VORSCHLÄGE FÜR DATENSCHUTZ UND PRIVATSPHÄRE BEI SMART METERN UND DEREN UMSETZUNG IM ÖSTERREICHISCHEN RECHT

Stephan Cejka

Research Scientist, Siemens AG, Corporate Technology, Research in Digitalization and Automation
Siemensstraße 90, 1210 Wien, AT
stephan.cejka@siemens.com, http://ct.siemens.com

Schlagworte: ***Smart Meter, Datenschutz, Privatsphäre***

Abstract: *Durch die Installation von intelligenten Messgeräten (Smart Meter) in den Haushalten kommen Verbraucher erstmals in Berührung mit den Veränderungen der Energieinfrastruktur und der Energiewende. Da bei den vorgesehenen kurzen Ausleseintervallen weitreichende Daten über das individuelle Benutzerverhalten und die Gesundheit des Verbrauchers aus dem Stromverbrauch eruiert werden können, ergeben sich Probleme in Bezug auf Privatsphäre und Datenschutz. Der Artikel zeigt mögliche Lösungsvorschläge auf und vergleicht diese mit der Umsetzung im österreichischen Recht.*

1. Einleitung

Die Energiewende führt zum Wandel von traditionellen zu intelligenten Stromnetzen (Smart Grids). Kleinkraftwerke, wie Photovoltaikanlagen, die in das Niederspannungsnetz einspeisen, führen zu einer Umstellung von einer zentralen zu einer dezentralen Energieversorgung [Ernst&Young 2013]. Die Intelligenz eines Smart Grids setzt die Übermittlung von zeitnahen Mess- und Kontrolldaten von Sensoren im Netz voraus. Diese inkludieren intelligente Messgeräte (Smart Meter), die damit für viele Verbraucher den ersten Berührungspunkt mit den Veränderungen der Energieinfrastruktur darstellen [Bernhardt 2014]. Dadurch sollen Kunden, Netzbetreibern und Stromlieferanten Daten zur Verfügung stehen, um das Netz besser stabilisieren zu können, erneuerbare Energien besser zu integrieren und die Abrechnung zu verbessern [Ernst&Young 2013]. Weltweit empfehlen oder zwingen staatliche Regulierungsbehörden oder gesetzliche Regelungen innerhalb des nächsten Jahrzehnts Smart Meter einzuführen [Budka et al. 2014]. Auch in den österreichischen Haushalten müssen bis 2019 95% der Kunden mit Smart Metern ausgestattet werden, die in kurzen Intervallen den aktuellen Energieverbrauch an den Netzbetreiber melden.

Der Artikel soll sich zentral mit konkreten Vorschlägen für die Sicherstellung von Datenschutz und Privatsphäre beschäftigen und diese mit der derzeitigen österreichischen Rechtslage vergleichen.

2. Österreichische Rechtslage inklusive europarechtlicher Vorgaben

Für die Einführung von intelligenten Zählern ist die RL 2009/72/EG maßgeblich, welche durch das Elektrizitätswirtschafts- und -organisationsgesetz 2010 (ElWOG 2010) umgesetzt wird. Zu erwähnen ist weiters die Empfehlung 2012/148/EU, die sich umfangreich, jedoch nicht rechtsverbindlich mit Datenschutz und Datensicherheit intelligenter Messsysteme beschäftigt. Eine Legaldefinition des Begriffs «intelligentes Messgerät» findet sich in § 7 Abs. 1 Z. 31 ElWOG 2010 als «*eine technische Einrichtung die den tatsächlichen Energieverbrauch und Nutzungszeitraum zeitnah misst, und die über eine fernauslesbare, bidirektionale Datenübertragung verfügt*». In der Definition der Z. 3 lit. b der Empfehlung 2012/48/EU wird darauf abgestellt, dass mehr Informationen als mit einem herkömmlichen Zähler bereitgestellt werden.

2.1. Grundrechte

Von Smart Metern gemessene Daten können einem Verbraucher eindeutig zugeordnet werden und sind damit personenbezogene Daten. Der Schutz personenbezogener Daten ist in der Verfassungsbestimmung des § 1 Abs. 1 DSG 2000 ausdrücklich als Grundrecht bezeichnet. In engem Zusammenhang steht das Grundrecht der Achtung des Privat- und Familienlebens in Art. 8 EMRK. Bedenken bezüglich eines Verstoßes gegen Art. 8 EMRK verzögerten die Einführung von Smart Metern in den Niederlanden um zwei Jahre [Cujipers/Koops 2013].

Bei Eingriffen in Grundrechte muss der Gesetzgeber das Verhältnismäßigkeitsprinzip wahren. Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen nicht verletzt werden. Diese sind dann nicht verletzt, wenn eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht. Solche ergeben sich aus dem ElWOG 2010 und den darauf basierenden Verordnungen.

Hornung und Fuchs beschäftigen sich mit der Frage, ob Smart Meter in das (deutsche) Grundrecht auf Unverletzlichkeit der Wohnung eingreifen [Hornung/Fuchs 2012]. Der (deutsche) BVerfG bestimmt 2004 in einem Urteil (BVerfGE 109, 279) zum «großen Lauschangriff» (akustische Wohnraumüberwachung), dass «*[d]er Schutzzweck der Grundrechtsnorm […] vereitelt [wäre], wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung […] umfasst wäre.*» Eine Entscheidung des Supreme Court of the United States von 2001 (Kyllo v. United States, 533 U.S. 27) zu einem Wärmebild eines Hauses besagt: «*In the home […] all details are intimate details, because the entire area is held safe from prying government eyes. […The] hour each night [that] the lady of the house takes her daily sauna and bath [is] a detail that many would consider ‹intimate›.*» Kapitel 3 wird zeigen, dass Smart Meter Daten noch mehr Details preisgeben.

2.2. Elektrizitätswirtschafts- und -organisationsgesetz 2010 (ElWOG 2010)

Die Einführung von intelligenten Zählern soll laut den ErwGr. der RL 2009/72/EG die Energieeffizienz fördern und Vorteile für Verbraucher bringen. Datenschutz wird dabei weder in den ErwGr., noch in den im Anhang normierten Maßnahmen zum Schutz der Kunden genannt. Die Umsetzung der Richtlinie erfolgt für den Strommarkt im Elektrizitätswirtschafts- und -organisationsgesetz 2010 (ElWOG 2010), welches als Reaktion auf Kritik von Branche und Datenschützern seit der Novelle 2013 auch umfassende datenschutzrechtliche Begleitregelungen enthält [Knyrim/Trieb 2013]. Die Einführung von Smart Metern wird insbesondere in der Intelligente Messgeräte-Einführungsverordnung (IME-VO) geregelt. Datenschutzrechtliche Anforderungen für Messgeräte und Kommunikation finden sich in der Intelligente Messgeräte-AnforderungsVO 2011 (IMA-VO) und der Datenformat- und VerbrauchsinformationsdarstellungsVO 2012 (DAVID-VO).

Neben den datenschutzrechtlichen Straf- und Verwaltungsstrafbestimmungen im DSG 2000 sieht das ElWOG 2010 darüberhinausgehende Bestimmungen vor: Wird in § 51 DSG 2000 in Bezug auf die widerrechtliche Offenbarung oder Verwertung von Daten noch eine Gewinn- oder Schädigungsabsicht verlangt, so ist in § 108 Abs. 1 ElWOG 2010 die Eignung berechtigte Interessen des Betroffenen zu verletzen ausreichend. Gemäß Abs. 2 leg.cit. kann die Öffentlichkeit in der Hauptverhandlung ausgeschlossen werden, sofern dies im Interesse der Verfahrensbeteiligten oder auch nicht-beteiligter Personen geboten ist. In § 99 ElWOG 2010 werden Verwaltungsübertretungen bestimmt. Zu nennen ist Abs. 3 Z. 1 leg.cit., wonach mit Geldstrafe bis zu 100‘000 Euro zu bestrafen ist, wer Daten widerrechtlich offenbart. Zusätzlich sind die Verwaltungsstrafbestimmungen in § 52 DSG 2000 einschlägig.

2.3. Ausgewählte weitere EU-Rechtsakte

Die Empfehlung 2012/148/EU beschäftigt sich zentral mit Datensicherheit und Informationspolitik bei der Einführung intelligenter Messsysteme. Die Kommission empfiehlt die Nutzung geeigneter Datenschutzzer-

tifizierungsverfahren, Datenschutzsiegel und -prüfzeichen, eine Informationspolitik in Bezug auf personenbezogene Daten der Kunden, deren Rechte, Kontaktdaten, Zweck der Datenverarbeitung und Speicherfrist. Zusätzliche Regelungen zu Smart Metern befinden sich auch in der Energieeffizienzrichtlinie 2012/27/EU.

3. Datenschutzproblematik

Smart Meter übermitteln den Stromverbrauch in viel häufigeren Intervallen an den Netzbetreiber als die Ablesung der elektromechanischen Ferraris-Zähler bisher erfolgt. Bisher waren der Jahresverbrauch und die durchschnittliche Verteilung des Stromverbrauchs über den Tag die einzigen Informationen, die Netzbetreiber und Lieferant bezüglich des voraussichtlich erforderlichen Strombedarfs hatten. Probleme in Bezug auf Privatsphäre und Datenschutz ergeben sich dahingehend, dass bei kurzen Ausleseintervallen weitreichende Daten über das individuelle Benutzerverhalten oder die Gesundheit aus dem benötigten Stromverbrauch eruiert werden können. Anhand charakteristischer Verbrauchskurven können Geräte im Haushalt identifiziert werden [Hart 1992] und dadurch genaue Profile über die Gewohnheiten des Verbrauchers gewonnen werden. Dadurch können aber auch illegale Tätigkeiten, wie z.B. über den charakteristischen Stromverbrauch von Lampen zur Cannabiszucht festgestellt werden [Mayer/Cukier 2013]. Je kürzer das Ausleseintervall festgelegt ist, desto mehr persönliche Daten können identifiziert werden und desto höher ist der Eingriff in die Privatsphäre des Kunden. Bei Ausleseintervallen von 0,5 Hz kann selbst das konsumierte TV-Programm festgestellt werden [Greveler et al. 2012]. Bei einer viertelstündlichen Auslesung lassen sich Backofen und andere Geräte aus der Kurve erkennen [Jeske 2011]. Höhere Zeitintervalle erlauben immerhin noch die Feststellung von Schlaf- und Abwesenheitszeiten. Informationen, die sich aus diesen Daten extrahieren lassen und potentiell Dritte interessieren könnten sind z.B.:

- Feststellung von Schlaf oder Abwesenheit bei potenziellen Einbruchsopfern
- Auswertung der Nutzung von Haushaltsgeräten für targeted advertising [Skopik 2012]
- Feststellung, ob der Arbeitnehmer während eines Krankenstandes tatsächlich zuhause war [Molina et al. 2010]
- Rechtzeitige Abfahrt des Arbeitnehmers zur Arbeit
- Gesundheitliche Probleme durch untypischen Verbrauch während der Nacht [Molina et al. 2010]
- Vereinbarungsgemäße Nutzung eines Mietobjekts [Renner 2011]

4. Sicherstellung von Privacy und die Umsetzung im österreichischen Recht

ErwGr. 5 der Empfehlung 2012/148/EU nennt das Finden von zweckmäßigen technischen und rechtlichen Lösungen für den Schutz personenbezogener Daten als eine der zentralen Aufgaben und Voraussetzungen für die Nutzung intelligenter Messsysteme. Aus der Sensibilität der Daten ergibt sich die notwendige Intensität datenschutzrechtlich gebotener Maßnahmen. Privacy by Design ist ein Konzept, bei dem datenschutzrechtliche Überlegungen von Beginn der Entwicklung an über den gesamten Lebenszyklus eines Produkts stehen und zentral in dieses eingebettet ist [Cavoukian et al. 2010] – in der Empfehlung als «konzeptionsbedingter Datenschutz» bezeichnet. ErwGr. 10 sieht den Einbau von Datenschutz- und Informationssicherheitsmerkmalen vor der Einführung und Nutzung vor. Der konzeptionsbedingte Datenschutz ist laut Z. 12 leg.cit. durch Rechtsvorschriften auf legislativer Ebene, durch geeignete Anforderungen auf technischer Ebene und auf organisatorischer Ebene umzusetzen. Nach den Mindestanforderungen an intelligente Messgeräte in § 3 Z. 12 IMA-VO haben diese den datenschutzrechtlichen Bestimmungen sowie dem anerkannten Stand der Technik zu entsprechen. Dieser ist nach den Erläuterungen zur IMA-VO «*der auf den einschlägigen wissenschaftlichen Erkenntnissen beruhende Entwicklungsstand fortschrittlicher technologischer Verfahren, Einrichtungen und Betriebsweisen, deren Funktionstüchtigkeit erprobt und erwiesen ist*» und wird durch international oder national anerkannte Normen, Standards, Guidelines u.Ä. definiert. Technische Sicherungen, wie das verschlüsselte

Senden von Daten zwischen Netzbetreiber und Smart Meter sind ein wichtiger Aspekt, jedoch nicht ausreichend zur Sicherstellung von Datenschutz und Datensicherheit [Skopik 2012].

Zur Lösung des Datenschutzproblems werden im Folgenden einige Vorschläge der Literatur vorgestellt. Teilweise werden diese auch in der o.g. Empfehlung angesprochen und haben Eingang in die österreichischen Rechtsnormen gefunden.

4.1. Datensicherheit, Technischer Datenschutz

Smart Meter und jegliche Kommunikation sind gegen unbefugtes Auslesen und Verändern abzusichern. Das Auslesen der Zähler kann durch geeignete mechanische Sperrmechanismen, das Aufstellung in Bereichen, die nur dem Vertragspartner zugänglich sind und softwaretechnische Sicherungsmaßnahmen (Authentifizierung) erfolgen [Renner 2011]. Unberechtigten darf der Zugang über den aktuellen Zählerstand hinaus nicht ermöglicht werden [Knyrim/Trieb 2013]. Daher ist nach § 83 Abs. 3 ElWOG 2010 am Zähler standardmäßig nur der aktuelle Zählerstand anzuzeigen. Gemäß Abs. 1 leg.cit. werden die erhobenen Daten 60 Tage im Zähler gespeichert, doch muss nach Abs. 4 leg.cit. sichergestellt werden, dass auch bei einem Mieterwechsel nicht auf Daten früherer Mieter zugegriffen werden kann.

Mit der Entwicklung zu Smart Grids geht notwendigerweise auch der Aufbau eines IKT-Systems zur Übertragung der Daten einher [Haberler et al. 2013]. Dies wirft Probleme auf, wie sie in anderen IKT-Systemen wie dem Internet bereits bekannt sind (z.B. Hacker). Da die Stromversorgung der Zukunft maßgeblich von diesem IKT-Netz abhängen wird, können Sicherheitsprobleme schwerwiegende Folgen haben. Der Stellenwert von Cyber Security im Energieversorgungsbereich wird dadurch steigen. Nachrichten zwischen dem Smart Meter des Endverbrauchers und dem Netzbetreiber dürfen nicht von Unberechtigten aus- bzw. mitgelesen werden. Dementsprechend sind laut § 3 Z. 7 IMA-VO intelligente Messgeräte und ihre Kommunikation nach dem anerkannten Stand der Technik abzusichern und zu verschlüsseln. Außerdem müssen Zugriffe auf Daten von Mitarbeitern der Netzbetreiber eingeschränkt und geloggt werden [Richter/Trieb 2016].

Ebenso sieht § 2 DAVID-VO für die Übermittlung von Daten durch den Netzbetreiber an den Lieferanten vor, dass diese nach dem Stand der Technik vor dem Zugriff Dritter geschützt ist, sowie die Übermittlung der Daten verschlüsselt zu erfolgen hat. § 3 Z. 11 IMA-VO fordert die Möglichkeit Softwareupdates aus der Ferne durchführen zu können. Da heutige kryptografische Verfahren durch die weitere Entwicklung in wenigen Jahren als nicht mehr sicher gelten könnten, ist es notwendig diese durch Softwareupdates aus der Ferne aktualisieren zu können [Khurana et al. 2010]. Daher soll eine gesetzlich normierte Vorgabe von Verschlüsselungsmethoden vermieden werden, da bei technischen Änderungen ansonsten keine Verpflichtung bestünde, die Systeme umzurüsten.

4.2. Datenminimierung, Minimale und lokale Datenspeicherung

Es soll nur das Minimum an personenbezogenen Daten erhoben werden, d.h. jene die für die Vertragserfüllung erforderlich sind. In diesem Zusammenhang ist insbesondere an eine seltenere Auslesung zu denken. Eine genaue Feststellung der Lebensgewohnheiten ist umso einfacher möglich, je höher das Ausleseintervall des Smart Meters ist. Der Netzbetreiber verliert durch die fehlende Verfügbarkeit realer zeitnaher Messdaten allerdings Informationen über den Netzstatus. Daher muss ein Kompromiss zwischen den Erfordernissen des Netzbetreibers und des Datenschutzes des Nutzers gefunden werden [Skopik 2012]. Einige Vorschläge verschieben auch die Durchführung der Abrechnung in die Sphäre des Verbrauchers (u.a. [Rial/Danezis 2011]). Damit wäre sichergestellt, dass keine privaten Daten den Haushalt verlassen.

Nach ErwGr. 13 der Empfehlung 2012/148/EU ist die Verarbeitung personenbezogener Daten auf das erforderliche Mindestmaß zu beschränken. Jede Verarbeitung personenbezogener Daten muss nach Z. 16 notwendig und angemessen sein. Daten sollen nach dem Grundsatz des § 6 Abs. 1 Z. 5 DSG 2000 nur solange gespeichert werden, wie diese für die Erreichung des Zweckes, für die sie ermittelt wurden, erforderlich sind. Eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen Vorschriften ergeben. So sieht § 81 Abs. 4

ElWOG 2010 eine Speicherung der Daten bis zu drei Jahren vor und geht damit wohl weit über die für die Abrechnung notwendige Dauer hinaus. Andererseits sieht § 84 Abs. 4 vor, dass der Kunde Daten im Web-Portal auch vor Ablauf dieser Zeit löschen kann.

Daten die nur lokal benötigt werden, sollen diese Ebene auch nicht verlassen. Werden beispielswese Daten nur für die Überwachung des Niederspannungsnetzes benötigt und ist eine intelligente Ortsnetzstation fähig auf auftretende Probleme im Ortsnetz autonom zu reagieren [vgl. Cejka et al. 2016], so ist eine Übertragung zu zentralen Datenbanken des Netzbetreibers nicht notwendig.

4.3. Opt-Out

Im datenschutzrechtlichen Optimalfall sollte jeder Verbraucher selbst entscheiden können, ob dieser ein Smart Meter installiert haben möchte oder auf die damit zusammenhängenden Vorteile wie dynamische Preise verzichten möchte (Opt-In). Dies ist in Österreich nicht möglich, da nach den festgelegten Prozentwerten in § 1 Abs. 1 Z. 2 und 3 IME-VO 70% der Kunden bis Ende 2017 und 95% bis Ende 2019 mit Smart Meter auszustatten sind.

In Österreich hat laut § 83 Abs. 1 ElWOG 2010 der Netzbetreiber die Ablehnung der Installation von Smart Metern durch den Kunden nur im Rahmen der Verordnung zu berücksichtigen (Opt-Out). Dem Wunsch ist nur dann zu entsprechen, wenn die Erreichung des maßgeblichen Prozentwertes trotzdem erreicht werden kann. Das Gesetz sieht damit laut einer parlamentarischen Anfrage (4994/J XXV.GP) keinen Rechtsanspruch auf die Ablehnung eines Smart-Meters vor. In diesem Sinne bezeichnen Knyrim/Trieb die «*oft falsch als ‹Opt-Out-Möglichkeit› […] bezeichnete Regelung*» als missglückt [Knyrim/Trieb 2013]. Diese sehen die Regelung auch im Lichte des verfassungsrechtlichen Gleichheitsgrundsatzes in Art. 7 B-VG als bedenklich. Durch die Fiskalgeltung der Grundrechte gelte dieser auch für die durch die öffentliche Hand betriebene Unternehmen mit Monopolstellung, somit auch für Netzbetreiber. Völlig unklar sei es auch, welche Regeln bei dem Neubezug einer Wohnung gelten, die bereits mit einem Smart Meter ausgestattet ist, doch der Neumieter den Smart Meter ablehnt [Knyrim/Trieb 2013].

In der Praxis werden derzeitige Zähler dennoch durch intelligente Zähler ausgetauscht und lediglich die Übertragung von 15-Minuten-Werten deaktiviert. Dies wird damit gerechtfertigt, dass damit die in § 7 Abs. 1 Z. 31 ElWOG 2010 geforderte zeitnahe Messung nicht mehr durchgeführt werde und dadurch kein intelligentes Messgerät mehr vorliege. Diese Praxis wird in einer parlamentarischen Anfrage (6234/J XXV.GP) kritisiert, da die dennoch durchgeführte Ablesung von Tageswerten ebenso eine zeitnahe Ablesung darstelle. Laut parlamentarischer Anfragebeantwortung (6033/AB XXV.GP) ist es die Entscheidung des Netzbetreibers, ob er den alten Ferraris-Zähler installiert lässt oder einen Zähler einbaut, der die Voraussetzungen des § 7 Abs. 1 Z. 31 bzw. der IMA-VO nicht erfüllt. Doch lässt sich bei Installation eines derartigen Geräts trotz Deaktivierung mancher Funktionen die Gefahr der illegalen Auslesung von Nutzungsdaten nicht völlig beseitigen.

4.4. Opt-In für hochfrequente Ablesungen

Da gemäß § 84 Abs. 1 ElWOG 2010 eine tägliche Verbrauchserfassung vorzunehmen ist, ist hierfür keine Zustimmung notwendig. Sollen Smart Meter Daten in einem häufigen Intervall (z.B. für die Nutzung dynamischer Tarife) ausgelesen werden, so soll dies nur durch ein explizites Opt-In des Verbrauchers erlaubt werden. Die österreichische Rechtslage sieht dies in § 84a Abs. 1 ElWOG 2010 vor. Demnach dürfen Viertelstundenwerte grundsätzlich nur mit ausdrücklicher Zustimmung des Endverbrauchers oder zur Erfüllung vertraglicher Pflichten, d.h. bei Nutzung eines auf Viertelstundenwerte basierenden Vertrags, ausgelesen werden. Daraus lässt sich noch nicht zwingend ablesen, dass Netzbetreiber auch verpflichtet wären einen Basistarif ohne Zeitbezug anzubieten. Jedoch ergibt sich dies wohl aus der Monopolstellung und dem in § 77 ElWOG 2010 normierten Recht auf Grundversorgung.

Ausleseintervalle sind gesetzlich oder regulatorisch spezifiziert, kürzere Intervalle sind jedoch technisch möglich und können jedenfalls für Anwendungsfälle im Haushalt, bei denen diese Daten die Sphäre des Kunden

nicht verlassen sollten, erforderlich sein (z.B. lokale «Smarte Applikationen», wie Smart Home Systems). Hierfür sollen jedenfalls alle Daten in kurzen Intervallen (denkbar sind auch Sekundenintervalle) verfügbar sein. Folglich sieht auch § 84 Abs. 5 vor, dass alle im Messgerät erfassten Daten in einem Intervall ausgegeben werden müssen, welches einen sinnvollen Betrieb von modernen Anwendungen des Endverbrauchers erlaubt.

4.5. Datenanonymisierung, Unverknüpfbarkeit

Nach ErwGr. 13 der Empfehlung 2012/148/EU sind nach Möglichkeit anonyme und pseudonymisierte Daten zu verwenden. Daten sollen gemäß ErwGr. 12 nicht zu einer bestimmten Person zurückverfolgt werden können. Der Netzbetreiber muss zwar um den Status des Netzes zu überwachen auf aktuelle Messwerte zugreifen können, jedoch ist nicht immer eine genaue Zuordnung zu einem Verbraucher notwendig [Efthymiou/Kalogridis 2010]. Anonymisierte Daten unterliegen nicht dem DSG 2000, sofern diese nicht mit vertretbaren Mitteln auf eine Person zurückführbar sind. Abrechnungsdaten müssen zwar einem Verbraucher zugeordnet werden können, doch ist es bei diesen Daten – zumindest bei der Nutzung traditioneller Tarife – nicht notwendig diese in einem hohen Zeitintervall zu übermitteln [Efthymiou/Kalogridis 2010].

Jeske stellt ein Protokoll vor, das viertelstündlich anonymisierte Werte an den Netzbetreiber sendet [Jeske 2011]. Dadurch ist eine Zuordnung zu einem Haushalt nicht mehr möglich. Derartig anonymisierte Datenpakete dürfen auch nicht miteinander in Beziehung gesetzt werden können. Dabei werden Verbrauchern bei jedem Sendevorgang zufällige Identifikationsnummern zugewiesen (Pseudonyme) [Cavoukian et al. 2010], wodurch die Daten auch untereinander nicht mehr verknüpfbar sind. Jeske nennt zusätzlich den Austausch der IP-Adresse bei jedem Sendevorgang als notwendig [Jeske 2011]. Dadurch kann bei zwei Datensätzen, die vom selben Smart Meter stammen, nicht mehr festgestellt werden, dass diese tatsächlich vom selben Verbraucher stammen.

4.6. Datenaggregation

Um den Status eines Netzes feststellen zu können ist es oftmals nicht notwendig die Daten von allen Haushalten zu überwachen. Oft genügt ein aggregierter Status von mehreren Messstellen, der nahe am Verbraucher z.B. in der Trafostation ermittelt werden kann. Beispiele sind der Minimal- und Maximalwert der Spannung bzw. die Summe der Leistungen oder des Stromflusses im Netz. Auch bei diesen aggregierten Werten gilt, dass diese datenschutzrechtlich nicht relevant sind, wenn diese nicht auf eine Person zurückführbar sind. Richter und Trieb verwenden hierfür einen Sensor (Grid Monitoring Device) im Hausanschlusskasten, dessen Werte verwendet werden, wenn an diesem ≥5 Haushalte angeschlossen sind [Richter/Trieb 2016].

4.7. Datensouveränität und Zweckbindung

Der Kunde soll – soweit anwendbar und möglich – entscheiden wofür seine Daten verwendet werden dürfen (Datensouveränität). Ein Zugriff auf Daten von Dritten darf nur im Rahmen einer Zustimmung bzw. bei aktiver Weitergabe durch den Kunden erfolgen. Daten sollen von Berechtigten nur zu definierten Zwecken verwendet, nicht mit Daten anderer Quellen verknüpft und nicht an Dritte weitergegeben werden. Dem entspricht der Grundsatz des § 6 Abs. 1 Z. 2 DSG 2000 wonach Daten «nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden» dürfen. Die Zwecke der Datenermittlung im ElWOG 2010 sind laut Renner Kundeninformation, Abrechnung und (unkonkret formuliert) Energieeffizienz [Renner 2011]. Gemeinte Bestimmung ist wohl § 84 Abs. 1 ElWOG 2010, welche zusätzlich auch Energiestatistik und der Aufrechterhaltung eines sicheren und effizienten Netzbetriebes nennt.

In Bezug auf Daten von Smart Metern ist vor allem sicherzustellen, dass diese Daten nicht an Vermieter, Versicherungen, Arbeitgeber, etc. weitergegeben werden. Zusätzlich normiert § 84a Abs. 5 ElWOG 2010 ein Beweisverwertungsverbot: Demnach ist die Verwendung der Daten in verwaltungsrechtlichen, verwaltungsgerichtlichen und zivilgerichtlichen Verfahren, soweit sich diese nicht auf das ElWOG beziehen, unzulässig;

mangels Aufzählung ist die Verwendung e contrario in strafgerichtlichen Verfahren zulässig [Knyrim/Trieb, 2013].

4.8. Verschleierung (Load-Hiding)

Im Unterschied zu den bisher erwähnten Methoden ist diese ausschließlich auf der Seite des Kunden zu implementieren. Hier wird versucht den Verbrauch durch Verfälschung der Lastkurve zu maskieren, z.B. durch die Nutzung von Energiespeichern [Kalogridis et al. 2010] oder E-Cars [Sun et al. 2015]. Diese werden strategisch geladen oder entladen um die nach außen ersichtliche Verbrauchskurve flach zu halten, sodass Anwesenheitsphasen oder verwendete Geräte nicht mehr festgestellt werden können [McLaughlin et al. 2011]. Die Batterie wird geladen, wenn der Momentanverbrauch unter einem festgelegten Wert liegt und entladen, wenn dieser höher ist. Dadurch ist es auch ohne Änderungen auf der Netzbetreiberseite unmöglich ein individuelles Kundenverhalten auszulesen. Der Gesamtverbrauch, der zur Abrechnung gelangt, bleibt hierbei unverändert [Skopik 2012]. Weitere Möglichkeiten sind das Hinzufügen von «Störungen» (Noises) zur Verbrauchskurve, z.B. durch zufälliges Ein- und Ausschalten von Geräten mit hohem Verbrauch wie Boilern [Egarter et al. 2014] oder die Beeinflussung der Einspeisung durch die Photovoltaikanlage [Reinhardt et al. 2015].

4.9. Datenkontrolle durch den Verbraucher

Da Smart Meter laut Richtlinie in erster Linie zu Verbraucherzwecken eingeführt werden, ist es notwendig den Verbraucher auch zeitnah die Kontrolle der Daten zu ermöglichen. ErwGr. 50 der RL 2009/72/EG nennt den Zugang zu objektiven und transparenten Verbrauchsdaten als zentralen Aspekt. § 3 DAVID-VO sieht vor, Verbrauchsdaten durch den Netzbetreiber mittels kundenfreundlicher Website zur Verfügung zu stellen und definiert Anforderungen an diese Website. Gemäß Z. 1 lit. c leg.cit. hat diese «in ihrer sicherheitstechnischen Ausgestaltung dem Stand der Technik zu entsprechen», sowie gemäß lit. d leg.cit. «in Bezug auf die Zugriffsrechte den datenschutzrechtlichen Bestimmungen zu entsprechen». Dies bedeutet damit wohl eine Authentifizierung des Verbrauchers am Web-Portal und die Verwendung einer gesicherten Verbindung. Direktzugriffe Dritter auf Daten des Web-Portals sind nicht möglich. In § 5 f DAVID-VO wird die Information des Endverbrauchers durch den Energielieferanten entsprechend § 81a Abs. 1 ElWOG geregelt und auf die datenschutzrechtlichen Regelungen in § 3 Z. 1 lit. c und d verwiesen.

5. Ergebnisse

Österreichische Umfragen zeigen, dass Konsumenten, die bereits mit Smart Metern ausgestattet wurden und die Vorteile nutzen können, diese überwiegend positiv sehen [Bernhardt 2014]. Kritisch seien hauptsächlich jene Kunden, die noch keinen Smart Meter zuhause haben. Die Mehrheit geht von generellen Energieeinsparungen aus, doch nur 34,7% erwarten diese für den eigenen Haushalt. 46,8% befürchten die Einführung des «gläsernen Menschen» und bemängeln fehlenden Datenschutz [Fredersdorf et al. 2015].

Skopik vergleicht Anonymisierung, Aggregation und Verschleierung miteinander und stellt fest, dass einige Vorteile von Smart Grids durch Umsetzung dieser Vorschläge nicht mehr oder nur noch eingeschränkt existieren [Skopik 2012]. Konkrete Abwägungen zwischen den Anforderungen des Netzbetreibers, der technologischen Umsetzung und der Privatsphäre der Kunden müssen im Auge behalten, dass zeitnahe Messungen zur Überwachung des Netzzustandes aus technischen Gründen notwendig sind.

6. Literatur

Bernhardt, Klaus, Smart Metering – ein «nicht» technischer Blickwinkel, e & i, 2014, S. 193–194.

Budka, Kenneth/Deshpande, Jayant/Thottan, Marina, Communication Networks for Smart Grids – Making Smart Grids Real, Springer, London 2014.

Cavoukian, Ann/Polonetsky, Jules/Wolf, Christopher, SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation, Identity in the Information Society, 2010, Heft 2, S. 275–294.

Cejka, Stephan/Hanzlik, Alexander/Plank. Andreas, A framework for communication and provisioning in an intelligent secondary substation, IEEE ETFA, 2016.

Cujipers, Colette/Koops Bert-Jaap, Smart metering and privacy in Europe: Lessons from the Dutch case. In: Gutwirth, Serge/Leenes, Ronald/de Hert, Paul/Poullet, Yves (Hrgs.), European data protection: Coming of age, Springer Netherlands, 2013, S. 269–293.

Efthymiou, Costas/Kalogridis, Georgios, Smart Grid privacy via anonymization of smart metering data, IEEE SmartGridComm, 2010, S. 238–243.

Egarter, Dominik/Prokop, Christoph/Elmenreich, Wilfried, Load hiding of household's power demand, IEEE SmartGridComm, 2014, S. 854–859.

Ernst&Young, Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler, 2013.

Fredersdorf, Frederic/Schwarzer, Judith/Engel, Dominik, Die Sicht der Endanwender im Smart Meter Datenschutz, Datenschutz und Datensicherheit, 2015, Heft 10, S. 682–686.

Greveler Ulrich/Glöseкötter, Peter/Justus, Benjamin/Loehr, Dennis, Multimedia Content Identification Through Smart Meter Power Usage Profiles, Computers, Privacy and Data Protection (CPDP), 2012.

Haberler, Berthold/Kienesberger, Georg/Kupzog, Friederich/Langer, Lucie, Smart-Grid-Architekturen in Österreich: Eine Bewertung der IKT-Sicherheitsaspekte relevanter Pilotprojekte, e & i, 2013, S. 115–120.

Hart, George, Nonintrusive Appliance Load Monitoring, Proceedings of the IEEE, 1992, Heft 80, S. 1870–1891.

Hornung, Gerrit/Fuchs, Katharina, Nutzerdaten im Smart Grid – zur Notwendigkeit einer differenzierten grundrechtlichen Bewertung, Datenschutz und Datensicherheit, 2012, Heft 1, S. 20–25.

Jeske, Tobias, Datenschutzfreundliches Smart Metering - Ein praktikables Lösungskonzept, Datenschutz und Datensicherheit, 2011, Heft 35, S. 530–534.

Kalogridis, Georgios/Efthymiou, Costas/Denic, Stojan/Lewis, Tim/Cepeda, Rafael, Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures, IEEE SmartGridComm, 2010, S. 232–237.

Khurana, Himanshu/Hadley, Mark/Lu, Ning/Frincke, Deborah, Smart-grid security issues, IEEE Security&Privacy, 2010, Heft 1, S. 81–85.

Knyrim, Rainer/Trieb, Gerald, Smart Metering NEU – die Änderungen durch die ElWOG-Novelle 2013, ecolex, 2013, Heft 12, S. 1123–1126.

Mayer-Schönberger, Viktor/Cukier, Kenneth, Big Data - Die Revolution, die unser Leben verändern wird, 1, Redline, München 2013.

McLaughlin, Stephan/McDaniel, Patrick/Aiello, William, Protecting consumer privacy from electric load monitoring, ACM CCS, 2011, S. 87–98.

Molina-markham, Andrés/Shenoy, Prashant/Fu, Kevin/Cecchet, Emmanuel/Irwin, David, Private memoirs of a smart meter, ACM BuildSys, 2010, S. 64–66.

Reinhardt, Andreas/Egarter, Dominik/Konstantinou Georgios/Christin, Delphine, Worried About Privacy? Let Your PV Converter Cover Your Electricity Consumption Fingerprints, IEEE SmartGridComm, 2015, S. 25–30.

Renner, Stephan, Smart Metering und Datenschutz in Österreich - Empfehlungen für die Einführung intelligenter Messgeräte, Datenschutz und Datensicherheit, Heft 35, S. 524–529.

Rial, Alfredo/Danezis, George, Privacy-Preserving Smart Metering, ACM WPES, 2011, S. 49–60.

Richter, Bernd/ Trieb, Gerald, Praxisprojekt Seestadt Aspern: datenschutzkonforme Forschung für die Energiezukunft, Datenschutz konkret, 2016, Heft 3, S. 52–55.

Skopik, Florian, Security Is Not Enough! On Privacy Challenges in Smart Grids, International Journal of Smart Grid and Clean Energy (IJSGCE), 2012, Heft 1, S. 7–14.

Sun, Yanan/Lampe, Lutz/Wong, Vincent, Combining electric vehicle and rechargeable battery for household load hiding, IEEE SmartGridComm, 2015, S. 611–616.