaltung (dh nach den Akteuren, die neue Daten an die Blockchain anhängen dürfen) eingeteilt werden:

> Bei Permissionless Blockchains (zB Bitcoin), ist der Kreis der Teilnehmer nicht beschränkt; die datenverarbeitenden Nodes sind dadurch aber auch nicht notwendigerweise bekannt. Dagegen gewährleistet die Kontrolle durch zahlreiche, voneinander unabhängige Teilnehmer eine hohe Integrität.[53]
> Bei Permissioned Blockchains (zB Blockchain-Anwendungen durch kooperierende Unternehmen), ist die Teilnahme beschränkt und somit eine zentrale Stelle zur Verwaltung erforderlich. Daher ist idR immer ein Personenbezug feststellbar.[54]

Außerdem können Blockchains hinsichtlich des Zugangs eingeteilt werden (dh wer Zugriff auf das Netzwerk hat und zumindest Leserechte besitzt):

> Öffentliche (public) Blockchains, diese sind für jedermann einsehbar, damit ergibt sich hier auch eine besondere Datenschutzproblematik.
> Private Blockchains sind nur für bestimmte Personen einsehbar.

50 Vgl *(dt) Bundesamt für Sicherheit in der Informationstechnik*, BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen (2020) 41.

51 Vgl *Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.*, Blockchain und Datenschutz Faktenpapier (2017) 20.

52 Vgl *Erbguth*, Datenschutz auf öffentlichen Blockchains, Internationales Rechtsinformatik Symposion 2018.

53 Vgl *Schock*, Ausgewählte rechtliche Aspekte der Blockchain-Technologie in Raffling/Schock, Digitale Wirtschaft und Industrie 4.0. (2018) 165.

54 Vgl *Schock*, Rechtliche Aspekte (FN 53) 165.

Dabei ist in erster Linie an die Paarungen Public/Permissionless und Private/Permissioned zu denken, doch sind auch andere Kombinationen denkbar.

B. Blockchain im Lichte der DSGVO

In diesem Kapitel wird, wie oben geschildert, der Fall zugrunde gelegt, dass in der Blockchain personenbezogene Daten natürlicher Personen (konkret Energiedaten) verarbeitet werden und somit die DSGVO zur Anwendung gelangt. Es wird zunächst beurteilt, wer in der Blockchain als Verantwortlicher iSd DSGVO zu qualifizieren ist. Außerdem wird ausgeführt, wie die Verpflichtung des Verantwortlichen zur Einhaltung des Rechts auf Löschung mit dem Einsatz der unveränderlichen Blockchain in Einklang zu bringen ist.

1. Verantwortlicher in der Blockchain

IZm der Blockchain ist nicht von Vornherein eindeutig, wer der Verantwortliche ist. Es gibt viele verschiedene Akteure, die als solche in Frage kommen. Die konkrete Ausgestaltung der Blockchain ist entscheidend für die Beurteilung, wer tatsächlich als der für die Verarbeitung Verantwortliche zu qualifizieren ist. Daher kann keine allgemeingültige Aussage getroffen werden, sondern es muss eine Einzelfallprüfung durchgeführt werden.[55] In einer „public permissionless" Blockchain können ua der Softwareentwickler, die „Miner" und die „Nodes" als Verantwortliche für die Datenverarbeitung gelten. Im Folgenden wird kurz erläutert, welche dieser Akteure tatsächlich in Frage kommen und warum.

Auch wenn Software-Entwickler anderen Akteuren Software-Aktualisierungen vorschlagen, entscheiden sie idR nicht darüber, ob sie angenommen werden oder nicht. Da sie nur begrenzten Einfluss auf die Art und Weise der Verarbeitung haben, kommen Software-Entwickler eher nicht als für die Verarbeitung Verantwortliche in Frage.[56] Auch bei den Minern ist zu prüfen, inwieweit sie Einfluss auf die Bestimmung der „Zwecke und Mittel" der Verarbeitung haben. Miner profitieren finanziell von ihrer Beteiligung an dem verteilten Netzwerk.[57] Ihr Einfluss geht jedoch nicht über die Berechnung neuer Blöcke hinaus. Aufgrund der fehlenden Bestimmung des Zwecks bestimmter Transaktionen sind sie eher als „gehorsame Diener des Systems"[58] und nicht als Verantwortliche zu qualifizieren. Nach *Martini* und *Weinzierl* ist jeder einzelne Node, der eine Transaktion durchführt oder in einer eigenen Kopie der Blockchain speichert, als ein Verantwortlicher iSd DSGVO zu qualifizieren, da er damit die Teilnahme am Netzwerk bezweckt und frei über die auf seinem Node gesammelten und gespeicherten personenbezogenen Daten verfügt. Unter der Voraussetzung, dass die Zwecke und Mittel der Verarbeitung gemeinsam festgelegt werden, können mehrere Nodes grundsätzlich gemeinsam Verantwortliche gem Art 26 DSGVO sein.[59]

Bei privaten Blockchains ist es meistens einfacher, den für die Verarbeitung Verantwortlichen zu bestimmen, da sie idR so strukturiert sind, dass eine juristische Person bestimmt wird, in deren Zuständigkeit es liegt, die Mittel der Verarbeitung personenbezogener Daten und häufig auch die Zwecke zu bestimmen. Wenn die private Blockchain derart strukturiert ist, gilt diese bestimmte juristische Person als für die Verarbeitung Verantwortliche.[60]

Wie bereits oben ausgeführt, hat sich gezeigt, dass die Beurteilung des Verantwortlichen von der jeweiligen Konstellation abhängt und daher von Fall zu Fall zu beurteilen ist.[61] Dies gilt auch für Energiegemeinschaften. Es kann keine allgemeine Feststellung getroffen werden, dass der eine oder andere Akteur innerhalb einer Energiegemeinschaft verantwortlich wäre. Dennoch hat sich gezeigt, dass es Lösungsansätze gibt, die für die jeweilige Bewertung in Betracht gezogen werden sollten. Für Erneuerbare-Energie-Gemeinschaften zB ist die private Blockchain sicherlich eine Option, die aufgrund des in Art 2 Z 16 lit a EE-RL 2018 verankerten Nähekriteriums in Betracht gezogen werden kann. Ist diese wie oben skizziert strukturiert, ist die Identifizierung des für die Datenverarbeitung Verantwortlichen eher unproblematisch. Allerdings wird die Blockchain oft gerade wegen der Eigenschaften, die eine öffentliche Blockchain mit sich bringt gewählt. Diese sind im Falle der privaten Blockchain nur in eingeschränktem Maße gegeben. Bei der öffentlichen Blockchain ist die Einhaltung der vorgeschriebenen Datenschutzpflichten jedoch nicht ohne weiteres möglich, wie im folgenden Kapitel gezeigt wird.

2. Einhaltung des Rechts auf Löschung gem Art 17 DSGVO

Die Blockchain ist so konzipiert, dass sie nicht verändert werden kann. Gleichzeitig sind jedoch bei der Verarbeitung personenbezogener Daten in einer Blockchain die Grundsätze, die Rechte und die Pflichten iSd DSGVO einzuhalten, die ua eine Veränderung der Blockchain erforderlich machen. Konkret handelt es sich bspw um das bereits erläuterte „Recht auf Ver-

55 Vgl *Finck*, Blockchain (FN 32) 42.
56 Vgl *Finck*, Blockchain (FN 32) 45.
57 Vgl *Finck*, Blockchain (FN 32) 46.
58 *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1253).
59 Vgl *Martini/Weinzierl*, Blockchain-Technologie (FN 58) 1253 f.
60 Vgl *Finck*, Blockchain (FN 32) 44.
61 Vgl *Finck*, Blockchain (FN 32) 42.

gessenwerden", das der betroffenen Person das Recht auf Löschung personenbezogener Daten einräumt und somit ein Spannungsfeld zwischen dem Einsatz der unveränderlichen Blockchain und der Einhaltung dieses Rechts erzeugt. Um dennoch der Löschungspflicht nachzukommen, werden nun mögliche Lösungsansätze aufgezeigt.

Interessant ist in erster Linie die Tatsache, dass die DSGVO zwischen Löschung und Vernichtung[62] unterscheidet. Auch wenn die DSGVO keine Definition der Löschung enthält, kann allein aufgrund des Wortlautes (Löschung im Vergleich zur Vernichtung) argumentiert werden, dass nicht allzu hohe Anforderungen an die Löschung gestellt werden. Für eine Löschung scheint jedenfalls keine endgültige Vernichtung notwendig zu sein.[63] Es ist auch zu beachten, dass das Recht auf Löschung selbst nur den Begriff „Löschung" und nicht „Vernichtung" verwendet. Es wird jedoch auch gegenteilig argumentiert, dass der Begriff „Löschung" als gleichbedeutend mit „Vernichtung" anzusehen sei.[64] Eine Klarstellung hinsichtlich der anzuwendenden Interpretation wäre daher wünschenswert.

Außerdem werden, um dem Recht auf Löschung gerecht zu werden, folgende Optionen in der Literatur vertreten:

> Zero-Knowledge-Proof:[65] Bei diesem Verfahren werden Transaktionen nur in verschlüsselter Form durchgeführt, sodass eine Identifizierung der Teilnehmer nicht möglich ist. Dieses Verfahren liefert binäre Richtig/Falsch-Antworten, ohne Zugriff auf die zugrundeliegenden Daten zu gewähren. Die Transaktionen werden auf einer öffentlichen Blockchain veröffentlicht. Die Details der Transaktion wie Betrag, Quelle und Ziel bleiben jedoch vertraulich. Lediglich das Hauptbuch der Blockchain zeigt an, ob eine Transaktion ausgeführt wurde (aber nicht von welchem öffentlichen Schlüssel zu welchem öffentlichen Schlüssel).[66]
> Kombiniertes System: Die Verwendung einer Kombination aus Blockchain und einer traditionellen Datenbank ist eine weitere mögliche Lösung. Hierbei sind Zeiger (die erst unter Zuhilfenahme der traditionellen Datenbank eine Zuordnung der Datensätze zu betroffenen Personen ermöglichen) in der unveränderlichen Blockchain eingebettet, die mit veränderlichen Daten in der Datenbank verknüpft sind, sodass spätere Korrekturen und die Entfernung personenbezogener Daten möglich sind.[67]

V. Fazit

Die Energiewende erfordert vielfach „smarte" Lösungen, die wiederum große Mengen an Daten benötigen und verarbeiten. Energie(verbrauchs)daten sind personenbezogene Daten. Die Verarbeitung dieser unterliegt daher den Vorschriften der EU-weiten DSGVO, die ua zahlreiche Rechte zugunsten der betroffenen natürlichen Person und Pflichten seitens des Verantwortlichen implementiert. Dem Netzbetreiber kommt jedenfalls die Rolle des Verantwortlichen beim Einsatz von Smart Metern zu. Energielieferanten erhalten vom Netzbetreiber die erhobenen Verbrauchsdaten für Verrechnungszwecke sowie zum Zweck der Stromverbrauchsinformation; sie sind iHa diese Verarbeitungen Verantwortliche.

Die Blockchain-Technologie kann die technische Implementierung von Energiegemeinschaften erleichtern, steht jedoch im Spannungsverhältnis mit dem Datenschutz. Die Festlegung des für die Verarbeitung Verantwortlichen ist nicht ohne Weiteres möglich. Es hat sich gezeigt, dass für jeden einzelnen Anwendungsfall eine Fall-zu-Fall Beurteilung notwendig ist. Gleichwohl gibt es Grundsätze nach denen die Beurteilung durchzuführen ist. Insb die Löschung von Daten ist aufgrund der für die Blockchain wesensimmanenten Unveränderlichkeit nicht ohne Weiteres möglich. Es ist jedoch ein nicht allzu strenger Maßstab an die Löschung zu stellen und es existieren Möglichkeiten um dem sog „Recht auf Vergessenwerden" gerecht werden. Dennoch ist hervorzuheben, dass einer der Hauptvorteile der Blockchain deren Unveränderlichkeit ist, weshalb es aus Sicht der AutorInnen weitgehend vermieden werden sollte, personenbezogene Daten in einer Blockchain zu speichern. Die Verfügbarkeit von Daten und deren Verarbeitung gewinnt zunehmend an Bedeutung, weshalb die rechtlichen Vorgaben des Datenschutzes auch zukünftig eine wichtige Rolle spielen werden.

62 Vgl die Definition von „Verarbeitung" in Art 4 Z 2 DSGVO.
63 Vgl Datenschutzbehörde 05.12.2018, DSB-D123.270/0009-DSB/2018.
64 Vgl EuGH 20.12.2017, C-434/16, *Nowak/Data Protection Commissioner*, EU:C:2017:994, Rz 55.
65 Vgl *Harikrishnan/Lakshmy*, Secure Digital Service Payments using Zero Knowledge Proof in Distributed Network, International Conference on Advanced Computing & Communication Systems 2019, 307 (307 f).
66 Vgl *Finck*, Blockchain (FN 32) 32 f; *Martini/Weinzierl*, Blockchain-Technologie (FN 58) 1255 mwN; *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1431, 1435).
67 Vgl *Zyskind* et al, Decentralizing Privacy: Using Blockchain to Protect Personal Data, IEEE Security and Privacy Workshops 2015, 180 (180, 184).

VI. Acknowledgement

Die durchgeführte rechtliche Betrachtung ist eine themenspezifische Zusammenführung der Ergebnisse des Horizon 2020 Projekts PEAKapp (H2020-Nummer: 695945), und der FFG Forschungsprojekte „SonnWende+“ (Projektnummer: 861621), „SPC SuedBgld“ (Projektnummer: 858896), sowie des Forschungsprojekts „Industrial Microgrids“ (Projektnummer: 868708), das im Rahmen der vom Klima- und Energiefonds geförderten Vorzeigeregion „New Energy For Industry“ durchgeführt wird. Die ProjektpartnerInnen des Projekts Industrial Microgrids sind FH OÖ, AIT, Energiesparverband OÖ, TU Wien Energy Economics Group, Energieinstitut an der JKU, Amt der OÖ Landesregierung, E-Control Austria, Wels Strom GmbH, STIWA AMS GmbH, ABM automation building messaging GmbH, Ing. Aigner Wasser-Wärme-Umwelt GmbH, Rübig Technologie GmbH & Co KG, Fronius International GmbH, STARLIM Spritzguß GmbH, Format Werk GmbH, Gerstl Bau GmbH & Co KG, PBS Austria Papier Büro und Schreibwaren GmbH, Helios-Sonnenstrom-GmbH, Salesianer Miettex GmbH, Biomontan Produktions und Handels GmbH.

> MAG.ª ARGJENTA VESELI

Abteilung Energierecht, Energieinstitut an der Johannes Kepler Universität Linz, 4040 Linz, Altenbergerstraße 69.
E-Mail: veseli@energieinstitut-linz.at,
Web: www.energieinstitut-linz.at.

> MAG.ª MARIE-THERES HOLZLEITNER

Abteilung Energierecht, Energieinstitut an der Johannes Kepler Universität Linz, 4040 Linz, Altenbergerstraße 69.
E-Mail: holzleitner@energieinstitut-linz.at,
Web: www.energieinstitut-linz.at.

> DI MAG. STEPHAN CEJKA

Siemens AG Österreich, 1210 Wien, Siemensstraße 90.
E-Mail: stephan.cejka@siemens.com, Web: www.siemens.com.