OBSOLETE VERSION

EINE ÜBERARBEITETE VERSION FINDET SICH UNTER:

http://compliance.zar.kit.edu/177_438.php

EMPFEHLUNGEN ZUM DATENSCHUTZ IM SMART GRID

Entwurf vom 14. Juni 2010

Oliver Raabe, Mieke Lorenz, Frank Pallas, Eva Weis

(Karlsruher Institut für Technologie, KIT)

INHALTSVERZEICHNIS

Vorwort 1

Einleitung 1

Teil I: Szenario „Widerspiegeln“ und dynamischer Echtzeittarif 5

Szenariodefinition 5

Personenbezug der Daten 5

Analyse 6

Handlungsbedarf 7

Rechtmäßigkeit 8

Analyse – Erheben Abrechnung 8

Handlungsbedarf 10

Analyse – Übermittlung 11

Analyse – Widerspiegeln des Stromverbrauchs 12

Handlungsempfehlung 15

Analyse – Drittstaatenübermittlung 16

Zweckbindung 17

Analyse 17

Handlungsbedarf 19

Erforderlichkeit 20

Analyse 21

Datensparsamkeit 22

Analyse 23

Handlungsbedarf 25

Transparenz 28

Analyse 29

Handlungsbedarf 29

Datensicherheit 31

Analyse 31
Handlungsbedarf 33
Nutzerrechte 38
Analyse 38
Handlungsbedarf 39
Kontrolle 39
Analyse 40
Handlungsbedarf 40
Teil II: Szenario Elektromobilität 42
Personenbezug der Daten 45
Analyse 45
Handlungsbedarf 46
Rechtmäßigkeit 46
Analyse – Erheben der Daten 47
Handlungsbedarf 48
Analyse – Rechtmäßigkeit der Datenerhebung 48
Handlungsbedarf 49
Analyse – weitere datenschutzrelevante Vorgänge (Messdaten) 50
Handlungsbedarf 50
Analyse – Fahrzeugzustandsinformationen 51
Zweckbindung 51
Analyse 51
Erforderlichkeit 52
Analyse 52
Handlungsbedarf 53
Datensparsamkeit 53
Analyse 54
Handlungsbedarf 54

Nutzerrechte 56
Analyse 56
Handlungsbedarf 57
Transparenz 57
Analyse 57
Handlungsbedarf 58
Teil III : Regulierungstheoretische Fragen 58
Bereichsspezifische Regelung 59
Regulierungsinstrumente 60
Ordnungsrecht 61
Kooperative Verfahren 61
Fazit 62
Literatur 64

VORWORT

Der vorliegende Entwurf von Empfehlungen ist im Rahmen der Begleitforschung des Förderprogramms des Bundesministeriums für Wirtschaft und Technologie, „E-Energy - IKT-basiertes Energiesystem der Zukunft", entstanden. Die Autoren danken Kay Diedrich, Alfred Malina und Katharina Vera Boesche für ihre Mitwirkung und Jonas Fluhr, Oliver Franz, Knut Schmelzer, Patrick Breyer, Mathias Reinis, Rolf-Dieter Kasper und Holm Diening für die konstruktiven Anmerkungen zum Entwurf.

EINLEITUNG

Im Jahr 2007 hat die Europäische Kommission ein integriertes Paket von Rechtsvorschriften zum Thema Energie/Klimawandel vorgelegt, das in der 10-Jahres Perspektive auf die Themen Energieversorgung, Klimawandel und industrielle Entwicklung eingeht. Im Ergebnis ist hiernach eine 20-prozentige Steigerung der Energieeffizienz, eine 20-prozentige Verringerung der Treibhausgasemissionen und ein Zielwert von 20 % für den Anteil erneuerbarer Energiequellen am Gesamtenergieverbrauch der EU im Jahr 2020 vorgesehen. Zudem finden sich mit der Richtlinie zur - Endenergieeffizienz und Energiedienstleistungen auch schon kurzfristig wirkende Maßnahmen im Prozess der Umsetzung in nationales Recht, die das Thema Energie nicht mehr nur unter dem Aspekt der Gewährleistung des binnenmarktrelevanten ökonomischen Wettbewerbs adressieren. Aus globaler Sicht geht es bei den insofern vorgesehenen Maßnahmen um die Steigerung der Energieeffizienz durch die Nutzung einer Kommunikationsinfrastruktur zum Echtzeit-Informationsaustausch zwischen Akteuren des Energiemarktes. Man kann sich dieses Paradigma auch durch die Substitution von verlustbehafteten, weil unscharf prognostizierten, realen Stromflüssen durch Informationsflüsse verbildlichen. Hierdurch soll ermöglicht werden, dass Angebot und Nachfrage zeitnah und hochauflösend aufeinander abgestimmt werden. In einem ersten Schritt werden deshalb auf gesetzlicher Grundlage des § 21b Abs. 3a EnWG ab 2010 schrittweise bei Neubauten und bei Renovierungen von Gebäuden nur noch solche Energiezähler eingebaut werden,[1] die den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit zeigen. In der Folge werden diese Zähler durch die Anbindung an die IKT-Infrastrukturen u. a. des Internets auch zur Weitergabe der Messdaten an Mehrwertdienste im Internet genutzt werden können. Die insofern datenschutzrelevanten Gefahrenlagen des Einsatzes von Smart Meter[2] hat das ULD Schleswig-Holstein jüngst in einem Gutachten dargelegt.[3]

[1] Allerdings soll nach dem Gutachten der BNetzA eine sinnvolle Entscheidung über die Ausbauziele erst nach einer umfänglichen Kosten-Nutzen-Analyse möglich sein, die unter Ausnutzung der zeitlichen Spielräume des 3. RL-Pakets für frühestens 2011 ins Auge zu fassen sei. Vgl. BNetzA, Bericht - Wettbewerbliche Entwicklungen und Handlungsoptionen im Bereich Zähl- und Messewesen und bei variablen Tarifen, S. 94.

[2] Unter Smart Meter wird im Folgenden der Einsatz von EDL-40 Systemen verstanden, siehe hierzu Ecofys u.A. Ökonomische und technische Aspekte eines flächendeckenden Rollouts intelligenter Zähler, 2009, S. 22 ff, http://www.bundesnetzagentur.de/cae/servlet/contentblob/153300/publicationFile/6482/EcofysFlaechendeckenderRollout19042010pdf.pdf [12.05.2010].

[3] Vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein (ULD-SH), Datenschutzrechtliche Bewertung des Einsatzes von Intelligenten Messeinrichtungen für die Messung gelieferter Energie (Smart Meter), 2010, https://www.datenschutzzentrum.de/ smartmeter/20090925-smartmeter.pdf [10.05.2010].

Die nicht so ferne Zukunft der angestrebten Energieeffizienzsteigerungen wird durch ein intelligentes Stromnetz, das sog. Smart Grid, gekennzeichnet sein, welches neben der Erfassung der relevanten Parameter des Netzzustandes an allen Stellen der Topologie, insbesondere auch bidirektionale Datenkommunikation zur Steuerung von Lasten erlauben und den Anforderungen für einen hochkomplexen Netzbetrieb genügen.

Dabei liegen z.B. die Potentiale zur Verbesserung des Klimaschutzes durch die Integration von Elektromobilität in den Energiemarkt auf der Hand, wenn man neben der besseren CO_2-Bilanz der klassischen Elektromobilitätsszenarien auch noch den Einsatz im Bereich der Minutenreserve in die Betrachtung einbezieht. Eines der wesentlichen Probleme bei der Verwendung von unsteten regenerativen Energieerzeugungsanlagen wie der Windkraft liegt in dem Bedarf an (konventionellen) Reservekapazitäten. Durch die Nutzung der Batteriespeicher von Elektromobilen zur Aufnahme von Überkapazitäten und Einspeisung bei Lieferengpässen lassen sich diese Nachteile verringern – im Hinblick z.B. auf den Ausbau von Offshore-Windparks ein sicher entscheidendes Argument für die Marktfähigkeit dieser Planungen. Daneben können auf Basis feingranular aufgelöster Sensordaten zukünftig auch neue Geschäftsfelder der internetbasierten Energieeffizienzberatung ermöglicht werden, die bis hin zum Steuern von Haushaltsgeräten reichen.

Aus rechtlicher Perspektive ist in Bezug auf die auf Informations- und Kommunikationstechnik (IKT) basierende informatorische Vernetzung der Akteure des Energiemarktes in diesem Zusammenhang ein doppelter Paradigmenwechsel zu konstatieren. Einerseits ein Wechsel von einem geschlossenen Markt mit energiewirtschaftsrechtlich klar definierten Rollen, Akteuren und Prozessen zu einem offenen Markt, der unter dem Gesichtspunkt von energieeffizienzsteigernden Maßnahmen zukünftig auch Kleinanbieter, Kooperationen von Nachfragern und Anbietern und den schnellen Rollenwechsel im Rahmen der Integration dezentraler Erzeugung und Speicherung aufnehmen muss. Auf der anderen Seite bedingt ein intelligentes Energiemanagement zur Unterstützung von Prozessen der Virtualisierung und ggf. Selbstorganisation eine Abkehr von den bislang dominierenden offline-Geschäftsprozessen zu einer vollständigen IKT-Basierung aller Kommunikation und der jedenfalls teilweisen Lösung von der Orientierung an der Netztopologie. Damit treffen IKT-spezifische Sachmaterien, wie das Paradigma des „Internets der Dinge“ oder des „Internets der Dienste“, aber auch IT-Substitute von vormaligen offline-Prozessen, wie die eichrechtliche Nachvollziehbarkeit von Abrechnungen, auf das klassisch geprägte Prozessmodell des Energiesystems. In beiden Perspektiven muss damit auch eine Integrationsleistung für bestehende und neuartige Regulierungsanforderungen erbracht werden, die sich in besonderem Maße im datenschutzrechtlichen Kontext kumuliert.

Eine datenschutzrechtliche Herausforderung ist die Auflösung der klaren Prozess-, Akteurs- und Rollenstruktur des klassischen Energiemarktes, die sonst, vergleichbar dem Telekommunikationsmarkt, eine ideale Grundlage für ordnungsrechtlich strukturierende bereichsspezifische Vorgaben zum Datenschutz im Energiesystem gewesen wäre. Auf der anderen Seite sind die bestehenden Regelungen des IKT-Datenschutzrechts vielfältig nicht auf die spezifischen Herausforderungen des zukünftigen Smart Grid wie Maschine-Maschine-Kommunikation und Flexibilität durch Medienbruchfreiheit von Transaktionen angelegt und bedürfen einer Untersuchung, angepassten Integration oder Revision.

Als wesentliche datenschutzrechtliche Herausforderung für das Smart Grid erweist sich der Umstand, dass in die normativen Überlegungen zur Abwägung konkurrierender Belange nicht wie in den üblichen Sachgestaltungen des Datenschutzes im nichtöffentlichen Bereich lediglich die

Verbürgungen und Notwendigkeiten wirtschaftlicher Betätigung als konkurrierendes Schutzgut einzustellen sind.

> Bei der rechtlichen Gestaltung des normativen Datenschutzkonzeptes für das Smart Grid ist das Spannungsfeld vom Schutz der informationellen Selbstbestimmung und einer Grundbedingung menschlichen Lebens, dem Klimaschutz, durch Steigerung von Energieeffizienz bei gleichzeitiger Innovationsoffenheit und Rechtssicherheit, in Ausgleich zu bringen.

Im internationalen Umfeld fehlt es im Hinblick auf diese Herausforderungen an rechtsvergleichend zu betrachtenden Normierungsaktivitäten. In den USA wurde jüngst für die korrespondierenden datenschutzrechtlichen Problemlagen des Smart Grid der Begriff „Smart Privacy“[4] eingeführt, allerdings motiviert die diesbezügliche Studie wegen des visionären Charakters des Smart Grid eher noch das Gefahrenpotential und beschränkt sich im Wesentlichen auf datenschutzrechtliche Allgemeinplätze. Daneben finden sich schon vereinzelte Literaturstimmen[5], Gutachten[6] und Stellungnahmen der Datenschutzbehörden zu datenschutzrechtlichen Teilaspekten des Smart Grid.

Den vorgenannten Betrachtungen ist allerdings gemein, dass die zur rechtlichen Bewertung notwendigen Tatsachengrundlagen eine nur so unvollständige Hypothesenbildung über die möglichen Einsatzzwecke und Ziele des Smart Grid zulassen, dass konkrete rechtliche Schlussfolgerungen regelmäßig der Komplexität und den zu erwartenden Wechselwirkungen in der konkurrierenden Zielkonstellation Klimaschutz/Energieeffizienz, Innovationsoffenheit und Grundrechtsschutz zum gegenwärtigen Zeitpunkt nicht hinreichend gerecht werden können. Konkretere Grundlagen ließen sich beispielsweise durch eine an die DKE-Normungsroadmap für das Smart Grid[7] angelehnte Formalisierung von Referenzszenarien beziehungsweise Anwendungsfällen schaffen. Insofern kann vor die Klammer gezogen schon einleitend eine erste Empfehlung ausgesprochen werden:

> Es sollte nach dem Vorbild der DKE-Normungsroadmap für das Smart Grid ein formaler Rahmen für die Sammlung von Anwendungsfällen (UseCases) etabliert werden. In datenschutzrechtlicher Perspektive sind hier insbesondere die Akteure/Rollen im Energiemarkt, Informationsflüsse, Erforderlichkeit und Zwecke der Verarbeitung von Energieinformationen in einem einheitlichen Format zu modellieren.

---

[4] The Future of Privacy Forum, Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation, 2009, http://www.futureofprivacy.org/wp-content/uploads/2009/11/smartprivacy-for-the-smart-grid.pdf [12.05.2010].

[5] Göge/Boers, ZNER 2009, 368 ff.

[6] Roßnagel/Jandt, Datenschutzfragen eines Energieinformationsnetzes, Rechtsgutachten im Auftrag der Alcatel-Lucent-Stiftung für Kommunikationsforschung, Kassel, Stand 26. März 2010

[7] DKE, Die deutsche Normungsroadmap E-Energy / Smart Grid, 2010, Online unter http://www.dke.de/KoEn [12.05.2010].

Vor diesem Hintergrund haben die beitragenden Modellregionen der E-Energy- und Elektromobilitätsmodellprojekte in diesen Empfehlungen den Versuch unternommen, anhand zweier generischer Modellszenarien einerseits das wesentliche Vorbringen aus vorhandenen Stellungnahmen und Literaturbeiträgen und auf der anderen Seite auch eigene Betrachtungen im Rahmen der Projektarbeiten zu konsolidieren. Dabei werden datenschutzrechtliche Fragen, die sich aus der Forschungsperspektive der Modellregionen ergeben, insofern nicht vertieft betrachtet, als es vornehmlich um erste Ansätze zum künftigen gesetzlichen Normierungsrahmen und um Impulse für die Markt- und Technikentwicklung durch die beteiligten Akteure gehen soll.

Die gewählten Referenzszenarien orientieren sich einerseits an den bereits gesetzlich terminierten Herausforderungen, die aus der Integration der Smart Meter in das Energiesystem entstehen, und im zweiten Schritt an den besonderen Herausforderungen, die aus der Integration von Elektromobilität erwachsen können. Schließlich werden im dritten Teil grundlegende regulierungstheoretische Überlegungen zur Effektivierung des Datenschutzes im Smart Grid angestellt. Wegen der notwendigen Integration der neuen Architekturen in den bestehenden energiewirtschaftsrechtlichen Rahmen werden die diesbezüglich bestehenden Vorgaben der BNetzA zu den Geschäftsprozessen weitestgehend zugrunde gelegt.[8]

Die Darstellung orientiert sich dabei wegen ihres Querschnittscharakters, dem heterogenen Empfängerkreis und im Bemühen um szenariospezifische Vollständigkeit an den so genannten „7 goldenen Regeln des Datenschutzes“.[9] Der Bestand insbesondere verfahrensrechtlich wirkender Normierungen des BDSG, wie die Funktion des betrieblichen Datenschutzbeauftragten oder das Führen von Verfahrensverzeichnissen werden insofern nicht ausführlich diskutiert. Wegen der grundsätzlichen Dimensionen der Notwendigkeit der Modernisierung des Datenschutzrechts wird insbesondere auf das nach wie vor aktuelle Modernisierungsgutachten[10] verwiesen.

[8] Vgl. zum aktuellen Stand die Prozessdefinitionen der BNetzA in den Konsultationen zum Festlegungsverfahren zur Standardisierung von Verträgen und Geschäftsprozessen im Bereich des Messwesens, BK6-09-034 / BK7-09-001, Messstellenbetreiber- und Messdienstleisterprozesse bei Strom und Gas, Stand: 23.02.2009, Online über http://www.bundesnetzagentur.de [10.05.2010].

[9] Bizer, DuD 2007, 350 ff.

[10] Roßnagel/Pfitzmann/Garstka; Zu den Grenzen des bestehenden normativen Schutzkonzeptes im Hinblick auf schon jetzt absehbare Entwicklungen siehe auch Roßnagel, Datenschutz in einem informatisierten Alltag, S. 127 ff.

TEIL I: SZENARIO„WIDERSPIEGELN“ UND DYNAMISCHER ECHTZEITTARIF

SZENARIODEFINITION

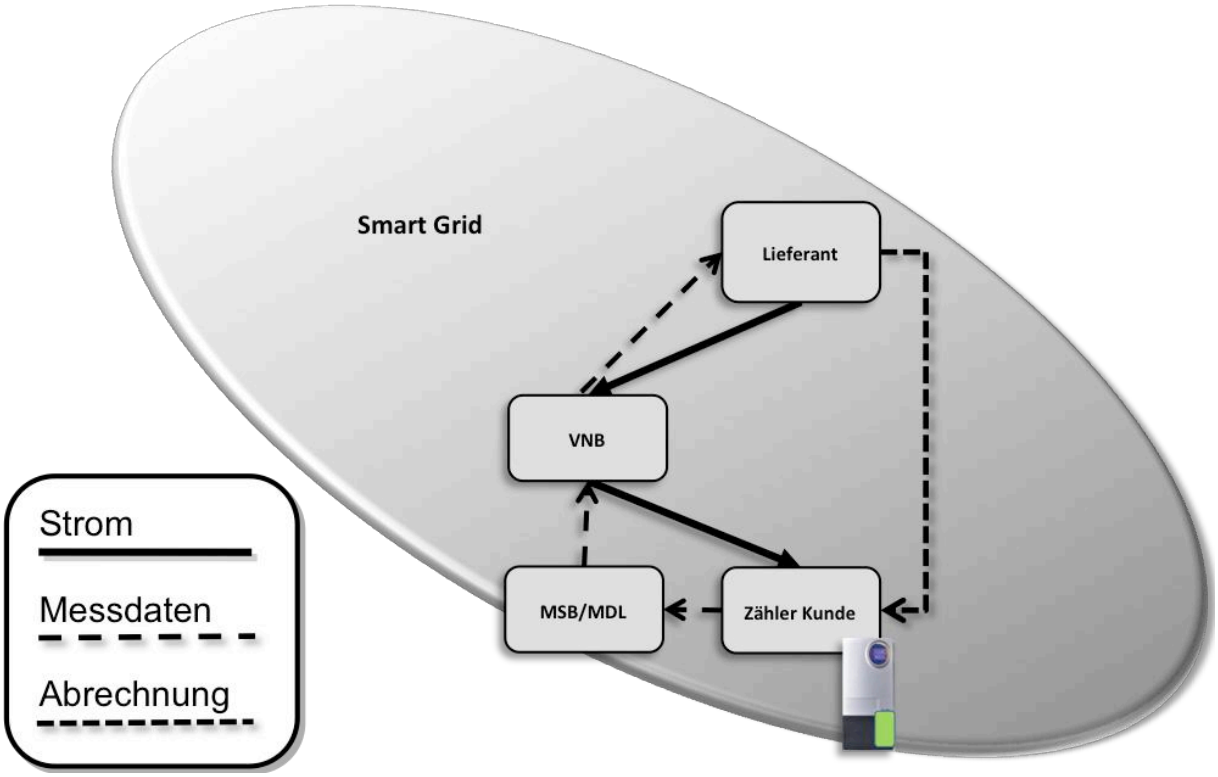

Abbildung 1: Messung zur Abrechnung

Im ersten Referenzszenario soll zugrunde gelegt werden, dass bei einem Anschlussnutzer im Energiesystem der Stromverbrauch mittels Smart Meter sowohl in klassischen Ableseintervallen, als auch bei Nutzung lastvariabler und tageszeitabhängiger Tarife abgerechnet werden soll. Hinsichtlich der Rollen und Informationsflüsse wird zu Zwecken der Illustration insofern auf jene Prozessfestlegungen der BNetzA[11] abgestellt, die eine größtmögliche Differenzierung der Rollen und Informationsflüsse erlauben[12] und mithin die aus der Perspektive des Datenschutzes die größtmögliche Gefahranlage in sich bergen.

PERSONENBEZUG DER DATEN

Das Datenschutzrecht schützt als einfachgesetzliche Ausgestaltung des Rechts auf Informationelle Selbstbestimmung die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.[13] Da das Recht auf Informationelle

[11] Vgl. Prozessdefinitionen der BNetzA in den Konsultationen BK6-09-034 / BK7-09-001, Messstellenbetreiber- und Messdienstleisterprozesse bei Strom und Gas, S. 122 ff.

[12] Dabei soll nicht verkannt werden, dass dies nicht der derzeitigen Praxis entspricht, in der die Rollen MSB/MDL regelmäßig mit dem VNB zusammenfallen.

[13] BVerfGE 65, 1, 43.

Selbstbestimmung nur natürliche Personen vor der Preisgabe ihrer Daten schützt, gilt das Datenschutzrecht nur für personenbezogene Daten. Klärungsbedarf besteht daher zunächst hinsichtlich der Frage, ob die im Smart Grid verwendeten Daten einen Personenbezug aufweisen, wobei auch auf die Veränderungen durch den Einsatz des Smart Meters und die dadurch geschaffenen Gefährdungslagen eingegangen wird.

ANALYSE

Grundsätzlich handelt es sich bei den Messdaten zur Abrechnung des Stromverbrauchs um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, dem Betroffenen, und somit um personenbezogenen Daten i. S. d. § 1 Abs. 2 i.V.m. § 3 Abs. 1BDSG.

Betrachtete man den bisherigen Zähler und die damit verbundenen jährlichen Ableseintervalle für eine ebenfalls jährliche Rechnungsstellung, so hatte man es bislang mit wenigen Daten zu tun. Diese boten zudem keine Möglichkeit der Erstellung von besonders sensiblen Personen- und Verhaltensprofilen, da aus dem jährlichen Energieverbrauch kaum Rückschlüsse auf Lebensgewohnheiten der Betroffenen gezogen werden können. Zudem findet bislang keine Fernübermittlung der Daten statt. In aller Regel wird turnusmäßig einmal im Jahr durch einen Mitarbeiter des Verteilnetzbetreibers der Zählerstand abgelesen, ergänzend und in einigen Fällen alternativ besteht die Option der Selbstablesung und Einsendung des Zählerstands per Postkartedirekt an den Stromlieferanten, der Übermittlung des Zählerstands via Internet usw. sowie dem Einsatz dritter Dienstleistungsunternehmen (Auftragsdatenverarbeitung).

Den Meseberger Beschlüssen kann entnommen werden, dass die Bundesregierung den Rollout der modernen Smart Meter,[14] welche einen Teil des sogenannten Smart Grid, einem komplexen Energieinformationsnetz, darstellen, befürwortet, was zur einer grundlegenden Änderung der bisherigen Praxis geführt hätte. Inzwischen ist aber zu erwarten, dass nicht zuletzt der Bericht der BNetzA zum Messwesen für eine gewisse Entschleunigung zumindest des flächendeckenden Einbaus reiner Smart Meter sorgen wird. Er hat aber auch klar aufgezeigt, dass gerade systemische Ansätze wie sie in den E-Energy Modellregionen entwickelt werden, die von einem intelligenten Gesamtsystem (Internet der Energie) ausgehen und es nicht bei einem Zählerwechsel bewenden lassen, ein guter Weg sein können, die Zukunft insbesondere mit Blick auf die Ziele Klimaschutz (CO_2-Einsparung, höhere und integrierte Einspeisung Erneuerbarer Energien), Lastmanagement, Preissignale und -transparenz sinnvoll zu gestalten.

Dies bringt folgende Wandlungen mit sich: Einerseits werden eine Vielzahl neuer Akteure die Daten benötigen – beispielsweisegänzlich neue Marktteilnehmer wie (Energieeffizienz-) Optimierungsdienste für den Verbraucher. Andererseits wird, bedingt durch die dann mögliche (nicht zwingende)

[14] Vgl. Gesetzesentwurf der Bundesregierung, BT-Drs. 16/8306, S. 7 sowie den Bericht der Bundesnetzagentur, Wettbewerbliche Entwicklungen und Handlungsoptionen im Bereich Zähl- und Messwesen und bei variablen Tarifen, 2010, S. 17, http://www.bundesnetzagentur.de/cae/servlet/contentblob/151968/publicationFile/6321/BerichtZaehlMesswesenpdf.pdf [10.05.2010].

viertelstündlich erfolgende Aufzeichnung der Messwerte[15] im Smart Meter, die Menge der Daten und damit das Datenvolumen in ganz erheblichem Maße steigen. Die Funktion einer viertelstündlichen Erfassung der Messwerte müssen Smart Meter im Fall einer vom Kunden gewünschten feingranularen Tarifierung in jedem Fall erfüllen, da sich nur mit einem solchen Zähler die Möglichkeit des Angebots derartiger dynamischer lastvariabler oder tageszeitabhängiger Tarife nach § 40 Abs. 3 EnWG umsetzen lässt. Ein so genannter Standardlastprofilkunde i. S. d. § 12 StromNZV kann nach § 10 Abs. 3 MessZV die Erfassung seines Elektrizitätsverbrauches in 15-minütigen Abständen verlangen, wenn er dies mit dem Messstellenbetreiber vereinbart hat.[16] Technisch grundsätzlich möglich ist jedoch auch die Erfassung des Stromverbrauchs in Quasi-Echtzeit und damit sekundengenau. Zur Verdeutlichung des datenschutzrechtlichen Gefährdungspotentials der Nutzung des Smart Grid wird folgender Vergleich angestellt:[17] Wo bisher einmal im Jahr eine Gesamtverbrauchsangabe erfolgte, fallen künftig bei einer Verbrauchsmessung in Intervallen von 15 Minuten pro Jahr an den Zählpunkten 35.040 Messwerte an. Das Ganze gewinnt an Komplexität, sofern man auch einen Blick auf das sogenannte Smart Home wirft. Hier soll der Zähler sogar den Verbrauch gerätespezifisch erfassen, sodass eine Aufschlüsselung des Verbrauchs einzelner Geräte möglich wird, mit dem Ziel die letztgenannten auch zu steuern, um günstige Tarife optimal auszunutzen. Des Weiteren wird den Daten eine stark erhöhte Aussagekraft zugeschrieben, sodass sie unmittelbar großes Interesse Dritter auf sich ziehen werden. Nimmt man also in den Blick, dass ein Großteil der Handlungen eines Menschen heute Strom benötigt, so geben die oben beschriebenen Daten ein ziemlich genaues Bild von den täglichen Beschäftigungen der in einem Haushalt lebenden stromverbrauchenden Personen. Selbst wenn man den reinen Energiemessdaten aus dem Zähler noch keinen Personenbezug zuschreiben möchte, sind diese jedoch, sobald sie mit den bei den jeweiligen Vertragspartnern wie dem Lieferanten und dem Messstellenbetreiber bzw. Messdienstleister[18] vorhandenen Stammdaten verknüpft werden, als personenbezogene Daten für diese Akteure des Energiesektors einzuordnen.

HANDLUNGSBEDARF

Im Hinblick auf den Wandel des datenschutzrechtlich relevanten Personenbezuges und der Aussagekraft von Messdaten im zukünftigen Smart Grid wird wie folgt empfohlen:

> Wegen der neuartigen, zukünftig grundsätzlich möglichen Profilbildung über das Nutzerverhalten von Energienachfragern und damit über Lebensgewohnheiten im privaten Bereich, sollte grundsätzlich sowohl bei den Marktakteuren als auch im Rahmen normativer Prozesse dem Schutz des Anschlussnutzers/Verbrauchers im Smart Grid ein hoher Stellenwert eingeräumt werden.

[15] Die Erhebung von 1/4h-Werten ergibt sich aus den Konventionen des Stromhandelsmarktes bzw. der Bilanzierung; sie ist jedoch gekürt, d.h. es könnte auch (fast) jede andere kleine Zeiteinheit gewählt werden.

[16] ULD-SH, S. 11.

[17] Vgl. Roßnagel/Jandt, S. 9.

[18] Im Folgenden MSB/MDL genannt.

RECHTMÄßIGKEIT

Aufgrund des in § 4 Abs. 1 BDSG verankerten datenschutzrechtlichen Erlaubnisvorbehalts ist ein Erheben, Verarbeiten und Nutzen personenbezogener Daten grundsätzlich verboten. Nur mit einer ausdrücklichen Legitimation ist der Umgang mit den Daten erlaubt. Im Ergebnis muss für alle stattfindenden Datenflüsse bzw. Datenprozesse – ganz gleich, ob es sich um ein Erheben, Nutzen oder Verarbeiten handelt – geprüft werden, ob diese durch Gesetz oder durch Einwilligung legitimiert und damit rechtmäßig sind. In Frage kommt dabei das BDSG als Auffanggesetz, aber auch alle bereichsspezifischen Regelungen, was die Formulierung „andere Rechtsvorschriften" deutlich macht. Ist eine solche Regelung nicht vorhanden, so kann die Rechtmäßigkeit durch eine Einwilligung des Betroffenen erreicht werden.

Im Referenzszenario kommt zunächst der Fernabruf der Daten vom Smart Meter zu Abrechnungszwecken durch den MSB/MDL bzw. Verteilnetzbetreiber und sodann die Visualisierung des Verbrauchs für den Anschlussnutzer in Betracht. Zudem soll die Weiterverteilung der Daten durch den Verteilnetzbetreiber bzw. MSB/MDL beispielsweise an Energielieferanten sowohl für Abrechnungszwecke, aber auch für die Tarifbildung betrachtet werden. In diesem Rahmen soll auch eine Betrachtung der Weitergabe der Daten an sogenannte Dritte für die Bereitstellung von sog. Optimierungsdiensten oder auch für Webanwendungen im Internet wie beispielsweise Google PowerMeter stattfinden.

ANALYSE – ERHEBEN ABRECHNUNG

Grundsätzlich ist ein Erhebender abrechnungsrelevanten Daten nach § 3 Abs. 3 BDSG seitens des MSB/MDL mit Hilfe des Smart Meters durch den zwischen dem MSB/MDL und dem Betroffenen geschlossenen Vertrag gemäß § 28 Abs. 1 Nr. 1 BDSG legitimiert. Das Erheben dient auch der Zweckbestimmung – Messung und Betrieb der Messstelle – des Vertrages.[19]Nimmt – wie in den zahlenmäßig derzeit ganz überwiegenden Fällen – der VNB oder der Lieferant diese Rolle wahr, so liegt zumindest für die Messung kein expliziter Vertrag vor, da diese über den Lieferanten vereinbart wird. Eine Legitimation könnte in den Fällen dieser All-Inclusive-Verträge zwischen Lieferanten und Nutzern insofern allenfalls über ein gesetzliches Schuldverhältnis zwischen VNB und Anschlussnutzer aus § 3 NAV statuiert werden[20].

Allerdings wirft die Erhebung in Form der Fernauslese Probleme auf, denn der Anschlussnutzer hat keine Kontrolle darüber, wann und wie oft Daten aus seinem Gerät ausgelesen werden. Dabei ist zwischen zwei zukünftigen Grundszenarien zu unterscheiden. Möglich ist, dass eine klassische, jährlich aggregierte Abrechnung durch den Lieferanten erstellt wird und eine Auslesung hierbei den klassischen Ableseintervallen folgt. Alternativ können Daten bei Tarifen gemäß § 40 Abs. 3 EnWG auch in sehr kleinen Intervallen ausgelesen werden, soweit dies zur Laststeuerung oder zur Unterbreitung von attraktiven Preisangeboten erforderlich ist. Möglich ist in diesen Fällen allerdings, dass

[19] Regelfall § 21b Abs. 1 EnWG, Übertragung an Dritte § 21b Abs. 2 und 3 EnWG.

[20] Dem könnte allerdings entgegen gehalten werden, dass durch § 3 Abs. 1 NAV allein das Recht des Anschlussnutzers den Anschluss zum Energiebezug zu nutzen konstatiert würde. Damit ist die Belieferung mit Energie nicht Teil der Anschlussnutzung. Bei dieser Sicht, würde es hier an einem gesetzlichen Legitimationstatbestand mangeln.

die auf Tarifen mit unterschiedlichen Last- oder Zeitintervallen beruhende Abrechnung monatlich erfolgt, eine gesetzliche Pflicht zur untertageszeitigen Abrechnung besteht nicht.

In der Literatur wird von den wenigen derzeit kundgegebenen Stimmen für den Fall lastvariabler und tageszeitabhängiger Tarife i.S.d. § 40 Abs. 3 EnWG die Notwendigkeit zur Mitwirkung des Anschlussnutzers im Rahmen des Direkterhebungsgebotes nach § 4 Abs.2 BDSG grundsätzlich verneint, da eine Erhebung des Verbrauches unter Mitwirkung der Betroffenen einen unverhältnismäßigen Aufwand i. S. d. § 4 Abs. 2 Nr. 2b BDSG bedeuten würde.[21]

Für den Fall des klassischen Ableseintervalls wird insofern jedoch eine „Umgehung des Direkterhebungsgebotes“ konstatiert, wenn nicht – wie bei der klassischen manuellen Ablesung – eine Beteiligung des Betroffenen erfolgt.[22] Insofern greift gemäß § 4 Abs. 3 BDSG die Pflicht, den Betroffenen über die Erhebung seiner Daten in Kenntnis zu setzen.

Sollen die Daten in den letztgenannten Fällen hingegen ohne Mitwirkung des Betroffenen erhoben werden, was wegen des Bequemlichkeitsvorteils durch Fernabruf durchaus auch im Interesse des Betroffenen liegen kann, soll eine Legitimation nur durch eine Einwilligung i. S. d. § 4a BDSG möglich sein.[23] Aber auch in anderen Fällen, wo es an einem anderen Legitimationstatbestand fehlt, ist die Erteilung der Einwilligung unumgänglich, weshalb schon an dieser Stelle auf den nach der geltenden Rechtslage programmierten Medienbruch bei der informatorischen Gestaltung des SmartGrid eingegangen werden soll.

Auch wenn derzeit die Stromlieferverträge regelmäßig noch in papierner Form geschlossen werden dürften, wird sich mit der IKT-basierten informatorischen Vernetzung aller Akteure des Energiemarktes auch hier ein Paradigmenwechsel vollziehen. Die Nutzung des Internet durch die Anschlussnutzer beispielsweise beim Tarifwechsel oder im Rahmen von lokalen Optimierungsclustern, bei denen lokale Nachfrager durch den Abgleich ihrer Lastprofile die gemeinsame Energienachfrage effizient gestalten, werden im Hinblick auf die notwendig häufig wechselnden Vertragsbeziehungen nur zu realisieren sein, wenn die notwendigen Willenserklärungen weitestgehend in elektronischer Form ausgetauscht werden. Da diesen Erklärungen häufig auch korrespondierende datenschutzrechtliche Erklärungen folgen können, würde ein aus dieser Perspektive folgender Medienbruch das diesbezügliche Marktgeschehen in seiner Entwicklung deutlich hemmen. Im Gegensatz zur Regelung des TMG stellt sich nunmehr die Möglichkeit einer medienbruchfreien elektronischen Einwilligung unter der Ägide des BDSG als problematisch dar. Die Formulierung „Schriftform” in § 4a Abs. 1 S. 3 BDSG bedeutet nach § 126 Abs. 1 BGB, dass die Erklärung vom Aussteller eigenhändig durch Namensunterschrift unterzeichnet werden muss. Allerdings ist anerkannt, dass die Einwilligung unter der Voraussetzung einer qualifizierten elektronischen Signatur nach dem Signaturgesetz auch elektronisch erklärt werden kann.[24] Aus

[21] Vgl. Roßnagel/Jandt, S. 36, ULD-SH, S. 11.

[22] Vgl. ULD-SH, S. 6. Siehe auch das Vorbringen bei Roßnagel/Jandt, S. 36: „Die Datenerhebung verstößt somit grundsätzlich gegen das Prinzip der Direkterhebung beim Betroffenen“.

[23] ULD-SH, S. 7.

[24] Gola/Schomerus, § 4a Rn. 13. Allerdings ist auch die Verwendung von signaturgesetzkonformen PIN-Verfahren im Hinblick auf den besonderen Rang des Schriftformerfordernisses im Datenschutzrecht in der Literatur in Abrede gestellt worden, vgl. Albrecht, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, S. 100.

praktischer Sicht stellt sich für Dienste im zukünftigen Smart Grid aber das Problem, dass die vom Gesetz geforderte qualifizierte elektronische Signatur bislang nur einen äußerst geringen Verbreitungsgrad gefunden hat. Für die hier untersuchungsgegenständliche Sachgestaltung greift zudem auch nicht das Formprivileg des § 28 Abs.3a BDSG. Aus der Gesetzesbegründung[25] ergibt sich, dass diese Konkretisierung von besonderen Umständen, bei denen eine andere Form angemessen sein kann, nur für die in § 28 Abs. 3 BDSG genannten Zwecke gelten soll.

Daraus folgt, dass in fast allen Fällen der Notwendigkeit einer Einwilligung zur Legitimation von Datenverwendungen im Smart Grid ein Medienbruch durch Versand von entsprechend verkörperten, unterschriebenen Erklärungen hinzunehmen wäre.

HANDLUNGSBEDARF

Da aus den ersten Erfahrungen der Modellprojekte in Zukunft davon auszugehen ist, dass sich kontinuierlich neue Geschäftsmodelle, Szenarien und Akteure am Rand des bestehenden Energiemarkts etablieren werden, die auf Basis von Messdaten einen Beitrag zur Energieeffizienzsteigerung leisten, diese Gestaltungen aber durch den Gesetzgeber nicht vollständig antizipiert werden können, wird die Bedeutung der datenschutzrechtlichen Einwilligung in diesem Bereich noch zunehmen.

Insofern ist es nahe liegend, dass, sofern keine hinreichende vertragliche oder gesetzliche Legitimation für eine Weitergabe der Daten durch den MSB/MDL an diese weiteren Akteure besteht, die informierte Einwilligung eine Aufwertung in diesem Bereich erfahren kann. Die personenbezogenen Verbrauchs- und Gerätedaten der Nutzer z. B. einer internetbasierten Effizienzberatung könnten auf den ersten Blick insofern als Nutzungsdaten i. S. d. Telemediengesetzes (TMG) angesehen werden. Unter dessen Ägide könnte eine an den Vorgaben des § 13 Abs. 2 TMG orientierte medienbruchfreie elektronische Einwilligung auf der Dienstplattform realisiert werden. Allerdings finden das TMG und damit seine Einwilligungsregelung nur im Hinblick auf die Bestands- und Nutzungsdaten der Dienstnutzer Anwendung. Hierzu zählen die Verbrauchsdaten nicht. Daneben gilt es zu bedenken, dass im zukünftigen Smart Grid auch der Stellenwert reiner Maschine-Maschine Kommunikation zunehmen wird. Allein diese Feststellung kann motivieren, dass ein an den Vorgaben des § 126a Abs.1 BGB orientiertes Schriftformerfordernis, welches aus der Perspektive der informationellen Selbstbestimmung primär in seiner Warnfunktion Bedeutung erlangt, hier eine bereichsspezifische Modifikation erfahren muss. Um den Anschlussnutzer in einer vernetzten Welt vor einer Überflutung durch Informationen zu schützen und mithin die Aufmerksamkeit für wirklich kritische Fälle zu erhalten, sollten für die Folgeszenarien der Maschine-Maschine-Kommunikation vielmehr Konzepte diskutiert werden, bei denen auf Basis einer Einwilligung mit verständlichen Informationen zur Systemstruktur und unter Verwendung von elektronischen Datenschutzpolicys, die eine Repräsentation der vom Nutzer gewünschten Datenverwendungen enthalten,[26] im laufenden Betrieb der menschliche Akteur Informationen nur noch beim Vorliegen von diesbezüglichen Anomalien erhält.

[25] BT-Drs. 16/12011, S. 31 ff.

[26] Vgl. Wagner/Speiser/Harth/Raabe/Weis, Basic Privacy Principles for the Smart Grid , W3C Workshop on Privacy for Advanced Web APIs, im Erscheinen 2010.

De lege ferenda scheint es geboten, für den Energiesektor eine vereinfachte elektronische Einwilligung nach dem Vorbild des § 13 Abs.2 TMG zu schaffen.

ANALYSE – ÜBERMITTLUNG

Die Übermittlung von Messwerten aus dem vom MSB betriebenen Zähler an den VNB und sodann an den Lieferantenist nur gerechtfertigt, wenn die Weitergabe Gegenstand des Vertrages mit dem MSB/MDL ist. Letzteres bedeutet, dass eine vertragliche Vereinbarung in den Messstellenvertrag aufgenommen werden muss, dass die Ableseergebnisse bzw. Messdaten an den Lieferanten übermittelt werden. Tritt der Lieferant selbst als Messstellenbetreiber auf, so ist die Übermittlung der Verbrauchsdaten nur im Rahmen des Energieliefervertrages zulässig.[27]

Nach Auffassung des ULD-SH besteht eine rechtliche Verpflichtung oder Berechtigung zur Übermittlung der Daten seitens des MSB/MDL nicht. Es bestehe kein berechtigtes Interesse gemäß § 28 Abs. 1 Nr. 2 oder Abs. 2 Nr. 2a BDSG. Auch aus dem Umkehrschluss aus § 4 Abs. 3 S. 3 MessZV ließe sich schließen, dass keine Verpflichtung oder Berechtigung besteht.[28]

Grundsätzlich muss der MSB/MDL die Rohmessdaten so aufbereiten, dass er nur die erforderlichen Daten an den Lieferanten weitergeben kann (z. B. für die Abrechnung in den vereinbarten Abrechnungsintervallen), ansonsten ist eine Übertragung datenschutzrechtlich aus Gründen der Datensparsamkeit und Erforderlichkeit unzulässig. Auf diese Prinzipien wird an späterer Stelle einzugehen sein[29]. Gemäß § 40 Abs. 3 EnWG sind Energieversorgungsunternehmen ab dem 30. Dezember 2010 verpflichtet dem Verbraucher Tarife anzubieten, welche einen Anreiz zu Energieeinsparung geben. Darunter sind insbesondere lastvariable oder tageszeitabhängige Tarife zu verstehen[30]. Das Anbieten solcher Tarife setzt die Kenntnis des Entnahmezeitpunktes und des Zeitpunktes einer konkret entnommenen Energiemenge voraus.

Die Verarbeitung, insbesondere die Übermittlung und die Nutzung solcher Lastprofile zur Erfüllung lastvariabler und tageszeitabhängiger Tarife durch den Lieferanten ist gemäß § 28 Abs. 1 Nr. 1 BDSG zur Vertragserfüllung des Energieliefervertrages nur zulässig, sofern einerseits die Erhebung dieser steuerungsrelevanten Daten Gegenstand eines zwischen dem MSB/MDL und dem Netznutzer/Verbraucher geschlossenen Vertrages sind und diese Daten auch erforderlich sind. Erforderlich ist die Erstellung von detaillierten und individuellen Lastgängen nur dann, wenn der Energieliefervertrag eine Abrechnung nach den verschiedenen Tarifen vorsieht. Es dürfen dann nur Messungen in solchen Zeitintervallen erhoben und übermittelt werden, soweit solche unter-

[27] Vgl. ULD-SH, S. 10 f.

[28] Vgl. ULD-SH, S. 10 f.

[29] Vgl. Abschnitt „Erforderlichkeit“ und „Datensparsamkeit“.

[30] Vgl. zu den Begrifflichkeiten, BNetzA, Bericht - Wettbewerbliche Entwicklungen und Handlungsoptionen im Bereich Zähl- und Messewesen und bei variablen Tarifen, S. 54 ff.

schiedlichen Tarife angeboten werden. Messungen in kleineren Zeitintervallen können durchaus zwischen MSB/MDL und dem Verbrauchern im Wege der informierten ausdrücklichen Einwilligung vereinbart werden. Übermittelt werden dürfen sie dem Lieferanten in der feineren zeitlichen Auflösung aber nicht, sofern dies kein Erfordernis für die Abrechnung der im Vertrag vereinbarten Tarife ist.[31]

ANALYSE – WIDERSPIEGELN DES STROMVERBRAUCHS

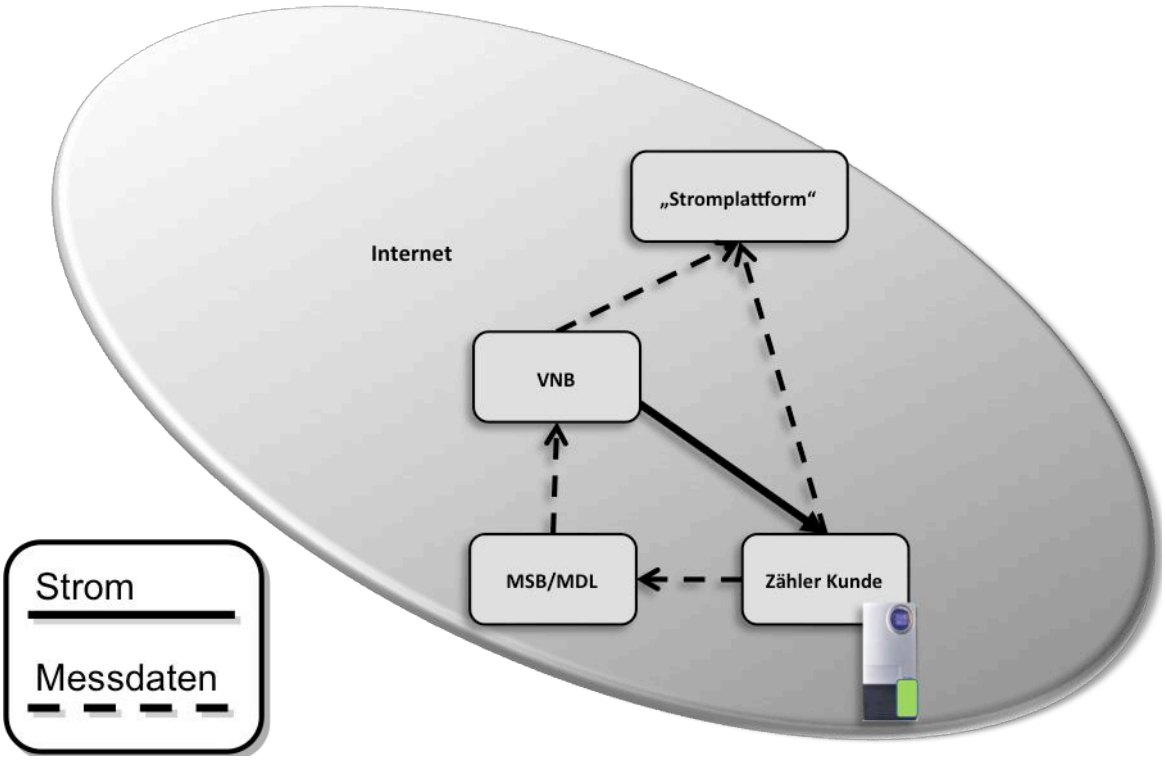

Abbildung 2: Widerspiegeln des Stromverbrauchs

Mit dem Einbau von Energiezählern nach § 21b Abs.3a EnWG soll dem Letztverbraucher die Möglichkeit eröffnet werden, sich den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegeln zu lassen. Welche Mindestanforderungen und Funktionalitäten die Messeinrichtung für diesen Zweck zu erfüllen hat, ergibt sich weder aus dem EnWG noch aus der MessZV. Vielmehr wurde von Seiten des Gesetzgebers ganz bewusst auf eine Festschreibung von technischen Standards und Mindestanforderungen sowie Ausstattungsdetails verzichtet, da das flächendeckende Rollout von Smart Metern als marktgetriebener Prozessgeschehen soll. Die Marktakteure, Unternehmer und Verbraucher sollen in ihrer Freiheit nur geringstmöglich durch gesetzliche Vorgaben eingeschränkt werden.[32] Nach Auffassung der BNetzA bedeutet der Begriff des Widerspiegelns, dass dem Anschlussnutzer die von der Messeinrichtung ermittelten Werte angezeigt werden.[33] Es reicht dabei jede Darstellungsform aus, sofern sie dem Anschlussnutzer die

[31] Vgl. ULD –SH, S. 11, 12 u. 14.

[32] Bericht BNetzA, S. 3. U. 7.

[33] Vgl. BNetzA, Konsultation eines Positionspapieres zu den Anforderungen an Messeinrichtungen im Sinne von § 21b Abs. 3 a und b EnWG, Az. BK6-09-170 vom 06.11.2009, online unter http://www.bundesnetzagentur.de [10.05.2010].

Informationen in geeigneter Form visualisiert. Dies kann auf einem elektronischen Display an der Messeinrichtung selbst geschehen, wobei der Wert entweder ständig oder auch rollierend angezeigt werden kann, oder aber auch auf einem Home Display in der Wohnung. Eine weitere Möglichkeit wird im Zugänglichmachen der Verbrauchswerte über ein Internetportal gesehen. Vorausgesetzt wird dabei in der Auslegung der BNetzA das Einverständnis des Anschlussnutzers, sofern bei der Visualisierung Dritte Kenntnis von den Werten erlangen können.[34] Damit ergeben sich nach dem bisherigen Verständnis drei zu untersuchende Gestaltungen, wobei die Frage, ob die Werte ständig oder rollierend angezeigt werden, vernachlässigt werden kann.

Bei einer Anzeige des Verbrauchs auf einem Display direkt an der Messeinrichtung selbst werden noch keine Informationen über eine mögliche Schnittstelle des Messgerätes nach außen gegeben. Es ist davon auszugehen, dass die Messwerte lediglich geräteintern aufbereitet und auf dem Display angezeigt werden.

Nach § 3 Abs.3 BDSG ist Erheben das „Beschaffen von Daten über den Betroffenen“. Welche Kriterien beim Beschaffen anzulegen sind, bleibt unklar. Wählte man eine eigentumsrechtliche Anknüpfung an dem Messgerät, wären die Daten schon vom MSB/MDL „beschafft“, wenn sie lediglich im Speicher des Messgerätes abgelegt werden, weil der Speicher insofern (auch) schon in der rechtlichen Herrschaftssphäre des MSB/MDL läge. Legte man hingegen die Auslegung des ULD zur Problematik der Direkterhebung zugrunde, würde wie beim klassischen Ablesen zum „Erheben“ noch die aktive Komponente des tatsächlichen Auslesens der Daten durch den MSB/MDL hinzutreten müssen. Sodann würden folgerichtig die datenschutzrechtlichen Transparenz und Mitwirkungspflichten des MSB/MDL erst mit dem Abruf der Daten erwachsen.

Ebenso verhielte es sich im Falle eines Home Displays. Auch hier werden die Messwerte nur in der Messeinrichtung verarbeitet und auf einer externen, also nicht direkt am Gerät befindlichen Anzeige dem Verbraucher zur Kenntnis gebracht. Dies geschieht aber nicht durch Einbeziehung weiterer Akteure, welche die Daten erhalten, sondern wird sinnvoller Weise lediglich durch eine sichere direkte Verbindung der Messeinrichtung mit dem Home Display in der Wohnung geschehen. Ein Erheben der Daten durch den MSB/MDL nach § 3 Abs. 3 BDSG liegt daher in beiden Fallgestaltungen nicht vor, denn die Daten befinden sich nur auf dem Zähler.

Damit würde aber nach der inhärenten Logik des BDSG für die Fälle der Speicherung der Messdaten zum Zwecke des „Widerspiegelns“ trotz der Speicherung der Daten im Messgerät und der damit einhergehenden erhöhten datenschutzrechtlichen Gefährdungslage keine verantwortliche Stelle zu identifizieren sein, welche Verfahrensvorkehrungen für diese Sachgestaltung pflichtig erfüllen muss. Denn selbst wenn man beispielsweise ein „Erheben“ der Daten durch den Anschlussnutzer selbst konstatieren würde, wäre diese Tätigkeit ggf. nach § 1 Abs.2 Nr. 3 BDSG als Erhebung für persönliche oder familiäre Tätigkeiten privilegiert und vom an die Erhebungsphase anknüpfenden Pflichtenkanon befreit. Vergegenwärtigt man sich, dass aus der feingranularen Auflösung von Stromverbrauchsdaten (selbst ohne gerätegenau verteilte Messsensorik) gerade einzelne Familienmitglieder sehr schnell eine Zuordnung von Stromverbrauch, Zeit und Gerätetypik zu Personen, die sich in der fraglichen Zeit in der Wohnung aufgehalten haben, vornehmen können, kann sich gerade ein innerfamiliärer Überwachungsdruck entwickeln, der eine Privilegierung nach § 1 Abs.2 Nr.3 BDSG in Frage stellen muss. Selbst wenn man aber insofern von einer datenschutzrechtlichen Verantwortlichkeit des Anschluss-

[34] Ebd. S. 4.

nutzers in dieser Phase ausgehen würde, wäre das Schutzprogramm für diesen Fall nicht hinreichend. Besonders problematisch ist aber, dass insofern gleichartige Sachverhalte einer unterschiedlichen Behandlung hinsichtlich des Normadressaten zugeführt würden, da das Widerspiegeln der Verbrauchsinformationen entsprechend der Auslegung der BNetzA auch ausdrücklich über ein Webportal / das Internet möglich sein soll.

Die Verbrauchsinformationen gelangen hierbei direkt vom Messgerät über eine entsprechende Schnittstelle zum MSB/MDL und zwar im Wege der Fernauslese. Ein direkter Zugriff beispielsweise auf einen Webserver, der in das Messgerät integriert wäre, dürfte aus Gründen der Datensicherheit ausscheiden. Damit wären nach klassischer Auslegung die Daten vom MSB/MDL beschafft und mithin auch erhoben. Es griffe folglich der datenschutzrechtliche Schutzpflichtenkanon in Person des MSB/MDL als verantwortlicher Stelle. Dieser legt die Daten auf einen Server, wo sie über das Internet vom Verbraucher wiederum durch Einloggen, also beispielsweise durch Eingabe seiner Benutzerdaten und einem Passwort, eingesehen werden können. Die Daten gelangen damit unter Umständen auch an den Verteilnetzbetreiber (VNB als originärer MSB/MDL).[35] Die Erhebung ist, wie oben ausgeführt, grundsätzlich zulässig.

Fraglich ist allerdings auch in dieser Fallgestaltung, wie der innerfamiliäre Schutz vor Überwachung, welche sich durch die hier gegebene Möglichkeit des weltweiten Datenabrufes noch verschärft, gesichert werden kann. Die BNetzA hat zwar insofern zu dem Fragenkreis Stellung bezogen, als inden Konsultationen ausgeführt wird, dass „[…]*soweit dabei die Werte zur Kenntnis Dritter gelangen, es dazu des Einverständnisses des Anschlussnutzers bedarf* […]“.Dies ist in datenschutzrechtlicher Sicht aber eine zu allgemeine Aussage und wirft absehbar weitere Fragenkreise auf. Die Reduzierung auf die „Kenntnis Dritter“ und das „Einverständnis des Anschlussnutzers“ greifen in zweierlei Hinsicht zu kurz:

Sofern „Dritte“ Kenntnis von den Daten erlangen können, ist allein das Einverständnis des „Anschlussnutzers“ aus datenschutzrechtlicher Sicht nicht hinreichend. Der verwendete (gesetzliche) Begriff des Anschlussnutzers ist mehrdeutig und lässt auf den ersten Blick nicht erkennen, ob nur der vertraglich gebundene Nutzer oder auch Familienangehörige, WG-Bewohner, Gäste und Untermieter ihr Einverständnis äußern müssen. In der Literatur wird, jedenfalls für den Fall der Haftung nach § 18 NAV bei der berechtigten Anschlussnutzung, auch ein Dritter (Untermieter, Gäste) in den Schutzzweck des Anschlussnutzungsverhältnisses einbezogen.[36] Demnach würde in der hier vorgenommenen Festlegung jede Person bei realer Stromentnahme ein entsprechendes Einverständnis erteilen müssen. Dieses Ergebnis wäre zwar aus datenschutzrechtlicher Sicht richtig, beruhte aber auf einer fehlerhaften Interpretation des Begriffs des Anschlussnutzers. Nach der Definition des § 1 Abs.3 NAV ist neben der tatsächlichen Entnahme von Energie auch noch das Bestehen eines Anschlussnutzungsverhältnisses konstitutiv, denn *„Anschlussnutzer ist jeder Letztverbraucher, der im Rahmen eines Anschlussnutzungsverhältnisses einen Anschluss an das Nieder-*

[35] Grundsätzlich ist der Verteilnetzbetreiber gemäß § 21b Abs.1 EnWG sowohl Messstellenbetreiber als auch Messdienstleister, sofern der Anschlussnutzer keinen dazu Dritten bestimmt hat. § 4 Abs. 4 MessZV legt nahe, dass der VNB in Zukunft als Datendrehscheibe im Energiewirtschaftssektor fungieren soll.

[36] Hartmann in Danner/Theobald, IV B2 § 18 RN. 35.

spannungsnetz zur Entnahme von Elektrizität nutzt“. Auch der Gesetzgeber geht davon aus, dass die reine Inanspruchnahme eines Anschlusses noch keine Eigenschaft als Anschlussnutzer begründet.[37]

Dass Dritte (Gäste, Untermieter, etc.) nicht in den Begriff des Anschlussnutzers aufgenommen sind, zeigt auch die systematische Betrachtung der Rechtsfolgen. So ist der Messstellenwechsel nach § 5 Abs.1 MessZV vom Anschlussnutzer zu erklären. § 5 Abs.1 MessZV bestimmt: „Ein Anschlussnutzer hat gegenüber dem Netzbetreiber in Textform zu erklären, dass er beabsichtigt, nach § 21b EnWG einen Dritten mit dem Messstellenbetrieb oder der Messung zu beauftragen“. Dass diese Erklärung durch Gäste oder Untermieter abgegeben werden soll, kann hier nicht intendiert sein. In der Folge dieser Auslegung würde mithin im Hinblick auf eine Kenntniserlangung durch Dritte ein Einverständnis durch den Vertragspartner des Anschlussnutzungsverhältnisses ausreichen. Aus datenschutzrechtlicher Sicht zeigt sich damit, dass die Verwendung des energiewirtschaftsrechtlichen Begriffs „Anschlussnutzer“ im Zusammenhang mit der hier vorgenommenen Konkretisierung von datenschutzrechtlichen Obliegenheiten nicht mehr, sondern weniger an Rechtsklarheit generiert.

HANDLUNGSEMPFEHLUNG

§ 21b EnWG gibt in den Fällen des Abs. 3a und 3b hinsichtlich der Forderung, dem jeweiligen Anschlussnutzer den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerzuspiegeln, keine technische Realisierung vor. Daher ist im Vorgriff auf den Aspekt der Datensparsamkeit hier schon zu konstatieren, dass in jedem Fall die datensparsame Variante einer Messeinrichtung mit elektronischem Display an der Messeinrichtung selbst oder aber auch auf einem Home Display und mithin eine Messeinrichtung ohne eine Kommunikationsschnittstelle zur externen Kommunikation angeboten werden muss.

Ein Angebot, welches den Anschlussnutzer zur Nutzung von externen IKT-Infrastrukturen zwingen würde, würde dieser datenschutzrechtlich gebotenen Konkretisierung nicht stand halten. Eine andere Frage ist aber gleichwohl, wie den auch in den datensparsameren Alternativen angelegten Gefahren für die informationelle Selbstbestimmung aller Betroffenen begegnet werden kann.Um eine eindeutige Verantwortlichkeit für das datenschutzrechtliche Pflichtenprogramm zu erreichen, sollte insofern zunächst die Frage nach dem Normadressaten auch im Hinblick auf die Pflicht zum Widerspiegeln der Verbrauchwerte vereinheitlicht werden. Diese Pflicht würde insofern nicht an der Frage ansetzen, ob und durch wen Daten zu Abrechnungszwecken verwendet würden oder welche Realisierung zum Widerspiegeln des Stromverbrauchs Einsatz findet. Wegen der grundsätzlich auch innerfamiliär erhöhten datenschutzrechtlichen Gefahrenlage im Vorfeld eines Messdatenabrufes sollte vielmehr für den MSB/MDL als verantwortliche Stelle bereichsspezifisch eine allgemeine verfahrensrechtliche Absicherung konstatiert werden. Insofern wäre es denkbar sich an der vergleichbaren Sachgestaltung des § 99 TKG zu orientieren.

[37] BR-Drs. 367/06; S. 35f.

Zum Schutz vor innerfamiliärer Überwachung bei der Verwendung hochaufgelöster Messdaten im Falle des § 21b Abs.3a EnWG, sollte dem MSB/MDL nach dem Vorbild des § 99 TKG eine verfahrensrechtliche Pflicht zur Absicherung der Rechte von weiteren Betroffenen normativ auferlegt werden.

ANALYSE – DRITTSTAATENÜBERMITTLUNG

Sollen die feingranularen Messdaten dem Anschlussnutzer über ein Webportal zugänglich gemacht werden, gelangen sie im Wege der Fernauslese regelmäßig direkt vom Messgerät über eine entsprechende Schnittstelle zum MSB/MDL. Dieser legt die Daten auf einen Server, wo sie über das Internet vom Verbraucher eingesehen werden können.

Die Erhebung der Daten zu Zwecken des § 21b Abs.3a EnWG ist, wie oben schon ausgeführt, grundsätzlich zulässig. Problematisch ist allerdings die Übertragung auf einen externen Server, denn dies ist einerseits nicht durch den bestehenden Vertrag legitimiert, andererseits kann sich ein solcher Serverbetreiber samt Server auch in Drittstaaten befinden. Ein solches Beispiel stellt die Webanwendung Google PowerMeter dar. Hier besteht die Möglichkeit, die Daten durch den eigenen Lieferanten (in Deutschland bisher Yellostrom) an die Plattform übertragen zu lassen.

Eine solche Weitergabe an Google stellt eine Zweckänderung dar, für welche eine neue Legitimation vorliegen muss. Der Verbraucher muss dies also in einem Vertrag mit seinem Stromanbieter regeln oder in eine solche geänderte Nutzung nach umfänglicher Aufklärung ausdrücklich einwilligen. Bei der Webanwendung Google PowerMeter sind die seitens des Stromanbieters zur Verfügung gestellten Messwerte pseudonymisiert. Google generiert beim Erstellen eines Kontos eine Kennung, welche dem Stromanbieter im Rahmen eines Aktivierungsprozesses mitgeteilt wird. Lediglich der Stromanbieter kann dann seinem Kunden die Kennung zuordnen und übermittelt lediglich die mit der Kennung versehenen Messdaten an den Server. Google selbst erhält damit Daten, bei welchen die Identifikationsmerkmale durch ein Kennzeichen ersetzt sind. Eine Speicherung bzw. Verarbeitung gegebenenfalls in den USA oder anderen Ländern, wie sie Google in seinen Datenschutzhinweisen für den Google Power Meter[38] ankündigt, erscheint somit zunächst unproblematisch.

Nimmt man aber in den Blick, dass im „Internet der Dienste“ in Zukunft viele neue Webanwendungen zur Verfügung gestellt werden, der Anbieter Google eine Vielzahl von Diensten betreibt und neben Verbrauchs- auch Nutzungsdaten wie IP-Adressen sammelt,[39] die ggf. eine Personalisierung des Nutzers zulassen und mithin die Möglichkeit der Zusammenführung dieser Informationen mit den Kontodaten des PowerMeters hinreichend wahrscheinlich erscheint, stellt sich die Frage, ob eine Übermittlung der Daten auf den Google-Server in einen Drittstaat ohne angemessenes Datenschutzniveau zulässig sein kann.

[38] Siehe http://www.google.com/powermeter/privacy [10.05.2010].

[39] Vgl.: Berliner Beauftragter für Datenschutz und Informationsfreiheit, Jahresbericht 2009, S. 20, http://www.datenschutz-berlin.de/attachments/669/Jahresbericht_2009.pdf?1269595949 [10.05.2010].

Wegen des Massencharakters der Übermittlungsvorgänge und der besonderen Gefahranlage erscheint es nicht hinreichend, eine Legitimation allein auf Grundlage einer Nutzerentscheidung nach § 4c Abs.1 Nr. 1-3 BDSG als zulässig zu erachten. Der Betroffene wird sich wegen des komplexen Gefüges der möglichen Informationsflüsse regelmäßig kein hinreichendes Bild über die Risiken und Verarbeitungsstrukturen als Basis einer freiwilligen und informierten Entscheidung machen können. Zudem sind einstweilen keine Gründe ersichtlich, weshalb eine gleichartige Dienstleistung nicht auch auf Servern erbracht werden kann, die in der EU beheimatet sind. Vielmehr sollten in diesem Sachbereich durch die Datenschutzaufsichtsbehörden geprüfte Garantien als regelmäßiger Legitimationstatbestand nach dem Vorbild des § 4c Abs.3 BDSG bereichsspezifisch normativ eingeführt werden. Mithin sollten insbesondere Vertragsklauseln oder verbindlichen Unternehmensregelungen für den Masseneinsatz der Übermittlung von nicht anonymisierten Messdaten in Drittstaaten ohne angemessenes Datenschutzniveau zwingend Verwendung finden.

Wegen der besonderen Sensibilität der feingranular aufgelösten Messdaten sollte bereichsspezifisch geregelt werden, dass weder eine Pseudonymisierung der Werte noch die Erfüllung der Voraussetzungen des § 4c Abs.1 Nr. 1-3 BDSG Grundlage für die Übermittlung in Drittsaaten ohne angemessenes Datenschutzniveau darstellen können.

ZWECKBINDUNG

Die Zulässigkeit des Einsatzes von Smart Metern kann nicht losgelöst von den damit verfolgten Zwecken beurteilt werden. „Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden (…), lässt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten.“[40] Art. 6 Abs. 1 lit. b der Datenschutzrichtlinie (RL 95/46/EG) bestimmt, dass die mit der Datenverarbeitung verfolgten Zwecke festgelegt, eindeutig und rechtmäßig sein müssen. Rechtmäßig ist ein Zweck im nicht-öffentlichen Bereich aber bereits dann, wenn er nicht verboten ist.[41] Entsprechend gilt nach h.M. auch zum BDSG, dass ein legitimer Zweck gesetzlich nicht ausdrücklich anerkannt zu sein braucht, sondern grundsätzlich tatsächliche, ideelle, wirtschaftliche oder sonstige von der Rechtsordnung gebilligte Interessen zu berücksichtigen sind.[42]

ANALYSE

Im Referenzszenario sind verschiedene Zwecke zu identifizieren, die eine Verwendung personenbezogener Daten erfordern. Zu nennen sind zuvorderst die Abrechnungserstellung, aber auch die Kontrolle der Funktionsfähigkeit von Messgeräten und das Energiemanagement (u.a. Lastverteilung,

[40] BVerfGE 65, 1, 44.

[41] Vgl. Brühann in Grabitz/Hilf, Art. 6 Rn. 10: „Datenverarbeitung für unrechtmäßige Zwecke“ sei beispielsweise ausgeschlossen.

[42] Vgl. Gola/Schomerus, § 28 Rn. 33; Schaffland/Wiltfang, § 28 Rn. 85; vgl. auch BGH NJW 1984, 1886, 1887: Ein berechtigtes Interesse sei weniger als ein rechtliches Interesse.

Sicherstellung der Energieversorgung, Einsparung des Energieverbrauchs, CO_2-Einsparung, Effizienz, Serviceleistungen, Preistransparenz, Kosteneinsparung, Marktkompatibilität, realistische Umsetzbarkeit, gesteigerte Abnahme Erneuerbarer Energien).

Wegen des begrenzten legislativen Prognosehorizontes im Hinblick auf das Smart Grid wird auch zukünftig die Bestimmung von bereichsspezifisch privilegierten, enumerativ aufgezählten legitimen Zwecken der Datenverwendung, wie sie in anderem Sachzusammenhang im modifizierten Listenprivileg des § 28 Abs.3 BDSG ihren Niederschlag gefunden hat, eher die Ausnahme denn die Regel bilden. Im Hinblick auf die notwendige Entwicklungs- und Innovationsoffenheit eines informatorischen Systems zur Energieeffizienzsteigerung ist dies systemimmanent. Damit bildet für die Marktakteure die Bestimmung der legitimen Zwecke einer Datenverwendung eine wesentliche Grenze. Im Interesse eines sachgemäßen Interessenausgleichs bei gleichzeitiger Schaffung von Rechtssicherheit, welche im Hinblick auf das enorme und zum Teil bereits geleistete Investitionsvolumen für konkrete Hard- und Softwaregestaltungen zur Steuerung von Datenflüssen notwendig ist, gewinnt damit aber die Bestimmung der Legitimität von Zweckfestlegungen durch die jeweiligen Datenschutzaufsichtsbehörden deutlich an Gewicht. Wie die bisherigen Erfahrungen in den Modellregionen zeigen, ist für eine zuverlässige datenschutzrechtliche Bewertung eine feingranulare Modellierung der in der jeweiligen Sachgestaltungen verfolgten Zwecke und Notwendigkeiten einzelner Datenverwendungen erforderlich. Grundsätzlich unterliegen die hier sachgegenständlichen Gestaltungen im Hinblick auf § 4d Abs. 4 BDSG sowohl der Meldepflicht mit den Inhalten nach § 4e BDSG, als auch gegebenenfalls der Vorabkontrolle nach § 4d Abs. 5 BDSG. Aber auch davon unabhängig sollte ein vitales Eigeninteresse gerade der Modellregionen bestehen, schon in den Forschungsprogrammen für hinreichende Sachverhaltskonkretisierungen bei den Aufsichtsbehörden zu sorgen und den Dialog zu suchen.

> Die Modellprojekte der Förderprogramme E-Energy und IKT für Elektromobiltät sollten für jede szenariospezifisch geplante Verwendung personenbezogener Daten eine genaue Bestimmung der Zwecke der Verarbeitung vornehmen, datensparsame Alternativen formulieren und den Datenschutzaufsichtsbehörden frühzeitig zur Kenntnis bringen.

Im Referenzszenario ergibt sich die Legitimität der Verwendung der Messdaten zum Zweck der Abrechnungserstellung schon daraus, dass Energielieferanten nicht nur ein vertragliches Interesse an der Vergütung der gelieferten Energie haben, sondern nach § 40 Abs. 2 EnWG auch gesetzlich zur Abrechnung verpflichtet sind.

Jenseits dieses allgemein anerkannten Zweckes einer Verwendung personenbezogener Daten im Smart Grid sind aber auch Sachgestaltungen als legitimer Zweck anzuerkennen, die nicht so offensichtlich im Fokus liegen.

So ist z.B. als legitimer Zweck einer Datenverwendung auch das Energiemanagement anzuerkennen. Es dient dem Umweltschutz (Einsparung von Energie und CO_2) und hat mit Aufnahme in den Vertrag von Lissabon (vgl. Art. 194 AEUV), in Vorgaben diverser Richtlinien wie der Elektrizitätsbinnenmarkt-

richtlinie (RL 2009/72/EG) oder der Energieeffizienzrichtlinie (RL 2006/32/EG) allgemeine Anerkennung erfahren[43].

Problematisch ist allerdings, ob bei der Bewertung der Legitimität von Zwecken auch Wirtschaftlichkeitserwägungen eingestellt werden können. Nach datenschutzrechtlichen Maßstäben ist Wirtschaftlichkeit im Rahmen der Interessenabwägung zu berücksichtigen. Auch nach der Elektrizitätsbinnenmarktrichtlinie ist die Wirtschaftlichkeit ein zentrales Kriterium für die Einführung intelligenter Messsysteme. So soll die Einführung auf Grundlage von wirtschaftlichen Erwägungen erfolgen (EG 55). Auch soll berücksichtigt werden, welche Art des intelligenten Messens wirtschaftlich vertretbar und kostengünstig ist (Anhang I Abs. 2). Auch nach Art. 13 Abs. 1 der Energieeffizienzrichtlinie sollen der finanzielle Aufwand zu berücksichtigen und individuelle Zähler zu „wettbewerbsorientierten Preisen“ zu liefern sein.

Auf der anderen Seite ist das Persönlichkeitsrecht der Betroffenen einhochrangiges Schutzgut. Wirtschaftlichkeit kann daher nur berücksichtigt werden, wenn dies nach datenschutzrechtlichen Maßstäben vorgegeben ist. So sind nach Art. 46 der Datenschutzrichtlinie Schutzinteressen der Betroffenen nicht nur bei der eigentlichen Verarbeitung von Daten, sondern bereits zum Zeitpunkt der Planung eines Datenverarbeitungssystems und damit auch im Zusammenhang mit der Planung des Einsatzes von Smart Metern zu berücksichtigen. Welche Schutzmaßnahmen insoweit erforderlich sind, ist abwägungsabhängig (vgl. Art. 17 Abs. 1 der Datenschutzrichtlinie). Zu berücksichtigen sind nach dieser Richtlinie nicht nur die von der Datenverarbeitung ausgehenden Risiken und die Art der jeweiligen Daten, sondern auch der Stand der Technik und grundsätzlich die „entstehenden Kosten“. Daneben enthält auch das BDSG zahlreiche Generalklauseln, die eine Interessenabwägung erforderlich machen. So sind etwa nach § 9 BDSG nur Schutzmaßnahmen erforderlich, die in Bezug auf Aufwand und Schutzzweck angemessen sind. Zu berücksichtigen sein soll insoweit auch der finanzielle Aufwand.[44]

Auch im Zusammenhang mit sonstigen Vorschriften, die eine Interessenabwägung erfordern, sollen wirtschaftliche Effizienzvorteile zu berücksichtigen sein. So hält etwa das BAG fest, dass auch eine wirtschaftlich sinnvolle, da schnelle und kostengünstige Datenverarbeitung einem berechtigten Interesse entspreche.[45] Insofern gibt auch hier das BDSG eine Berücksichtigung wirtschaftlicher Zusammenhänge im Rahmen der gebotenen Abwägung vor.

HANDLUNGSBEDARF

Neben den materiellen Aspekten die im Rahmen der Bestimmung legitimer Zwecke Berücksichtigung finden können verlangen die besonderen Gefährdungslagen des SmartGrid aber auch nach einer besonderen Absicherung des Zweckbindungsgebotes gegen nicht legitimierte Messdatenverwendungen.

[43] Wobei es zu beachten gilt, dass diese Datenverwendung natürlich auch anonymisiert oder pseudonymisiert zu erfogen hat, wo dieses möglich ist.

[44] Vgl. Ernestus in Simitis, § 9 Rn. 34.

[45] BAG DB 1987, 1048, 1050.

Wegen der besonderen Sensibilität der Messdaten sollten bei den verantwortlichen Stellen im SmartGrid technische Mechanismen zur Sicherung der Zweckbindung (wie ein regelbasierter technischer Zugriffsschutz) implementiert werden.

Gleichzeitig wird zukünftig zu diskutieren sein, inwiefern Gefahren für das strenge Zweckbindungsgebot, welches die informationelle Selbstbestimmung flankierend sichert, beispielsweise durch Maßnahmen der Strafverfolgungsbehörden entstehen können. Denn schon heute kann beispielsweise anhand hoher gleichförmiger Stromabnahme eine Indizwirkung für die Existenz einer Beleuchtungsanlage zur Aufzucht von illegalen Hanfpflanzen vorliegen. Was regelmäßig staatliches Interesse auf sich zieht.

ERFORDERLICHKEIT

Das Prinzip der Erforderlichkeit verlangt, dass die Datenverarbeitung auf den für ihren Erhebungszweck notwendigen Umfang zu begrenzen ist. Das BDSG nimmt auf dieErforderlichkeit als Tatbestandsmerkmal ausdrücklich etwa in § 32 Abs. 1 BDSG Bezug. Die Vorschrift des § 32 Abs. 1 Satz 1 BDSG soll nach der Gesetzesbegründung den von der Rechtsprechung entwickelten allgemeinen Grundsätzen im Arbeitsverhältnis entsprechen.[46] Nach der Rechtsprechung ist eine Interessenabwägung unter Berücksichtigung des Verhältnismäßigkeitsprinzips der Maßstab für eine zulässige Datenverwendung im Arbeitsverhältnis.[47] Insofern ist die Konkretisierung der BDSG-spezifischen „Erforderlichkeit“ durch Interessenabwägung geboten.[48]Nach verbreiteter Ansicht ist eine Verarbeitung erforderlich, wenn legitime Ziele auf andere Weise nicht bzw. nicht angemessen erreicht werden können. Erforderlich sind somit nicht nur zwingend notwendige Verarbeitungen, sondern es ist auch zu berücksichtigen, ob es eine zumutbare Alternative gibt.[49] Die Datenverarbeitung muss „bei vernünftiger Betrachtung“[50]ein sinnvolles Mittel darstellen.[51] Dies ist einzelfallbezogen im Rahmen einer Abwägung festzustellen. Dabei gilt, dass ein Zusatzaufwand umso eher zumutbar ist, je schwerwiegender die Maßnahme ist.[52]

[46] BT-Drs. 16/13657, S. 21.

[47] Vgl. BAG DB 1987, 1048, 1049; NZA 2008, 1187, 1189; Schaffland/Wiltfang, § 28 Rn. 19.

[48] So auch Wybitul, BB 2010, 1085, 1086.

[49] Simitis in Simitis, § 28 Rn. 143; Gola/Schomerus, § 28 Rn. 34; Schaffland/Wiltfang, § 28 Rn. 110; Wedde, in: Däubler/Klebe/Wedde/Weichert, § 28 Rn. 48.

[50] Gola/Schomerus, § 28 Rn. 34

[51] Vgl. Gola/Schomerus, § 28 Rn. 34; Schaffland/Wiltfang, § 28 Rn. 110.

[52] Vgl. Globig in Roßnagel, Handbuch Datenschutzrecht, S. 648 Rn. 59

Aus der Perspektive der Erforderlichkeit stellt sich szenariospezifisch zunächst die Frage, ob das durch die Einführung von Smart Metern ermöglichte Fernauslesen der Messwerte überhaupt erforderlich ist. Jedenfalls Energiemanagement und Kontrolltätigkeit setzen im Smart Grid aktuelle Werte voraus. Zudem zeigen sich Einsparpotentiale für Verbraucher. Bei unterjährigen, ggf. monatlichen (vgl. § 40 Abs. 2 EnWG) Abrechnungszeiträumen überwiegt der finanzielle Aufwand in Folge des bei einem Auslesen vor Ort erforderlichen Personalaufwands deutlich. § 40 Abs. 2 Satz 1 EnWG stellt es zwar grundsätzlich ins Ermessen des Energieunternehmens, in welchen Abständen eine Abrechnung erfolgen soll. Ermessensleitend ist aber zu berücksichtigen, dass die Abrechnung gem. Art. 13 Abs. 2 Satz 3 der Energieeffizienzrichtlinie auf der Grundlage des tatsächlichen Verbrauchs so häufig durchzuführen ist, dass die Kunden in der Lage sind, ihren eigenen Energieverbrauch zu steuern. Dies erfordert eine Abrechnung in kurzen Intervallen. Der finanzielle Mehraufwand bei einem Auslesen vor Ort dürfte auf den Verbraucher umgelegt werden und dazu führen, dass die umweltpolitisch gewünschte wirtschaftliche Anreizfunktion intelligenter Messsysteme konterkariert wird. Daneben ist das Fernauslesen auch angemessen, da die mit dem Einsatz von Smart-Metern verfolgten Zwecke auf Fernauslesen angewiesen sind, das Fernauslesen auch für den Betroffenen u.a. wirtschaftlich Sinn macht und regelmäßig vertraglich vereinbart sein bzw. als Kalkulationsgrundlage den vertraglichen Vergütungssätzen zu Grunde liegen wird.

Sodann ist im Referenzszenario zu fragen, welche Daten zur Abrechnungserstellung erforderlich sind. Benötigt werden hier abrechnungsrelevante Daten. Ist beispielsweise ein tageszeitvariabler Tarif vereinbart, sind für die Abrechnung auch Messdaten erforderlich, die Auskunft über den Verbrauchszeitraum (Datum und Uhrzeit) geben. Der jeweilige Tarif gibt somit vor, welche Daten erhoben werden müssen. Ein dynamischer Echtzeittarif setzt insofern voraus, dass ausreichend Informationen für effizientes Energiemanagement zur Verfügung stehen.

Schließlich stellen sich noch die Fragen nach den Ableseintervallen und der zeitlichen Auflösung von Lastprofilen. Grundsätzlich geht das ULD-SH hier davon aus, dass die Erstellung detaillierter und individueller Lastgänge bei Letztverbrauchern in stündlichen, 15 minütigen oder geringeren Zeitintervallen nur mit der ausdrücklichen Einwilligung oder auf Grundlage eines Vertrages i. S. d. § 28 Abs. 1 Nr. 1 BDSG zulässig ist. Für dessen Erfüllung müsse es erforderlich sein, in den genannten Zeitintervallen die entnommene Energie zu erfassen.[53] Die Verknüpfung von Tarifstruktur und Erforderlichkeit der Erhebung kann sich aber z. B. mit den Bedürfnissen von Fehlerkontrolle und Energiemanagement als nicht verträglich erweisen. Sofern das ULD in seiner Stellungnahme ausführt, „Existieren z. B. nur drei tageszeitabhängige Preisunterschiede pro entnommener kWh, ist der Verbrauch nur für den jeweiligen Zeitraum insgesamt und nicht kleinteiliger zu erheben“[54], kann dies zu Kollisionen führen. Denn sowohl Energiemanagement als auch Fehlerkontrolle setzen aktuelle Daten voraus. Dies dient zugleich der Datensicherheit und damit dem Schutz des Betroffenen. Insofern kann jedenfalls gelegentlich ein Auslesen in kürzeren Intervallen sinnvoll sein. Werden Messwerte in größeren Abständen fernausgelesen, werden zahlreiche Daten in einem Vorgang transportiert. Ein unzulässiger Zugriff auf die hierbei verwendete Datenverbindung könnte somit einen erheblichen Datenbestand abfangen. Werden die Daten hingegen zeitnah nach ihrer Speicherung transportiert, sind bei einem rechtswidrigen Zugriff lediglich Einzelinformationen

[53] ULD-SH, S. 11.

[54] ULD-SH, S. 12.

verfügbar, die kaum aussagekräftig sind und insbesondere keine Profilbildung erlauben. Bei einem „Leck“ in der Datenverbindung wird zudem Zeit benötigt, um die Sicherheit wieder herzustellen. Der dafür erforderliche Zeitraum birgt ein deutlich geringeres Gefahrenpotential, wenn lediglich kleine Informationseinheiten transportiert werden.

Für sich betrachtet aussagearme kleine Informationseinheiten können nach dem Fernauslesevorgang in Hochsicherheitszonen effektiv gegen unbefugten Zugriff geschützt werden. Eine Differenzierung dahingehend, welche Zwecke jeweils mit dem Auslesevorgang verfolgt werden, würde dazu führen, dass Messgeräte eine entsprechende Unterscheidbarkeit technisch umsetzen müssten. Dies würde technisch hochkomplexe Messgeräte erfordern. Mit der technischen Mächtigkeit von Messeinrichtungen steigt aber zugleich das Angriffspotential.

Bei der Beurteilung der Erforderlichkeit einer konkreten Datenverwendung müssen im Smart Grid regelmäßig auch Wechselwirkungen mit technisch bedingten Notwendigkeiten der Datensicherheit oder die Auswirkung auf die Realisierungschancen von Folgeszenarien bedacht werden.

DATENSPARSAMKEIT

Die in § 3a BDSG formulierten Prinzipien der Datenvermeidung und Datensparsamkeit sind Schlüsselprinzipien des Datenschutzes auch für das Smart Grid. Daten, die nicht erhoben werden, können auch nicht unrechtmäßig Verwendung finden. Nach § 3a BDSG haben sich daher „Gestaltung und Auswahl von Datenverarbeitungssystemen [...] an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.“ Technische Systeme sollen also so gestaltet werden, dass die Erhebung und Verwendung personenbezogener Daten begrenzt und im besten Falle ganz vermieden werden kann.[55] Hierbei bedeutet Datenvermeidung entgegen dem Wortlaut allerdings nicht die Vermeidung von Daten schlechthin, sondern nur die Vermeidung des Personenbezuges der Daten.[56]

Das durch diese Regelung verfolgte Ziel besteht darin, möglichst wenig schützenswerte personenbezogene Daten überhaupt erst entstehen zu lassen und damit die Datenschutzrisiken bereits an deren Quelle zu minimieren.[57]Als Erforderlichkeitsmaßstab konkretisiert das Gesetz, dass dies nach dem Verwendungszweck möglich sein solle und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. Für die Beurteilung wiederum ist mithin die konkrete technische Ausgestaltung und die wirtschaftliche Vertretbarkeit in angemessenen Ausgleich zur Gefahranlage zu bringen. Hierfür wiederum ist die konkrete technische Ausgestaltung von besonderer Relevanz. Gerade durch eine geeignete Ausgestaltung von Kommunikations- Speicher- und Verarbeitungsstrukturen lässt sich das Ausmaß der möglichen Einschränkungen für das informationelle Selbstbestimmungsrecht signifikant reduzieren. Explizit verpflichtet § 3a BDSG

[55] Gola/Schomerus, § 3a, Rn. 4

[56] Roßnagel/Jandt, S. 14

[57] Bizer in Simitis, § 3a, Rn. 27.

insbesondere dazu, „von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, (…)“ wo immer dies mit angemessenem Aufwand möglich ist. Dieses Gebot gilt immer, unabhängig vom Bestehen eines Legitimationstatbestandes für die Datenverarbeitung. Im Kern soll es daher nicht darum gehen, technische Entwicklungen zu blockieren, sondern den **Prinzipien der strikten Datensparsamkeit und der Datenvermeidung, die im deutschen Datenschutzrecht verankert sind, auch bei der Gestaltung des Smart Grid Geltung zu verschaffen**.[58] Für die praktische Umsetzung im Rahmen des Smart Grid bedeutet dies:[59]

> Wo immer es möglich ist, ist auf die Erfassung, Verarbeitung, Übermittlung etc. von (Mess-) Daten gänzlich zu verzichten.Wo immer es nach dem Verwendungszweck möglich ist und keinen unverhältnismäßigen Aufwand erfordert, sollten (Mess-) Daten anonymisiert oder pseudonymisiert werden.

ANALYSE

In Bezug auf die so skizzierte Datensparsamkeit stellt sich für die Ausgestaltung des Smart Grid insbesondere die Frage, in welchem Umfang und in welcher Form Messdaten vom Smart Meter erhoben und übermittelt werden. Die derzeitigen Planungen sehen hier vor, dass hochaufgelöste Verbrauchsdaten über Zeiträume von 15 Minuten oder kürzer zumindest innerhalb des Zählers gebildet werden. Die hierbei entstehenden Datenmengen sind ungleich größer als im bisherigen Vorgehen. Eine solche Auflösung gilt jedoch allgemein als erforderlich, um lastvariable Tarife in marktauglicher Art und Weise zu realisieren (vgl. oben: Erforderlichkeit). Es ist jedoch fraglich, ob die Verbrauchsdaten auch in dieser detaillierten Form an den MSB/MDL übermittelt werden müssen.

Grundsätzlich denkbar wäre hier auch eine Alternative, bei der die Verbrauchsdaten bereits im Smart Meter den unterschiedlichen Tarifen zugeordnet und dann lediglich in aggregierter Form an den MSB/MDL geschickt werden. Hierzu müsste jedoch innerhalb des Smart Meters bekannt sein, wann welcher Tarif aktiv ist, damit die entsprechenden Messdaten dann einem bestimmten Tarif zugeordnet werden können. Für einfache Tarifstrukturen (beispielsweise Tag- und Nachtstrom mit festen Wechselzeiten) mag ein solches Vorgehen praktikabel erscheinen, komplexe Szenarien, bei denen beispielsweise selbst die Tarifstufen nicht im Vorhinein festgelegt, sondern allein von der jeweiligen Angebots- und Nachfragesituation abhängig sind, lassen sich aber voraussichtlich nur äußerst schwer mittels Preiszuordnung und Aufsummierung im Zähler realisieren. Die Tatsache, dass elektronische Zähler und alle weiteren Einrichtungen, die beispielsweise abrechnungsrelevante Aufsummierungen realisieren, umfangreichen Eichpflichten unterliegen[60], würde ein solches Vorgehen

[58] Berliner Beauftragter für Datenschutz und Informationsfreiheit, Jahresbericht 2009, S. 18. http://www.datenschutz-berlin.de/attachments/669/Jahresbericht_2009.pdf?1269595949 [10.05.2010].

[59] Vgl. auch Roßnagel/Jandt, S. 27.

[60] Vgl. hierzu beispielsweise die Ausführungen zu Zusatzeinrichtungen und Neuen Messwerten in den „Anforderungen an elektronische und softwaregesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität , Gas, Wasser und Wärme “ der PTB, PTB-A 50.7. Online über http://www.ptb.de/de/org/q/q3/q31/ptb-a/ptb-a.htm [10.05.2010].

weiter erschweren. Und nicht zuletzt würde ein kategorischer Verbleib der Messdaten im Haushalt zudem die Einbindung neuer, innovativer Akteure in den Energiemarkt behindern.

Aus diesen Gründen ist derzeit vorgesehen, dass die Smart Meter komplette Lastgänge in Viertelstundenwerten an den MSB/MDL übermitteln. Die Zuordnung der verbrauchten kWh zu den jeweils angebotenen Tarifen erfolgt dann beim Lieferanten (im Falle eines einzelnen Netznutzungsvertrages des Kunden auch zum Zwecke der Abrechnung der Netznutzung beim VNB). Der Lieferant erstellt auf Basis der hochaufgelösten Messdaten die monatliche Stromabrechnung für den Kunden. Nicht abschließend geklärt ist derzeit noch die Frage, ob der MSB/MDL oder der Lieferant dem Kunden zudem aus eichrechtlichen Gründen (Nachvollziehbarkeit) die kompletten Messdaten zur Verfügung stellen muss – voraussichtlich wird aber auch dies der Fall sein.

Soweit die hochaufgelösten Messwerte nicht nur zu Zwecken der Abrechnung mit dem Lieferanten, sondern beispielsweise auch für das Netzmanagement durch die jeweiligen Netzbetreiber oder für zusätzliche Energiedienstleistungen verwendet sollen, ist ein Personenbezug der Daten in aller Regel nicht erforderlich. Daher können Messdaten nicht ausschließlich zwischen Zähler und MSB/MDL übermittelt werden, sondern müssen zumindest grundsätzlich auch an Dritte (Lieferant, Energiedienstleister, Verteilnetzbetreiber) übermittelt und durch diese eingesehen werden können.[61] Ein bereits heute relevantes Beispiel hierfür ist die von der BNetzA vorgegebene zweistufige Übermittlung an den Lieferanten.[62] Hierbei werden die Messdaten nicht direkt vom Zähler an den Lieferanten gesandt, sondern in einem ersten Schritt von einem Messstellenbetreiber erhoben und durch diesen an den lokalen Netzbetreiber übertragen, der die Daten daraufhin an den jeweiligen Lieferanten weiterleitet. Alternativ können die Messdaten auch vom Messstellenbetreiber direkt sowohl an den lokalen Netzbetreiber als auch an den Lieferanten übermittelt werden. In beiden Fällen erhalten Messstellenbetreiber und lokaler Netzbetreiber damit ebenfalls Kenntnis von denjenigen Verbrauchsdaten, die an den Lieferanten zu übermitteln sind.

In ähnlicher Weise stellt sich das Problem für nahezu alle zukünftig zu erwartenden zusätzlichen Dienstleistungen im Smart Grid dar. Unabhängig von den konkreten, heute nur bedingt absehbaren Zusatzdiensten wird die Verfügbarkeit hochaufgelöster Messdaten in den meisten Fällen zwingende Voraussetzung für die Erbringung solcher Dienstleistungen darstellen. Wie oben ausgeführt, ist zwar regelmäßig davon auszugehen, dass hierfür grundsätzlich eine rechtliche Grundlage existiert. Die skizzierten Prinzipien von Datenvermeidung und Datensparsamkeit sind aber auch hier einzuhalten. Bislang werden diese in den laufenden Planungen noch nicht in der gebotenen Art und Weise berücksichtigt.

Beispielhaft sei hier die Übermittlung hochaufgelöster Messdaten zum Netzbetreiber betrachtet. Dieser benötigt die Messdaten zum einen für ein möglichst effektives Netzmanagement und zum anderen für die Abrechnung von Netznutzungsentgelten gegenüber dem jeweiligen Lieferanten. **Das Netzmanagement lässt sich allerdings auch auf Basis zwar hochaufgelöster, aber aggregierter und**

[61] Auf welchem Weg und in welchen Datenformaten die Übermittlung an Dritte geschieht ist hier nur von sekundärer Bedeutung und soll daher nicht weiter diskutiert werden.

[62] Vgl. zum aktuellen Stand die Prozessdefinitionen der BNetzA in den Konsultationen zum Festlegungsverfahren zur Standardisierung von Verträgen und Geschäftsprozessen im Bereich des Messwesens, BK6-09-034 / BK7-09-001 , Messstellenbetreiber- und Messdienstleisterprozesse bei Strom und Gas, S. 122 ff. Stand: 23.02.2009, Online über http://www.bundesnetzagentur.de [10.05.2010].

damit anonymisierter Messdaten einzelner Straßenzüge bzw. Netzsegmente realisieren.[63]**Für die Abrechnung von Netznutzungsentgelten wiederum ist lediglich erforderlich, dass der Netzbetreiber die jeweiligen Messdaten einem Lieferanten zuordnen kann, eine Zuordnung zu einem einzelnen Kunden ist hierfür nicht erforderlich**. **In beiden Fällen sind somit grundsätzlich keine Messdaten mit explizitem Personenbezug erforderlich und auch ein impliziter Personenbezug auf Basis einer eindeutigen Zählpunktbezeichnung ist nicht notwendig.**

Den oben skizzierten Prinzipien folgend ergibt sich aus der Nicht-Erforderlichkeit eines expliziten oder impliziten Personenbezugs damit die **Pflicht zur anonymen oder pseudonymen Übermittlung der Messdaten an den Netzbetreiber**. **Insbesondere widersprechen solche Systemgestaltungen und Kommunikationsprozesse dem Prinzip von Datenvermeidung und Datensparsamkeit, bei denen der Netzbetreiber Einblick in hochaufgelöste Messdaten erhält, die mit einer Klartext-Zählernummer oder einer anderen, den Personenbezug herstellenden ID attributiert sind. In analoger Weise gilt dies auch für alle weiteren Prozesse der Erhebung, Verarbeitung etc. von (Mess-)Daten bei der Einbindung von zusätzlichen Akteuren wie Optimierungsdienstleistern oder Demand-Side-Managern. Systemgestaltungen, die auf zentralen Datenbanken aufbauen, in denen alle Mess-daten in personenbezogener Form abgelegt sind und bei denen lediglich der Zugriff auf diese Daten eingeschränkt ist, werden dem Vermeidungs- und Sparsamkeitsgebot ebenfalls nicht gerecht**.

Obwohl die diesbezüglichen rechtlichen Vorgaben klar formuliert sind, werden sie in den derzeitigen Planungen und Entwicklungen der unterschiedlichen Modellprojekte noch nicht angemessen berücksichtigt. Für eine nachhaltige Systemgestaltung ist dies jedoch unerlässlich, da andernfalls eine Übernahme der entsprechenden Systemarchitekturen in den Regelbetrieb nicht möglich wäre. Spätestens hierfür müssten die derzeit vorherrschenden Konzepte für die Erhebung, Verarbeitung etc. personenbezogener (Mess-)Daten im Smart Grid entweder verworfen oder aufwändig modifiziert werden.

HANDLUNGSBEDARF

Um zu vermeiden, dass die im Rahmen der Modellprojekte entwickelten Architekturen zu einem späteren Zeitpunkt aufwändig überarbeitet werden müssen, sollte in den einzelnen Projekten zeitnah diskutiert werden, wie das in § 3a BDSG kodifizierte Vermeidungs- und Sparsamkeitsgebot angemessen berücksichtigt werden kann.

Insbesondere sollten hierbei die bisherigen Systementwürfe auf Möglichkeiten überprüft werden, auf die **Erhebung, Verarbeitung und Übermittlung personenbezogener Daten gänzlich zu verzichten oder die entsprechenden Daten durch Aggregation zu anonymisieren**. So stellt sich regelmäßig die Frage nach der Übertragung gerätespezifischer Daten an Netzbetreiber oder insbesondere Optimierungsdienstleister bzw. Demand-Side-Manager. Eine Übertragung solch hochgradig detaillierter Daten würde dem Datensparsamkeitsgebot grundlegend widersprechen. **Eindeutig vorzuziehen wäre hier die Übermittlung aggregierter Werte für den gesamten Haushalt**. Gerätespezifische Steuersignale lassen sich ebenfalls innerhalb eines Haushalts durch eine entsprechende Steuereinheit realisieren, die lediglich auf vom Anbieter oder Netzbetreiber übermittelte Preissignale oder andere

[63] Ähnlich auch Roßnagel/Jandt, S. 29.

Anreize reagiert und keine detaillierten, gerätespezifischen Daten nach außen liefert.[64] Ähnliches gilt auch für die oben diskutierte Übertragung und Nutzung hochaufgelöster Messdaten zum Zweck des Netzmanagements. Auch hier würde eine haushaltsspezifische Übertragung dem Sparsamkeitsgebot widersprechen und eine Übertragung von durch Aggregation anonymisierten Daten wäre eindeutig vorzuziehen.

Für eine Vielzahl von Anwendungsfällen (z. B. Netzmanagement, zusätzliche Energiedienstleistungen an Kundenpools oder virtuelle Kraftwerke) ist ein Personenbezug von übermittelten und verarbeiteten Messdaten nicht zwingend erforderlich. In diesem Fällen sind die Daten frühestmöglich zu anonymisieren. Insbesondere ist hierbei von der Übermittlung und Verarbeitung aggregierter Messdaten Gebrauch zu machen.

Für andere Anwendungsfälle kann jedoch eine eindeutige Zuordnung von Daten zu einer bestimmten Person zum Beispiel zu Abrechnungszwecken zwingend erforderlich sein. Eine Anonymisierung der Daten scheidet in diesen Fällen aus prinzipiellen Gründen aus. Hier ist jedoch, soweit möglich, zumindest von den Möglichkeiten der Pseudonymisierung nebst möglichst später Auflösung der Pseudonyme Gebrauch zu machen, um zu verhindern, dass in die Übermittlung eingebundene dritte Parteien (wie z. B. Netzbetreiber bei der derzeit von der BNetzA vorgegebenen Übermittlung an den Lieferanten) Einblick in personenbezogene Daten erhalten. In diesem Zusammenhang ist insbesondere auch an die Verwendung temporärer und möglicherweise von einer zu etablierenden vertrauenswürdigen dritten Instanz (TrustedThird Party) ausgestellter Pseudonyme zu denken.

In Fällen, in denen ein Personenbezug von Daten zwingend notwendig ist, muss die Übertragung und Verarbeitung weitestmöglich in pseudonymisierter Form erfolgen. Um eine Langzeit-Profilierung durch unberechtigte Parteien auszuschließen, müssen hierzu temporäre Pseudonyme verwendet werden. Mittelfristig ist für die Generierung dieser temporären Pseudonyme auch die Etablierung einer TrustedThird Party zu diskutieren.

Gleichwohl stellt sich sodann die Frage, ob es reicht, wenn Messwerte unmittelbar nach dem Fernauslesen zweckspezifisch aggregiert, pseudonymisiert bzw. anonymisiert werden oder ob diese Vorgänge bereits durch die Messgeräte vorgenommen werden müssen.

Aus Gründen der **Ende-zu-Ende Datensicherheit wäre eine Pseudonymisierung der Daten an der Stelle der Entstehung geboten**. Dies bedeutete die **Integration von Pseudonymisierungseinheiten in elektronische Zähler oder unter bestimmten Voraussetzungen auch in die vorgesehenen Multi Utility Communication Units (MUCs)**. Hierbei wäre jedoch zu beachten, dass eine Pseudonymisierung aus eichrechtlicher Sicht nach derzeitigem Stand eine Bildung neuer Messwerte darstellen und die die Pseudonymisierung umsetzende Einrichtung damit dem Eichrecht unterliegen würde. Im Fall einer aus **Datenschutzsicht wünschenswerten Pseudonymisierung in Zähler oder MUC müssten demnach die entsprechenden Pseudonymisierungseinheiten ebenfalls eichrechtlich geprüft werden. Dies würde zwar einen gewissen Aufwand erfordern, würde aber andererseits erstmalig**

[64] Vgl. auch Roßnagel/Jandt, S. 28.

eine obligatorische technische Prüfung datenschutzrelevanter Komponenten umsetzen. Es wäre dann zu diskutieren, inwiefern entsprechende vereinheitlichende Vorgaben zur Pseudonymisierung Eingang in den bestehenden eichrechtlichen Rahmen finden müssen. Mittelbar würde das Eichrecht damit sicherstellen, dass nur solche Messgeräte in Umlauf gebracht werden können, die dem Vermeidungs- und Sparsamkeitsgebot des § 3a BDSG tatsächlich gerecht werden.

Gegen eine Erweiterung der technischen Funktionalitäten von Zähler oder MUC könnte neben dem eichrechtlichen Aufwand sprechen, dass eine zweckspezifische Aggregation, Pseudonymisierung und Anonymisierung durch Messgeräte selbst erhebliche Anforderungen an die Technikgestaltung stellt. Die Geräte müssten in Abhängigkeit von den jeweils verfolgten Zwecken Messwerte unterschiedlichen Verwendungszusammenhängen zuordnen und unterschiedliche Funktionen ausführen können. Die Aggregationsparameter müssten zudem tarifabhängig konfiguriert werden. Die dann erforderliche Funktionsvielfalt würde technisch mächtige Geräte erfordern, die u.U. ein leichteres Angriffsziel für Fernsteuerungsmaßnahmen darstellen würden. Sicherer könnte es insofern sein, die Daten in kleinen Einheiten über eine unter Berücksichtigung des Standes der Technik sichere Verbindung zu transportieren und sie im Anschluss daran beim MSB/MDL im Rahmen einer (möglicherweise mit Mitteln des Trusted Computing) gesicherten Umgebung verwendungsspezifisch zu trennen („informationelle Gewaltenteilung“) und zu verändern (aggregieren, pseudonymisieren, etc.). Hier würde jedoch das beim MSB/MDL betriebene System aller Voraussicht nach der beschriebenen Eichpflicht unterliegen.

Für eine solche Lösung spricht zudem eine aktuelle Forsa-Umfrage.[65] Diese kommt zu dem Ergebnis, dass als Nachteile für den Einsatz von digitalen Zählern gleich nach dem Datenschutz zusätzliche Kosten genannt werden. Da die klimapolitischen Vorteile der Smart Meter aber nur dann greifen können, wenn auch die Bereitschaft der Nutzer zum Einbau der Geräte vorhanden ist, könnte gegen die datenschutzrechtlich ideale Lösung das **Kostenargument** der teuren Technikgestaltung im Smart Meter vorgebracht werden.

Aus Sicht der erstrebten Energieeffizienz ist weiterhin zu bedenken, dass ein flächendeckender Einsatz von Smart Metern gegenüber herkömmlichen Zählern zwar grundsätzlich ein erhebliches Energieeinsparungspotential bietet.[66] **Technisch komplexere Geräte erhöhen jedoch den Strombedarf deutlich und vereiteln somit die umweltpolitisch gewünschte Senkung des Strombedarfs**. In diesem Zusammenhang könnte auch zu berücksichtigen sein, dass eine technisch komplexe Lösung die Wettbewerbsfähigkeit im europäischen Vergleich in Frage stellen könnte. Da es aufgrund des Kompetenztitels zu den Zielen der DSRL zählt, in den Mitgliedstaaten ein einheitliches Schutzniveau zu gewährleisten, um die Ausübung von Wirtschaftstätigkeiten zu fördern und unverfälschten Wettbewerb zu ermöglichen (vgl. EG 7 f. DSRL), ist insofern ein einheitlicher europäischer Standard erforderlich.

Die Entscheidung für den einen oder anderen Weg würde insofern vom normativ gebotenen Gesamtkonzept der Datensicherheit im Smart Grid abhängen. Aus alleiniger Datenschutzsicht wäre fraglos eine Pseudonymisierung bereits im Zähler oder in der MUC vorzugswürdig. Unter

[65] Vgl. Verbraucherzentrale Bundesverband/Forsa, Vor- und Nachteile digitaler Stromzähler, http://www.neue-energieanbieter.de/data/uploads/20100510_vzbv_studie_presseinfo_%5Bkompatibilitaetsmodus%5D.pdf [11.05.2010]

[66] Benz, ZUR 2008, 457, 459.

Einbeziehung weiterer Aspekte ließe sich jedoch auch für eine unterschiedlich granulare Pseudonymisierung beim MSB/MDL argumentieren, sofern für die Übertragung zwischen Zähler/MUC und MSB/MDL eine hinreichend sichere Verbindung angenommen werden kann und die Pseudonymisierung beim MSB/MDL im Rahmen einer (eichrechtlich) zertifizierten, mit Mitteln des Trusted Computing gesicherten Infrastruktur erfolgte.

Wegen der Bedeutung eichpflichtiger Einrichtungen für den Datenschutz im Smart Grid sollte die Integration bereichsspezifischer Vorgaben zur datenschutzfreundlichen Technikgestaltung in dem derzeitigen eichrechtlichen Rahmen diskutiert werden. Es sollten aus Gründen der Planungssicherheit zügig Vorgaben für die Gerätehersteller normiert werden.

Alternativ zur Pseudonymisierung in Zähler oder MUC sollte auch die Integration von Pseudonymisierungsinfrastrukturen beim MSB/MDL diskutiert werden. Hierfür sprechen insbesondere Erwägungen zur Komplexität von Zähler und MUC und zu dem daraus erwachsenden zusätzlichen Aufwand.

Die von der BNetzA formulierten Prozessvorgaben zur Datenübermittlung gehen primär von der derzeitigen Marktrollenverteilungin der Energiewirtschaft aus. So ist für die Übermittlung von Messwerten vom MSB/MDL zum Lieferanten vorgesehen, dass die Daten grundsätzlich über den jeweiligen lokalen Netzbetreiber laufen.[67] Selbst bei Umsetzung der oben skizzierten Pseudonymisierung wäre hier im Sinne der Datensparsamkeit eine direkte Übertragung der personenbezogenen Daten vom MSB/MDL zum Lieferanten und eine aggregierte Übermittlung an den Netzbetreiber, die der Tarifierung angepasst ist, vorzuziehen.

Überlegungen zur datenschutzfreundlichen Gestaltung des Smart Grid müssen auch Berücksichtigung in den regulatorischen Vorgaben der BNetzA zu Prozessen und Datenformaten finden. Der derzeitige Stand der Festlegungen führt zu zwingend suboptimalen Systemgestaltungen und sollte im Sinne von Datenvermeidung und Datensparsamkeit im Smart Grid überdacht werden.

TRANSPARENZ

Die Erhebung und Verarbeitung personenbezogener Daten muss gegenüberdem Betroffenen transparent sein. Das Transparenzprinzip folgt dem Inhalt des informationellen Selbstbestimmungs-

[67] BNetzA, Konsultationen zum Festlegungsverfahren zur Standardisierung von Verträgen und Geschäftsprozessen im Bereich des Messwesens, BK6-09-034 / BK7-09-001, Messstellenbetreiber- und Messdienstleisterprozesse bei Strom und Gas, S. 122 ff. Stand: 23.02.2009, Online über http://www.bundesnetzagentur.de [10.05.2010].

rechts. Der Betroffene soll wissen können, wer was über ihn weiß. Die Regeln zur Transparenz unterscheiden sich in Informationspflichten, bei denen die verantwortliche Stelle von sich aus aktiv werden muss, und dem Auskunftsanspruch, den der Betroffene selbst geltend machen muss.[68]

ANALYSE

Im Referenzszenario gilt es im Hinblick auf die Transparenz insofern, den bereits erörterten Grundsatz der Direkterhebung beim Betroffen zu verwirklichen. Dies bezieht sich insbesondere auf die Mitwirkung und die Pflichtinformationen aus § 4 Abs.3 BDSG. Da durch die Möglichkeit einer vom Betroffenen unbemerkten Datenerhebung eine erhebliche Gefährdung für dieses Prinzip entsteht, auf der anderen Seite aber ein informatorischer Overhead vermieden werden sollte, ist es naheliegend schon in einer sehr frühen Phase des Vertragsschlusses dem Betroffenen Klarheit über Intervalle und Strukturen der Datenverwendung Klarheit zu verschaffen. Dazu können diesbezügliche Inhalte sinnvoll in die Vertragsgrundlagen aufgenommen werden.[69]

Zur Herstellung von Transparenz über die Messverfahren und der Datenübermittlungen für den Anschlussinhaber wird deshalb empfohlen, die Ablesezeitpunkte und Ableseintervalle mit den Betroffenen vertraglich zu vereinbaren.

Daneben wird für die Fälle der Erstellung von Lastprofilen durch den Messstellenbetreiber zu Abrechnungszwecken angeregt, dass der Nutzerin regelmäßigen Abständen zu informieren ist oder die Möglichkeit erhält, die erfassten Daten jederzeit einzusehen[70]. Es sollte im Eigeninteresse der Marktakteure liegen, im Sinne einer breiten Akzeptanz der Smart Meter hier für größtmögliche Klarheit beim Anschlussnutzer zu sorgen.

HANDLUNGSBEDARF

Insgesamt steht das derzeitige System der Absicherung des datenschutzrechtlichen Transparenzgebotes mit seinen vielfältigen Detailinformationen, die sich in der informierten Einwilligung des § 4a BDSG oder den Informations- und Nutzerrechten einfachrechtlich ausdrücken, wie auch bei anderen komplexen Systemgestaltungen des allgegenwärtigen Rechnens, auch im Smart Grid zur Revision an. Bei der vergleichbaren RFID-Problematik[71]stehen in diesen Systemen, die das menschliche Leben zukünftig durch stetige hochfrequente Datenverarbeitung in Hintergrundsystemen begleiten werden, das unbemerkte Rechnen nach dem Prinzip „Calm“, welches für den Nutzer Vorteile generieren kann, und auf der anderen Seite das Transparenzgebot in einem Spannungsverhältnis. **Wird der Mensch mit ständigen Pflichtinformationen über aktuelle Systemzustände und Verwendungszusammen-**

[68] Bizer, 2007, 350, 353 f.

[69] Vgl. Berliner Beauftragter für Datenschutz und Informationsfreiheit, Jahresbericht 2009, S. 19.

[70] ULD-SH, S. 12.

[71] Vgl. hierzu: Friedewald/Raabe/Georgieff/Koch/Neuhäusler, S. 205 ff.

hänge belastet, so wird der genannte Vorteil negiert oder es tritt eine Ermüdungshaltung gegenüber der Informationsflut ein. Insofern wird zu Recht konstatiert, dass die bisherigen Instrumente an subjektive Grenzen stoßen.[72]

Insofern ist zutreffend angemerkt worden, dass im Smart Grid in Zukunft zur Herstellung von Transparenz Strukturinformationen und Auskunft über den logischen Aufbau der automatisierten Verarbeitung der betreffenden Daten zu erteilen ist.[73]

In Zukunft sollte nach dem Vorbild des § 6a Abs.3 BDSG bereichsspezifisch bestimmt werden, dass die Marktakteure Auskünfte über Strukturinformationen zur Verarbeitung von personenbezogenen Daten erteilen müssen.

Dieser Ansatz wäre zudem mit dem schon im Rahmen der Einführung von RFID vorgeschlagenen Implementierung von Verfahren der Vorab-Datenschutzfolgenabschätzung verträglich, als in dieser Phase die notwendigen Strukturinformationen gesammelt werden könnten.[74]

Darüber hinaus können diese Strukturinformationen jedoch nicht den Anspruch des Betroffenen auf Auskunft über konkrete Datenverwendungen ersetzen,[75] da diese Informationen eher im vorwirkenden Bereich einer Datenverwendung den Betroffenen über grundsätzliche Gefährdungslagen informieren und kleinteilige Zwischeninformationen verhindern sollen. Gerade im Hinblick auf die Verwirklichung von Auskunftsansprüchen entsteht ein erheblicher Vorteil für die Nachvollziehbarkeit und Kontrolle von konkreten Anfragen über Datenverarbeitungsschritte in dem vorliegend konkretisierten Paradigma des „Privacy by Design“.[76] Sofern die notwendige Regelbasis technischer Mechanismen des Zugriffschutzes auch die Nutzerpräferenzen implementiert, kann insofern auf Basis von Maschine-Maschine-Kommunikation auf ständige Laufzeitinformationen des Anschlussnutzers verzichtet werden.

Sofern die Implementierung von regelbasierten Mechanismen des Zugriffsschutzes bei den Marktakteuren mit der Möglichkeit der Protokollierung von Anfragen und Verarbeitungsvorgängen normativ angeordnet würde, kann zukünftig die Durchsetzung von Auskunftsanprüchen der Betroffenen deutlich effektiviert und auf ständige Laufzeit-informationen verzichtet werden.

[72] Roßnagel in Taeger/Wiebe, S.62.

[73] Roßnagel/Jandt, S. 40.

[74] Vgl. hierzu: Friedewald/Raabe/Georgieff/Koch/Neuhäusler, S. 235 ff.

[75] A.A. offensichtlich Roßnagel/Jandt, S. 40

[76] Siehe folgender Abschnitt „Datensicherheit“.

Schließlich wird noch angeregt, dass bei einheitlichen Verarbeitungsvorgängen im Smart Grid auch einheitliche Datenschutzerklärungen zu den geplanten Datenverwendungen Einsatz finden sollten. Hierzu wären Verbändevereinbarungen nach § 38a BDSG ein gangbarer Weg.

DATENSICHERHEIT

In einem derart allgegenwärtigen, verteilten und hochkomplexen System wie dem zukünftigen Smart Grid kommt der Datensicherheit eine zentrale Rolle für die Gewährleistung eines angemessenen Datenschutzniveaus zu. Selbst unter weitgehender Beachtung des oben diskutierten Vermeidungs- und Sparsamkeitsgebotes wird die Menge der im Smart Grid anfallenden personenbezogene Daten weit über das bislang bekannte Maß hinausgehen. Für diese Daten sind entsprechend § 9 BDSG technische und organisatorische Maßnahmen zu ergreifen, um die in der entsprechenden Anlage 1 aufgeführten Kontrollziele zu erreichen. Angesichts der hochgradig verteilten Struktur des zukünftigen Smart Grid, der hohen Anzahl beteiligter Akteure und der zu erwartenden starken Interdependenzen zwischen diesen Akteuren erscheinen die etablierten organisatorischen Maßnahmen zunehmend ungeeignet zur Erreichung dieser Ziele. Dementsprechend werden vornehmlich technische Maßnahmen zu ergreifen sein, die hier diskutiert werden sollen. Wegen der gleichwohl auch notwendigen technisch–organisatorischen Schutzmaßnahmen im stationären Umfeld sei insofern hier auf einschlägige Stellungnahmen[77] verwiesen.

ANALYSE

Der Manipulationssicherheit der im Haushalt befindlichen elektronischen Zähler bzw. der auf diesen Zählern laufenden Software ist in der öffentlichen Diskussion eine besondere Aufmerksamkeit zugekommen. Insbesondere wurde hierbei das Risiko des Aufspielens modifizierter Firmware durch potentielle Angreifer thematisiert. Diesem Problem wird durch aktuelle elektronische Zähler bereits hinreichend Rechnung getragen. Insbesondere wird hier gewährleistet, dass Zähler nur solche Updates akzeptieren, die vom jeweiligen Hersteller signiert sind.[78] Das Vorgehen ist zwar primär aus dem Eichrecht motiviert, ein mögliches, sich aus dem unberechtigtem Aufspielen modifizierter Firmware durch einen Angreifer ergebendes Datenschutzrisiko wird dadurch aber ebenfalls auf ein Minimum reduziert und existiert zumindest in der öffentlich diskutierten Form somit nicht. Eine über die derzeitigen Spezifikationen hinausgehende Regelung für elektronische Zähler erscheint damit nicht notwendig.

Nach der Erhebung im elektronischen Zähler sollen die Messdaten an eine Multi Utility Communication Unit (MUC) übertragen und von dieser an den jeweiligen MSB/MDL übermittelt werden. Anders als für die Zähler selbst ist für diese MUCs nach derzeitigem Diskussionsstand eine

[77] Siehe z. B. Berliner Beauftragter für Datenschutz und Informationsfreiheit, Jahresbericht 2009, S. 19.

[78] Vgl. hierzu VDE, Lastenheft EDL, S. 39 f (online unter http://www.vde.com/de/fnn/arbeitsgebiete/messwesen/Seiten/zaehler.aspx [10.05.2010]) in Verbindung mit SyM^2, Pflichtenheft Synchronous Modular Meter, Version 1.03 (http://www.sym2.org/ [10.05.2010]). Zum genaueren Vorgehen mittels verketteter Firmware-Versionen siehe das Pflichtenheft SyM^2, S. 73 ff. Die hier vorgesehenen kryptographischen Verfahren (ECC, 192 bzw. 256 Bit) gewährleisten nach derzeitigem Stand der Technik ein auch auf längere Sicht ausreichendes Schutzniveau.

analoge Signierung von Firmware-Updates jedoch nicht explizit vorgesehen.[79] Da aber die MUC eine zentrale Rolle gerade in der Anbindung einzelner Haushalte an das Energieinformationsnetz spielt und zu einem späteren Zeitpunkt auch Steuerungsaufgaben übernehmen soll, ist eine solche analoge Signierung von Firmware-Updates auch hier zwingend notwendig.

Sowohl für die elektronischen Zähler als auch für die MUCs muss weiterhin sichergestellt werden, dass nur berechtigte Parteien Zugriff auf die Messdaten haben bzw. diese abrufen können.[80] Nach derzeitigem Entwicklungsstand ist hierzu ein Berechtigungskonzept auf Basis von Rollen, Nutzernamen und Passwörtern vorgesehen, mittels dessen sich innerhalb der MUC unterschiedliche Zugriffsberechtigungen beispielsweise für Netzbetreiber, MSB/MDL oder den Kunden selbst realisieren lassen.[81] Alternative Authentifikationsverfahren sind hier nach aktuellem Stand nicht vorgesehen.

Darüber hinaus ist der Datenzugriff bzw. die Kenntnisnahme durch unberechtigte Parteien auch bei der Übertragung der Messdaten zum jeweiligen MSB/MDL zu gewährleisten. Die Datenübermittlung muss daher in verschlüsselter Form erfolgen. Die derzeitige Vorgehensweise ergibt sich jedoch primär aus eichrechtlichen Erwägungen und stellt daher die Gewährleistung der Datenintegrität mittels Signaturen in den Vordergrund. Eine Verschlüsselung der Datenübertragung hingegen ist derzeit nicht explizit vorgesehen.[82] Bzgl. der nachgelagerten Datenübermittlungen (beispielsweise vom MSB/MDL zum lokalen Netzbetreiber, etc.) ist davon auszugehen, dass die verwendeten Datenverbindungen bereits im Zuge der üblichen Sicherheitsmaßnahmen in adäquater Weise (beispielsweise mittels VPN-Technologien auf Basis der schon derzeit existierenden Branchenstandards) verschlüsselt werden und dass für die Übertragungswege demnach keine weiteren Maßnahmen zum Schutz vor unbefugter Einsichtnahme durch Dritte erforderlich sind.

Dies gilt jedoch nicht für die nachgelagerten Datenverarbeitungssysteme bei weiteren zukünftig am Markt agierenden Dienstleistern. Da alle diese Parteien personenbezogene Daten speichern und verarbeiten werden, müssen für die entsprechenden Systeme ausreichende Schutzmaßnahmen ergriffen werden. Als absolutes Minimum sind hier geeignete Schutzkonzepte auf Basis etablierter Sicherheitsstandards zu erarbeiten und zu verfolgen.[83]Angesichts des immensen zu erwartenden Datenaufkommens, der hochgradig dezentralen und vernetzten Struktur sowie der hohen Anzahl an der Datenverarbeitung und -nutzung beteiligter Akteure sind die heute etablierten Mechanismen

[79] Gleichwohl erwähnt das entsprechende Lastenheft Multi Utility Communication in Version 1.0 (http://www.vde.com/de/fnn/arbeitsgebiete/messwesen/Seiten/muc.aspx [10.05.2010]) für den Prozess der Firmware-Aktualisierung explizit die Übermittlung einer „Signatur zur Autorisierung“ und legt damit einen analogen Mechanismus zum Schutz vor modifizierter Firmware zumindest nahe.

[80] So auch Roßnagel/Jandt, S. 35.

[81] Siehe VDE, Lastenheft Multi Utility Communication (Version 1.0), S. 42 f.

[82] Vgl. beispielsweise VDE, Lastenheft MUC, S. 22 f: „Eine Verschlüsselung der Übertragung ist nicht notwendig.“ Das Lastenheft erwähnt den Einsatz von Verschlüsselungsverfahren zwar sowohl für die Weitverkehrsschnittstelle (S. 45, hier insb. die Verwendung von VPNs) als auch für die lokale Kommunikation mit angeschlossenen Messeinrichtungen (S. 47), weitere Ausführungen hierzu existieren jedoch zumindest derzeit nicht.

[83] Insbesondere sei hier auf das Grundschutzhandbuch des BSI verwiesen.

jedoch kaum ausreichend, um einen angemessenen Schutz der im Smart Grid anfallenden personenbezogenen Daten zu gewährleisten.[84]

Eine besondere Herausforderung stellt schließlich noch die Sicherung der rechtmäßigen Datenverwendungen dar. Wie das Referenzbeispiel zeigt, sind zukünftig bei den jeweiligen Akteuren der Prozesskette eine Vielzahl von Entscheidungen zur Zulässigkeit und Granularität der Messdatenerhebung, Präsentation, Verarbeitung, und der Zulässigkeit von Datenverwendungen durch neue Akteure des Energieeffizienzmarktes zu treffen. Wie das in Teil II diskutierte Beispiel der Elektromobilität zeigt, sind allein die Entscheidungssituationen zur zulässigen und notwendigen Datenweitergabe beim elektromobilen Roaming so vielfältig, dass sie manuell nicht mehr beherrschbar sein dürften. Auch klassische Instrumentarien wie Vorabkontrolle, Verfahrensverzeichnisse, betrieblicher Datenschutz und Sanktionsandrohung dürften an der Komplexität der Systeme und Prozessvielfalt scheitern. Dieses klassische Schutzkonzept und organisatorisch ansetzende Maßnahmen für ein insofern gesichertes Zugriffs- und Kontrollregime wie die Nutzung des Vier-Augen-Prinzips und Instruktionen von Mitarbeitern könnten unter der Ägide des BDSG hier gleichwohl als hinreichend erachtet werden. Dieses Ergebnis kann aus datenschutzrechtlicher Perspektive nicht überzeugen, weshalb eine bereichsspezifische Konkretisierung zu diskutieren ist.

HANDLUNGSBEDARF

Die Schwerpunkte hinsichtlich des datenschutzrechtlichen Handlungsbedarfes in Sachgestaltungen des Smart Grid aus Perspektive der Datensicherheit liegen zum einen in dem Erfordernis neuer Konzepte der Informationssicherheit und auf der anderen Seite in der Konkretisierung des insofern unscharfen Begriffes von „Privacy by Design“.

INFORMATIONSSICHERHEIT

Aus der obigen Diskussion des derzeitigen Standes lässt sich zuallererst die Empfehlung ableiten, dass der Vorgang des Software-Updates für MUCs in der gleichen Art und Weise geschützt werden muss, wie dies derzeit schon für die elektronischen Zähler als solche vorgesehen ist. Zum einen verfügt die MUC potentiell über Zugriff auf unverschlüsselte Messdaten und leitet diese beispielsweise an den MSB/MDL weiter, zum anderen wird die MUC zu einem späteren Zeitpunkt möglicherweise auch Steuerungsfunktionen übernehmen. Beides setzt eine besondere Vertrauenswürdigkeit der MUC und somit auch der darauf laufenden Software voraus. Hierzu ist es notwendig, einer unberechtigten Modifikation der Firmware mit technischen Mitteln vorzubeugen. Das für elektronische Zähler vorgesehene Verfahren der signierten Firmware ist daher auch für MUCs anzuwenden. Die derzeitigen Spezifikationsdokumente schreiben einen solchen Mechanismus nicht explizit vor. Im Sinne eines einheitlich hohen Sicherheitsniveaus sollte das Verfahren jedoch auch für MUCs verpflichtend sein.

Die derzeitigen Spezifikationen für MUCs sehen zudem einen rollenbasierten Zugriffsschutz vor, mittels dessen sich unterschiedliche Berechtigungen beispielsweise für Netzbetreiber, Lieferanten und Kunden realisieren lassen. Hierbei ist jedoch ein passwortbasiertes Authentifikationsverfahren spezifiziert. Derartige Verfahren sind allerdings mit Risiken wie dem Verlust eines Passworts, der

[84] So auch Roßnagel/Jandt, S. 11 f, 41.

Wahl unsicherer Passwörter oder der Möglichkeit des Ausspähens verbunden. Angesichts der zu erwartenden Langfristwirkung einer solchen Festlegung sollte hier zumindest die Möglichkeit alternativer, modernerer Authentifikationsverfahren (Mehrfaktor-Authentifikation, Challenge-Response-Verfahren, etc.) diskutiert werden.

Für die Datenübermittlung vom Haushalt zum MSB/MDL wird in den derzeitigen Spezifikationen die Möglichkeit der Verschlüsselung zwar erwähnt, eine explizite Vorgabe oder Standardisierung hierzu existiert nicht. Eine sichere Datenübertragung ist aus Sicht des Datenschutzes jedoch unverzichtbar und sollte in den entsprechenden Spezifikationen als zwingend erforderlich aufgenommen werden.[85] Eine unverschlüsselte Übertragung von Messdaten ist nicht akzeptabel.

Das für elektronische Haushaltszähler standardisierte Verfahren zum sicheren Update der Firmware ist auch für MUCs zwingend vorzusehen und in die entsprechenden Spezifikationen aufzunehmen. Neben dem derzeitigen, passwortbasierten Verfahren für den Zugriff auf die MUC sollten auch alternative, fortgeschrittene Verfahren zumindest diskutiert werden. In den Spezifikationen zur MUC sollte eine angemessene Verschlüsselung der Datenübertragung zum MSB/MDL zwingend vorgeschrieben werden.

Die Verschlüsselung der Datenübertragung kann sich selbstverständlich nicht nur auf den Weg vom Kundenzum MSB/MDL beziehen, sondern muss in gleicher Art und Weise auch für alle weiteren Vorgänge der Datenübertragung gewährleistet werden. Das Risiko der Einsichtnahme durch unbefugte Dritte würde andernfalls nur auf andere Kommunikationsstrecken verlagert. Anders als für den Übertragungsweg vom Kunden zum MSB/MDL bestehen allerdings bereits branchenweit einheitliche Vorgehensweisen wie die entsprechenden Verbandsempfehlungen des BDEW.[86] Es ist zu diskutieren, inwiefern die entsprechenden Verfahren sich auch auf das Smart Grid abbilden lassen.

Auch der Datenverkehr zwischen den unterschiedlichen Marktakteuren muss in verschlüsselter Form erfolgen. Eine Anwendung bereits existierender diesbezüglicher Vorgehensweisen ist zu prüfen.

Bzgl. der Sicherheit der nachgelagerten Datenverarbeitungsanlagen bei MSB/MDL, Netzbetreiber, Lieferanten, etc. existieren in einigen Modellregionen bereits erste Ansätze übergreifender Sicherheitskonzepte, die beispielsweise auch den physischen Zutrittsschutz berücksichtigen. Die hierbei zu Grunde gelegten Annahmen und Vorgehensweisen sind jedoch noch nicht über die unterschiedlichen Modellregionen konsolidiert und somit schwer vergleichbar. Dies führt wiederum zu Unsicherheiten und Mehrfachaufwand sowohl auf Seiten der systemverantwortlichen Parteien als auch auf Seiten

[85] Diesbezüglich und im Hinblick auf die weiter oben erwähnten sicheren Software-Updates ist insbesondere das in der Modellregion E-DeMa derzeit in Entwicklung befindliche Common-Criteria Schutzprofil für IKT-Gateways zu erwähnen.

[86] Vgl. beispielsweise die „Studie über sichere webbasierte Übertragungswege“ des BDEW, online unter http://www.bdew.de/ [10.05.2010]

der Aufsichtsbehörden. Zumindest ein vereinheitlichtes Verständnis des zu realisierenden Schutzprofils würde die Arbeit auf allen Seiten deutlich erleichtern.

Angesichts der herausgehobenen Bedeutung der Sicherheit nachgelagerter Datenverarbeitungsanlagen ist eine modellregionenübergreifende Abstimmung und Konsolidierung von Grundannahmen und Schutzprofilen anzustreben.

PRIVACY BY DESIGN

Neben dem Datenschutz muss im Energiemarkt auch aus Gründen der informationellen Entflechtung und des Schutzes von Geschäftsgeheimnissen gewährleistet werden, dass bei einer Übermittlung der Messdaten nur der berechtigte Empfänger Kenntnis von diesen Daten erlangen kann. Die Notwendigkeit eines entsprechenden Geheimnisschutzes lässt sich dadurch illustrieren, dass im Falle einer IKT-gestützten Energieberatung die gerätegenaue Verteilung der Stromflüsse in einem Unternehmen auch Rückschlüsse auf die Unternehmenstätigkeit zulassen kann.

Sowohl der Geheimnisschutz als auch die datenschutzrechtlichen Obliegenheiten konnten im Rahmen des Systemdatenschutzes im klassischen Energiemarkt noch durch organisatorische Maßnahmen sichergestellt werden. Einerseits wird dem Geheimnisschutz für die hier interessierenden Fälle schonmittelbar durch organisatorische Maßnahmen im Rahmen der informatorischen Entflechtung beim Netzbetrieb nach § 9 Abs.1 EnWG Rechnung getragen.[87] Auf der anderen Seite konnte bislang mittels organisatorischer Maßnahmen nach § 9 BDSG, wie Instruktionen zum zulässigen Datenumgang, auch den datenschutzrechtlichen Obliegenheiten genügt werden, da aufgrund der langfristigen Ableseintervalle ein geringes Missbrauchsrisiko bestand. Wegen der geringen Anzahlmöglicher Empfänger der Messdaten und der gesetzlich fixierten Verarbeitungsschritte war dies nicht grundlegend in Frage zu stellen.

Angesichts der hochgradig dezentralen und komplexen Systemstruktur des zukünftigen Smart Grid, ist es fraglich, ob sich derzeit etablierte Sicherheitsmechanismen als nachhaltig erweisen können. Angesichts der bislang ungekannten Herausforderungen ist es daher angezeigt, auch neue Wege der Datensicherheit zu beschreiten, zumal sich mit dem Aufbau des Smart Grid die einmalige Chance ergibt, eine von Grund auf sichere und datenschutzfreundliche Infrastruktur zu schaffen.

Insbesondere ist hier die Möglichkeit zum breiten Einsatz von Technologien des Trusted Computing zu diskutieren. Schon der oben skizzierte Mechanismus der signierten Firmware-Updates für Zähler und MUC stellt im Kern eines der grundlegenden Konzepte des Trusted Computing dar. Im Sinne

[87] Vgl. BNetzA, Gemeinsame Richtlinien der Regulierungsbehörden des Bundes und der Länder zur Umsetzung der Informatorischen Entflechtung nach § 9 EnWG, S. 16, 2007, online unter http://bundesnetzagentur.de [10.05.2010].

einer vertrauenswürdigen Kommunikationsinfrastruktur[88] für das Smart Grid sollte eine breitere Verwendung derartiger Konzepte des Privacy by Design auch für die Kommunikation zwischen den Marktbeteiligten durchaus in Erwägung gezogen werden. Ob und inwieweit sich ein legislativer Handlungsauftrag für einen ggf. bereichsspezifisch geregelten Zwang zur Verwendung von technischen Mechanismen des Systemdatenschutzes aus den grundrechtlichen Schutzpflichten des Art. 2 Abs.1 i. V. m. Art. 1 Abs.1 GG verdichtet, muss noch weitergehend untersucht werden.

Die Einführung der Smart Meter ist eine Sachgestaltung, die in ihrer praktischen Konsequenz auf die Pflicht zur Verwendung von IKT-Infrastrukturen im Hausanschlussbereich hinausläuft. Es ist naheliegend, dem damit staatlich gesetzten Risiko einen korrespondierenden Sicherungsauftrag für die informationelle Selbstbestimmung zuzumessen, der insbesondere durch verbindliche Vorgaben für die Gestaltung der Systeme nach einem gesetzlich konkretisierten Prinzip „Privacyby Design“ erfüllt wird.

Im europäischen Kontext des Datenschutzes ist dabei zu beachten, dass der niederländische Parlament im April 2009 der im Gesetzentwurf enthaltenen Verpflichtung zur Verwendung von Smart Metern durch Endkunden gerade im Hinblick auf Datenschutzaspekte nicht zugestimmt hat.[89] Ein Datenschutzkonzept, welches in diesem grundrechtsrelevanten Bereich einen angemessenen Ausgleich im Sinne der Verwirklichung praktischer Konkordanz herstellen will, muss aber, wie schon die Erfahrungen bei der Einführung der RFID-Technologie zeigen, einen deutlichen Schwerpunkt in den Bereich des technischen Datenschutzes legen.[90]

In der Tat dürfte sich die Abwägung zwischen den berechtigten Schutzinteressen der Endkunden einerseits und den Interessen der datenverarbeitenden Stellen an einer möglichst ungehinderten Verwendung der Daten für eine Vielzahl von möglichen Auswertungen und Übermittlungen andererseits vor dem Hintergrund der gesteigerten Sensibilität der Messdaten verschieben. Die Bereitstellung von Mechanismen des technischen Zugriffsschutzes erfordert zwar einen anfänglichen Implementierungsaufwand, meidet aber die Schwächen des organisatorischen Datenschutzes, wie personelle Diskontinuität, fehlendes Rechtswissen und bewusste Ausnutzung von Schutzlücken.

Allerdings ergibt sich aus der bereits mehrfach angesprochenen Komplexität und den vielfältigen absehbaren Interdependenzen zwischen den beteiligten Akteuren eine nur eingeschränkte Tauglichkeit etablierter Zugriffsschutzmechanismen. Diese gehen grundsätzlich von der Existenz wohldefinierter Rollen und Zugriffsrechte aus und führen bekanntermaßen besonders in hoch-dynamischen Umfeldern mit häufig wechselnden Beteiligten, Relationen und nicht zuletzt rechtlichen Vorgaben zu Problemen. Wenn insofern in der Literatur vorgeschlagen wird, unter anderem eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffs-regime unter Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung

[88] Roßnagel/Jandt sprechen hier lediglich von einer „vertraulichen Kommunikationsinfrastruktur“.

[89] Vgl. beispielsweise http://vortex.uvt.nl/TILTblog/?p=54 [10.05.2010].

[90] Vgl. nur für den insofern vergleichbaren Bereich die „Stellungnahme des Europäischen Datenschutz-beauftragten zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Thema „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen“ (KOM(2007) 96) , ABl. C 101/1, S.7.

vorzusehen, würde in einer gesetzlichen Ausgestaltung derzeit genügen,[91] so kann dem nicht gefolgt werden.

Als vielversprechende Alternative und Kern einer Architektur nach den „Privacy by Design“-Prinzipien erscheinen hier Ansätze regelbasierter Zugriffssteuerungssysteme, mittels derer die Zuweisung von Zugriffsrechten für jedwede Datenverwendung bei den Marktakteuren weitgehend automatisiert werden kann. Zudem könnten regelbasierte technische Mechanismen des Zugriffschutzes eine unmittelbare Repräsentation des Nutzerwillens in dem technischen System und die zwingende Durchsetzung gesetzlicher Vorgaben wie Transparenz der Datenverarbeitung oder die Durchsetzung von gesetzlichen Nutzerrechten effektivieren. Verfahrensrechtliche Vorkehrungen wären insofern normativ zu installieren, als im Wege von kooperativen Verfahren, nach dem Vorbild der Festlegungen des § 21b EnWG, auf Basis von normativen Zielvorgaben, Vorschlägen der Verbände und betroffenen Kreise in technische Regelwerke überführt würden, die von den datenverarbeitenden Stellen des Energiemarktes verpflichtend als Regelbasis für eine gesicherte Zugriffssteuerung zu verwenden wären. Ein solches Verfahren würde im Hinblick auf die notwendige Innovationsoffenheit und damit Flexibilität für neue Energieeffizienzdienstleistungen eine zügige Revision der Regelbasis zulassen und gleichzeitig als technischer Durchsetzungsmechanismus der normativen Vorgaben dienen. Solche Mechanismen sollten daher in Betracht gezogen und auf Ihre Tauglichkeit für das Smart Grid untersucht werden.

Angesichts der besonderen Herausforderungen und der einmaligen Chance, eine von Grund auf vertrauenswürdige und datenschutzfreundliche Kommunikationsinfrastruktur aufzubauen, sollte der breite Einsatz moderner Sicherheitsmechanismen eingehend diskutiert werden. Insbesondere gehören hierzu Technologien des Trusted Computing sowie auf marktweit einheitlichen formalen Verarbeitungsregeln basierende Mechanismen der Zugriffssteuerung.

Da neben dendurch gesetzliche Vorgaben terminierten Verarbeitungsregeln im Smart Grid aber auch die Entscheidung des Betroffenen zu erlaubten oder verbotenen Verwendungen der Mess- und Vertragsdaten in jeder Entscheidungssituation zwingend berücksichtigt werden müssten, wäre ein möglicher Mechanismus, die notwendigen Informationen schon an der Quelle, dem Messgerät, den Messdaten beizufügen. Eine technische Kapselung und Zugriffssteuerung wie sie im Markt bereits entwickelt ist, müsste insofern allerdings durch alle Protokolle und Datenmodellierungsstandards der Marktkommunikation unterstützt werden.

In diese Richtung sind auf europäischer Ebene die Bemühungen des ebIX[92] angelegt. Im RFC "Exchange of metered data" findet sich insbesondere der Use Case „Apply Confidentiality Rules".[93]Der ebIX ist zwar noch nicht ausdefiniert, aber es zeigt sich, dass auf europäischer Ebene davon ausgegangen wird, dass Messdaten künftig technisch geschützt werden sollen. Die „European Federation of Energy Traders (EFET)“ hat folgerichtig in der Spezifikation für den Datenaustausch im Energiehandel EFET eCM im Rahmen der ebXML-Standardisierung die vorgenannten Aspekte

[91] Roßnagel/Jandt, S.41

[92] European forum for energy Business Information eXchange (ebIX)

[93] Exchange of metered data v0.9, S. 32, online unter http://www.ebix.org/ [10.05.2010].

ebenfalls standardisiert,[94] um die erforderliche Ende-zu-Ende Sicherheit zu gewährleisten. Ergänzend kommt noch hinzu, dass aus dem Eichrecht beweisrelevante Vertrauenstatbestände für die Richtigkeit der Messdaten erwachsen, die in die digitale Welt transformiert werden müssen. Im Hinblick auf die vielfältigen zukünftigen Messdatenempfänger, die in besonderer Weise auf die Sicherstellung der Herkunft und Unverfälschtheit der Messdaten angewiesen sind, ist eine elektronische Signierung und Sicherung vor Verfälschung der relevanten Verbrauchsdaten am Ort der Entstehung notwendig. Die einmal generierten Vertrauenstatbestände müssen auch auf dem Energiekernmarkt transparent Ende-zu-Ende gewährleistet werden.

Die verwendeten Nachrichtenformate und Sicherungsmechanismen für die Messdatenübermittlung müssen eine entsprechende Repräsentation des Nutzerwillens unterstützen.

NUTZERRECHTE

Neben den Auskunftsrechten (§ 34 BDSG) sind im Hinblick auf das informationelle Selbstbestimmungsrecht des Betroffenen insbesondere auch noch die Rechte aus § 35 BDSG, mithin also der Anspruch auf Berichtigung, Löschung und Sperrung von Daten auch von den Akteuren des Smart Grid zu beachten.

ANALYSE

Sofern, wie im ersten Referenzszenario des Einsatzes von Smart Metern im klassischen Energiekernmarkt, die Akteure und Prozessketten im Rahmen der Abrechnung auf Basis der Ermächtigungsgrundlage des § 21b EnWG zur Festlegung von Geschäftsprozessen durch die BNetzA noch verbindlich definiert sind,[95]lassen sich regelmäßig die Datenverwendungen in der Prozesskette nachvollziehen und so grundsätzlich die vorgenannten Betroffenenrechte auch realisieren.

Für alle Sachgestaltungen ist anzumerken, dass dann, wenn die erhobenen und gespeicherten Daten nicht mehr für ihren ursprünglichen Zweck benötigt werden, die in § 35 Abs. 2 S. 2 Nr. 3 BDSG niedergelegte Pflicht besteht, diese zu löschen (bzw. zu sperren, wenn beispielsweise noch steuerrechtlich motivierte Aufbewahrungspflichten existieren).

Problematisch ist im ersten Szenario allerdings, ob und wie diese Rechte z. B. nach der Übermittlung von Messwerten in Drittstaaten ohne angemessenes Datenschutzniveau durchgesetzt werden können. Dies betrifft insbesondere Sachgestaltungen wie das Google PowerMeter.

[94] Vgl. Electronic Confirmation Matching Standards Version 3.3.1 Final, 2009, S. 127 – 129.

[95] Vgl. Konsultationen BNetzA

In Folgeszenarien wie der Datenverwendung bei der Energieeffizienzberatung und Optimierung werden derartig klare, normativ geprägte Strukturen des klassischen Energiemarktes allerdings nicht mehr vorliegen. Insofern ist schon heute Beobachtungs- und Handlungsbedarf adressiert.

HANDLUNGSBEDARF

Bei den verschiedenen Akteuren des Energiemarktes müssen die Messdaten für unterschiedliche Zwecke und in unterschiedlicher Form gespeichert werden. Im Sinne von Rechtsklarheit und im Hinblick auf die nunmehr bestehende Sensibilität der feingranularen Messdaten wird insofern empfohlen:

> Es sollten nach dem Vorbild der Verkehrsdaten im Telekommunikationsrecht neben spezifischen Erlaubnistatbeständen bereichsspezifisch differenzierte Lösch- bzw. Sperrpflichten für die Messdaten bei den Akteuren (MSB, VNB und LF) statuiert werden.

Für die Folgeszenarien der Einführung von Smart Metern, die durch eine Vielzahl neuer Marktakteure und Geschäftsprozesse gekennzeichnet sind, sollte die Chance genutzt werden, im Rahmen der Entwicklung der Softwareinfrastrukturen schon frühzeitig mit der Implementierung von technischen Mechanismen zu beginnen, die auchin einem offenen System die Durchsetzung von Nutzerrechten garantieren.

> Im Hinblick auf die Ausübung von Nutzerrechten bei zukünftigen Systemgestaltungendes Smart Grid können neben formal beschriebenen nutzergenerierten Zugriffsregeln im Rahmen des Konzeptes „Privacy by Design“ auch Sperr- und Löschpflichten als formale technische Regeln in das System integriert werden und somit automatisierte Verfahren eine Durchsetzung der Nutzerrechte garantieren.

KONTROLLE

Grundsätzlich bietet das BDSG das Instrumentarium, um den Betroffenen hinsichtlich seiner personenbezogenen Daten zu schützen. In der Praxis wird davon aber nicht immer Gebrauch gemacht bzw. das Potential nicht ausgeschöpft. Dies liegt größtenteils daran, dass für die datenverarbeitenden Stellen kein Anreiz gesetzt wird, dem Betroffenen ein bestimmtes (höheres) Schutzniveau zu bieten.

Die Kontrolle der Einhaltung des Datenschutzrechts erfolgt einerseits durch das Instrument der Selbstkontrolle, indem betriebliche Datenschutzbeauftragte (§ 4 f BDSG) eingesetzt werden und andererseits in Form von staatlicher Kontrolle durch staatliche Aufsichtsbehörden (§ 38 Abs. 1 S.1 BDSG).

Sogenannte Selbstverpflichtungen wie Privacy Statements sind lediglich als gute Vorsätze zu betrachten, die weder allgemeingültig noch durchsetzbar sind. In diesem Zusammenhang gewinnt in jüngerer Zeit die Selbstregulierung immer mehr an Bedeutung. Dies verdankt sie der Erkenntnis und Erfahrung, dass in einer hochkomplexen sowie technisch geprägten, sich rasch verändernden Welt der Datenschutz nicht mehr vollständig und umfassend vom Staat gewährleistet werden kann. [96]

Als Beispiel einer Selbstregulierung im Bereich des Datenschutzrechts, wie sie Art. 27 der EG-Datenschutzrichtlinie fordert, wäre hier das schon seit Mitte der 90er Jahre angedachte und diskutierte Datenschutzaudit zu nennen, welches durch den seit dem 22.05.2001 eingeführten § 9a BDSG und die damit ermöglichte Einführung eines Datenschutzauditgesetzes auch konkretere Formen angenommen hat.[97]

ANALYSE

Mit einem allgemeinen Datenschutzauditgesetz[98] könnte ein rechtlich verbindlicher Rahmen gesetzt werden, innerhalb dessen eine Kooperation von Behörden und Verbänden (Datenschutzauditausschuss) die materiellen Vorgaben flexibel festsetzen können und die für alle Parteien, die sich freiwillig einem Datenschutzaudit unterziehen, verbindlich sind.

Ziele und Vorteile eines Datenschutzaudits sind unter anderem die Stärkung der Selbstverantwortung und des Wettbewerbs und die kontinuierliche Verbesserung von Datenschutz und Datensicherheit sowie eine erhöhte Transparenz für den Verbraucher.[99] Des Weiteren werden der Datenschutzbeauftragte und die Aufsichtsbehörden unterstützt und entlastet.

Die Durchführung eines Datenschutzaudits soll freiwillig sein. Es wird jedoch ein Anreiz zur Durchführung eines Audits geschaffen, indem die Unternehmen durch das Datenschutzauditsiegel einen Mehrwert in Form eines Marktvorteils erhalten. Sie dürfen das Siegel für die Außendarstellung – und somit Werbung – verwenden, was ihnen einen Wettbewerbsvorteil verschaffen kann. Einen marktwirtschaftlichen Mehrwert stellt das Prüfsiegel sinnvoller Weise nur dar, wenn nicht nur die Gesetzeskonformität des Produktes oder der Stelle geprüft wird, sondern vielmehr zuvor festgesetzte über das gesetzlich gewährte Datenschutzniveau hinausgehende Richtlinien. Da es nach der geltenden Rechtslage an einem einheitlichen Datenschutzauditgesetz fehlt, können dessen Vorteile derzeit auch nicht durch die Akteure des Smart Grid genutzt werden.

HANDLUNGSBEDARF

Im Hinblick darauf, dass für die Prozesse der Marktkommunikation bei der Nutzung von Smart Metern einheitliche Festelegungen erfolgen werden, wäre es sinnvoll auch einheitliche Datenschutzstandards sachspezifisch zu verankern. Hinsichtlich der Datenschutzkonzepte kommt das schon angesprochene Auditverfahren in Betracht. Hieraus würde die Zertifizierung ganzer Organisationen

[96] Roßnagel, Handbuch Datenschutzrecht, S. 389, Rn. 4.

[97] Roßnagel, Handbuch Datenschutzrecht, S. 442, 3. 7, Rn. 9; S. 459, 3.7, Rn 51.

[98] Sie insofern den Gesetzentwurf der Bundesregierung zu einem Datenschutzauditgesetz, https://www.datenschutzzentrum.de/bdsauditg/20070907-entwurf-bdsauditg.pdf [10.05.2010]

[99] Roßnagel, Datenschutzaudit, S. 3 ff.

wie der verantwortlichen Stellen im Smart Grid (sogenanntes Systemaudit) folgen. Dazu muss der Nachweis erbracht werden, dass der Datenschutz in der Organisation wirkungsvoll umgesetzt wird.

Produktbezogen, also im Hinblick auf die Hardware oder Software sowie Dienstleistungen und automatisierte Verfahren im Smart Grid wäre ein Produktauditnach dem Vorbild des § 4 Abs. 2 LDSG SH denkbar. In Schleswig-Holstein wird öffentlichen Stellen empfohlen IT-Produkte die mit den Vorschriften über Datenschutz und Datensicherheit vereinbar sind, vorrangig einzusetzen. Solche Produktzertifizierungen beziehen sich meist auf Hardware oder Software sowie Dienstleistungen und automatisierte Verfahren. Das auf dieser Basis verliehene Gütesiegel kennzeichnet Produkte, die diese Voraussetzungen nach einem förmlichen Verfahren erfüllen.[100]

Durch die Einführung eines allgemeinen Datenschutzauditgesetzes zur Konkretisierung des § 9a BDSG, könnte dafür gesorgt werden, dass bei entsprechenden Anwendung im Smart Grid einerseits Rechtssicherheit für die verantwortlichen Stellen und andererseits ein höheres Schutzniveau für den Betroffenen erreicht werden kann. Ein ergänzendes produktbezogenes Gütesiegel könnte zudem für Rechtssicherheit bei den Architekten der Softwareinfrastrukturen sorgen.

[100] Siehe https://www.datenschutzzentrum.de/guetesiegel/

TEIL II: SZENARIO ELEKTROMOBILITÄT

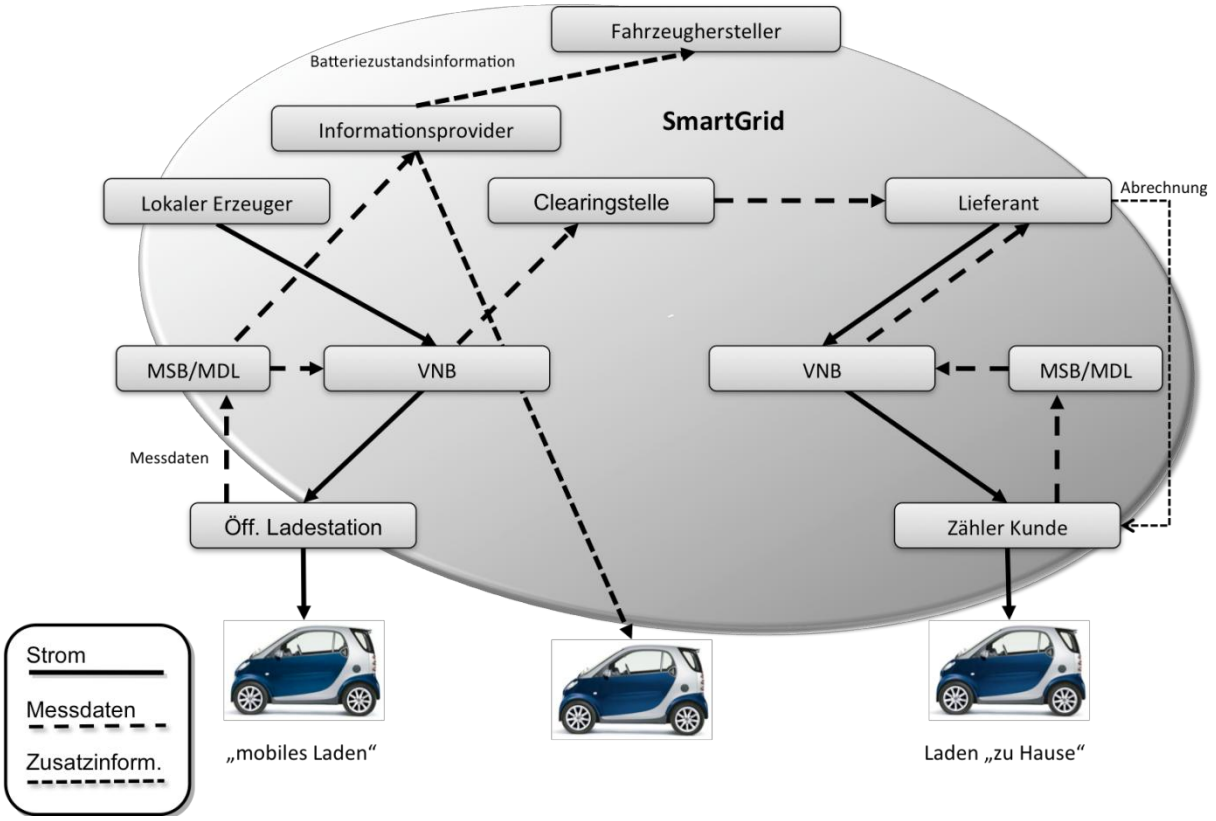

Abbildung 3: Elektromobilität

Das bislang betrachtete Szenario der dynamischen Tarifierung im Smart Grid bezog sich lediglich auf die Abnahme von Strom innerhalb eines Haushalts. Darüber hinaus wird zukünftig auch die Elektromobilität eine zentrale Rolle für das Smart Grid spielen. In diesem Bereich ergeben sich jedoch zusätzliche Datenschutzfragen, die auf Basis des folgenden generischen Szenarios betrachtet werden sollen. Die Planungen zur konkreten Ausgestaltung sind in diesem Bereich derzeit noch weniger ausgeprägt als für den Anwendungsfall der Haushaltszähler. Es besteht auch insofern ein dringender Bedarf zur Sachverhaltsermittlung und mithin zu Einführung eines regionenübergreifenden UseCase-Repositorys. Die in den derzeitigen Modellprojekten verwendeten Ansätze werden deshalb einstweilen als Interimslösungen angesehen, die für einen späteren Rollout der Elektromobilität sicher noch eine deutliche Überarbeitung erfahren werden.

Gleichwohl wurden im Rahmen der derzeitigen Forschungsprojekte bereits erste Weichenstellungen vorgenommen. Dies betrifft u.a. das Nummerierungsschema zur Identifikation von Fahrstromverträgen. Die genaue Spezifikation steht zwar auch hier noch aus, es zeichnet sich aber ab, dass die hierbei verwendeten IDs prinzipiell aus vier Blöcken bestehen. Vorgesehen sind eine Länderkennung, eine Anbieterkennung, eine anbieterspezifische Vertrags-ID und eine Prüfziffer. Im Rahmen der Pilotphase sollen die so strukturierten Vertrags-IDs im Überwiegenden Teil der Modellregionen auf

RFID-Karten[101] aufgebracht werden, mittels derer die Kunden sich an der zu verwendenden Ladestation anmelden können.[102] Die von der Ladestation ausgelesenen Identifikationsdaten sollen dann an eine Steuerungsinstanz übermittelt werden, welche daraufhin die Ladestation freischaltet.

Derartige, RFID-basierte Verfahren stellen jedoch lediglich eine interims-Lösung dar und werden auf mittel- bis langfristige Sicht durch fortgeschrittene Plug&Charge-Verfahren ersetzt werden, bei denen der Anmeldevorgang zwischen Fahrzeug und Ladestation stattfindet und dieselbe Verbindung auch für weitere Kommunikationsvorgänge zwischen Fahrzeug und unterschiedlichen Komponenten des Smart Grid erfolgt.[103] Nur auf Basis derartiger Kommunikationsverbindungen lassen sich die für die Einbindung von Elektromobilität angestrebten Funktionalitäten realisieren. Ein derartiger Ansatz wird schon jetzt von zumindest einer Modellregion verfolgt.[104]Nur so lassen sich die für die Einbindung von Elektromobilität angestrebten Funktionalitäten tatsächlich realisieren.

Da für den Fall der Integration von Elektromobilität keine Rollen- und Prozessdefinitionen vorliegen, wie sie im Bereich des Smart Meters durch die Konsultationen der BNetzA skizziert sind, orientieren sich die gezeigten Informationsflüsse insofern an diesen Vorgaben, als es zur nahtlosen Integration in das bestehende System notwendig wäre. Folgt man den Ausführungen der Bunderegierung im Nationalen Entwicklungsplan Elektromobilität, so sollen *„künftige öffentliche Ladestellen […] für jeden Stromlieferanten und jedes Fahrzeugmodell diskriminierungsfrei nutzbar sein. Es wäre nicht wünschenswert, wenn jeder Anbieter eine separate Infrastruktur von Ladestationen für seine Kunden schaffen müsste. Die Strombelieferung von Elektrofahrzeugen muss ebenso im Wettbewerb erfolgen können wie eine Strombelieferung der Haushalte*“.[105] Hiervon ausgehend lässt sich folgendes generisches Szenario für die Analyse der mobilen Stromabnahme („Roaming“) skizzieren:

Ein Kunde verfügt über ein Elektrofahrzeug und über einen Fahrstromvertrag mit seinem Heimlieferanten. Der Heimlieferant betreibt eine Vielzahl öffentlicher Ladestationen, über die der Kunde sein Fahrzeug aufladen kann. Hierzu schließt er das Fahrzeug an eine Ladestation an.[106] Daraufhin wird der Ladevorgang über eine zwischen Fahrzeug und Ladestation bestehende Kommunikationsverbindung initialisiert. Die genaue Vorgehensweise hierzu ist noch nicht abschließend festgelegt, gezwungenermaßen muss jedoch der Kunde oder das Fahrzeug in diesem Szenario in Hinblick auf

[101] Der genaue Typ der zu verwendenden Karten ist hierbei noch nicht genauer spezifiziert. In jedem Fall werden aber Karten zum Einsatz kommen, die ein dem aktuellen Stand der Technik entsprechendes Sicherheitsniveau aufweisen und beispielsweise keine unsicheren MiFare-Classic Karten.

[102] Alternativ hierzu sollen auch zusätzliche Verfahren wie die Freischaltung per SMS oder Telefonanruf angeboten werden, diese werden mangels langfristiger Perspektive hier jedoch nicht gesondert betrachtet.

[103] Insbesondere ist hier der derzeit in Entwicklung befindliche ISO-Standard 15118 zu nennen.

[104] Die Modellregion E-DeMa setzt einvernehmlich mit internationalen und nationalen Standardisierungsgremien auf eine Plug & Charge Lösung, nach der sich das Fahrzeug anmeldet und RFID nicht zum Einsatz kommt.

[105] Bundesregierung, Nationaler Entwicklungsplan Elektromobilität, Stand August 2009, http://www.bmwi.de/Dateien/BMWi/PDF/nationaler-entwicklungsplan-elektromobilitaet-der-bundesregierung,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf [12.05.2010]

[106] Eventuell muss er die Ladestation hierzu vorher in geeigneter Art und Weise freischalten. Hierauf soll jedoch nicht gesondert eingegangen werden.

den jeweiligen Fahrstromvertrag identifiziert und für das Laden autorisiert werden.[107] Darüber hinaus können im Rahmen des Initialisierungsvorgangs weitere Parameter beispielsweise zum angestrebten Zeitpunkt der Abfahrt ausgetauscht werden, um z. B. den Ladezeitpunkt an Netzlast oder Stromverfügbarkeit anzupassen.

Das Fahrzeug wird daraufhin geladen und die jeweiligen Strommengen werden vom in der Ladestation befindlichen Zähler[108] erfasst und mit Zeitpunkten attributiert. Anders als bei elektronischen Haushaltszählern werden die Messwerte zudem mit der jeweiligen Vertrags-IDattributiert. Diese Messwerte werden dann vom für die Ladestation zuständigen MSB/MDL ausgelesen und über den VNB an den Heimlieferanten übermittelt. Dieser wiederum erstellt auf Basis der ihm übermittelten, ID-attributierten Messwerte die monatliche Abrechnung für den Kunden.

Deutlich komplexer stellt sich das Szenario dar, wenn man die zwingend notwendige Möglichkeit des Roamings zwischen verschiedenen Regionen betrachtet und zudem voraussetzt, dass Ladestationen auch beispielsweise von hierauf spezialisierten Anbietern betrieben werden können, die weder Stromlieferant noch lokaler Verteilnetzbetreiber sein müssen. Ausgehend von einer solchen, bislang noch nicht existierenden energiewirtschaftlichen Rolle „Ladestationsbetreiber“[109] (im Folgenden LSB) stellt sich ein Ladevorgang dann wie folgt dar:

Der Kunde schließt sein Fahrzeug an der vom LSB betriebenen Ladestation an. Das Fahrzeug soll beladen und die entnommene Strommenge über denjenigen Fahrstromvertrag abgerechnet werden, den der Kunde mit seinem Heimlieferanten geschlossen hat. Der Kunde muss daher durch seinen Heimlieferanten gegenüber dem LSB autorisiert werden. Nach einer wie oben beschriebener Initialisierung beginnen der Ladevorgang und die fortlaufende Messung der Stromentnahme. Logisch findet hierbei ein Stromfluss vom Heimlieferanten zur Ladestation bzw. zum Fahrzeug statt. Bereits während des Ladevorgangs oder nach dessen Abschluss werden die Zeit- und ID-attributierten Messdaten vom für die Ladestation zuständigen MSB/MDL erfasst und müssen aus den bereits für den Fall der Haushaltszähler beschriebenen Gründen an den lokalen Netzbetreiber und über diesen auch an den Heimlieferanten übermittelt werden. Für die Übermittlung an den Lieferanten bzw. die Abrechnung mit diesem ist dabei sowohl eine direkte Kommunikation als auch die Abwicklung über eine zentrale Clearingstelle[110] denkbar. In jedem Fall erstellt aber der Heimlieferant auf Basis der ihm übermittelten Daten die monatliche Abrechnung für den Kunden, in die insbesondere auch mögliche Nutzungsentgelte für den LSB einfließen können.

Darüberhinaus sind in die folgenden Überlegungen auch Zusatzdienste wie beispielsweise Aggregatoren zur kooperativen Bereitstellung von Regelenergiekapazität, „intelligente“ Routen-

[107] Hierbei kann sich aus unterschiedlich Gründen auch die Eingabe eines Passworts, einer PIN o. ä. als notwendig erweisen. Auch hiervon soll jedoch an dieser Stelle abstrahiert werden.

[108] Die grundsätzlich denkbare Option, den Zähler in den Fahrzeugen zu platzieren, scheidet aus vielerlei Gründen kategorisch aus. Vgl. allein Fest/Franz/Gaul, Energiewirtschaftliche und energiewirtschaftsrechtliche Fragen der Elektromobilität – Teil 2. Energiewirtschaftliche Tagesfragen, Heft 5/2010.

[109] Die Funktion des Ladestationsbetreibers könnte allerdings auch von bestehenden energiewirtschaftsrechtlichen Rollen wie z.B. dem MSB/MDL wahrgenommen werden.

[110] Die Notwendigkeit einer solchen Clearingstelle hängt letztlich von der energiewirtschaftsrechtlichen Ausgestaltung der Ladestation ab. Diesbezüglich besteht in jedem Fall weiterer Klärungsbedarf, für die grundsätzliche datenschutzrechtliche Bewertung ist diese Frage jedoch weniger relevant.

planungsdienste und die Übertragung von Fahrzeugzustandsinformationen einzubeziehen. Hier werden möglicherweise zusätzliche Anmelde- und Datenübermittlungsvorgänge notwendig sein. Stellvertretend für derartige Dienstleistungen wird im Folgenden angenommen, dass im Zuge der Anmeldung auch Informationen zum Batteriezustand an einen Fahrzeuginformationsprovider[111] übermittelt werden, der die Daten je nach Ausgestaltung beispielsweise an den Hersteller weiterleiten oder dem Fahrzeugeigentümer zur Online-Einsicht zur Verfügung stellen kann.

Das Szenario der Elektromobilität unterscheidet sich damit vor allem in dreierlei Hinsicht vom eingangs betrachteten Szenario des Haushaltsanschlusses: Zum ersten werden die Messdaten eines Kunden an unterschiedlichen Ladestationen und damit durch unterschiedliche Zähler erhoben, für die wiederum unterschiedliche MSBs/MDLs die Messungen durchführen. Dies macht eine explizite Identifizierung nebst Autorisierung des Kunden oder Fahrzeug[112] bei jedem Ladevorgang und eine entsprechende Attributierung der Messdaten zwingend erforderlich.

Zweitens sind mit dem Betreiber der Ladestation (LSB) sowie mit einer möglicherweise zu etablierenden Clearingstelle mindestens zwei zusätzliche Rollen in die Übermittlung und Verarbeitung der Messdaten involviert und müssen in den Datenschutzbetrachtungen ebenfalls berücksichtigt werden. Im Rahmen zusätzlicher Anwendungsfälle wie der Bereitstellung von Regelenergie (Minutenreserve) oder der Übermittlung von Fahrzeuginformationen über einen Informationsprovider kann sich der Kreis der zusätzlich involvierten Parteien noch weiter ausdehnen.

Darüberhinaus können die im Rahmen der Elektromobilität anfallenden Daten nicht nur einen Personenbezug, sondern auch einen expliziten oder impliziten Ortsbezug aufweisen. Anders als im Fall der oben betrachteten Haushaltszähler lassen sich hieraus beispielsweise Bewegungsprofile erstellen. Diesem Umstand muss durch ein angemessenes Datenschutzkonzept besonders Rechnung getragen werden.

PERSONENBEZUG DER DATEN

ANALYSE

Da die Abrechnung des Stromverbrauchs im Referenzszenario auch bei Inanspruchnahme unterschiedlicher Ladestationen über den Heimlieferanten des Fahrzeugnutzers erfolgen soll, muss der Lieferant wissen, welchem Kunden er die angefallenen Messwerte zuordnen muss. Die Messdaten müssen daher zwangsläufig mit Informationen zum jeweiligen Nutzer angereichert werden. Schon beim Speichern der Messwerte in der Ladestation handelt es sich um personenbezogene Daten, da die Messwerte in der Ladestation mit einer Kunden-ID verknüpft werden, welche zu Beginn des Ladevorgangs im Falle des Plug& Charge über das Fahrzeug oder im RFID-Szenario über eine dem

[111] Auch in Bezug auf den Fahrzeuginformationsprovider, den Aggregator etc. ist die konkrete Ausgestaltung bislang weitgehend unklar. Grundsätzlich denkbar wäre auch, dass ein LSB diese Rollen übernimmt.

[112] Wobei aus beweisrechtlicher Perspektive die Identifikation des Kunden vorzugswürdig ist, vgl. Pallas/Raabe/Weis, CR 2010 (im Erscheinen).

Kunden zuvor ausgehändigte Karte in die Ladestation übertragen werden[113]. Die **Kombination der Messwerte mit der Kunden-ID muss aus eichrechtlichen Gründen und zur Gewährleistung von Authentizität bereits in der Ladestation erfolgen**. Eine spätere Zuordnung würde hierfür aus Gründen der vom Eichrecht geforderten Nachvollziehbarkeit nicht ausreichen.

Die im Szenario Elektromobilität anfallenden Daten sind insbesondere wegen der Möglichkeit zur Erstellung von Bewegungsprofilen als kritisch zu beurteilen. Anhand der Daten kann insbesondere nachvollzogen werden, in welchem Gebiet sich der jeweilige Nutzerzu welchem Zeitpunkt aufgehalten hat, und auch eine Echtzeitanalyse des Standortes wäre grundsätzlich jederzeit möglich.

Ein weiteres datenschutzrechtliches Problem stellt sich dadurch, dass es teilweise beabsichtigt wird, dem Kunden den Ladezustand des Elektroautos sowie weitere Informationen beispielsweise mittels einer Mobilfunkapplikation anzuzeigen. Sollte eine Abrechnung der Stromentnahme über eine Identifikation des Fahrzeuges (und nicht des Nutzers) erfolgen, so wäre es möglich, dass der Fahrzeugeigentümer jederzeit darüber informiert ist, wo sich beispielsweise sein Ehepartner gerade aufhält. Zudem kommen auch hierbei noch weitere datenverarbeitende Stellen hinzu. Der Fahrzeuginformationsprovider soll die Zustandsdaten an das Handy des Nutzers übertragen. Zudem ist es z.B. möglich, dass der Fahrzeuginformationsprovider die Daten auch an den Fahrzeughersteller übertragen soll, was diesem möglicherweise ebenfalls in die Lage versetzt, Einblick in das Mobilitätsverhalten des Betroffenen zu gewinnen.

HANDLUNGSBEDARF

Die Integration von Elektromobilität in den Energiemarkt weist unter dem Gesichtspunkt grundsätzlicher datenschutzrelevanter Gefahrenlagen aufgrund der Qualität des Personenbezuges der Daten noch deutlich über die bestehenden Risiken der Integration von Smart Metern hinaus.

Wegen der weitergehenden Möglichkeiten der Bildung von Verhaltens- und Bewegungsprofilen ist in den Elektromobilitätsszenarien eine begleitende datenschutzrechtliche Analyse auch außerhalb der energiemarktspezifischen Sachverhalte geboten.

RECHTMÄßIGKEIT

Datenschutzrechtlich relevante Vorgänge finden im Szenario Elektromobilität sowohl beim MSB/MDL, beim VNB, beim Lieferanten und eventuell noch in der Clearingstelle statt. Hinzu kommt noch die Übermittlung der Daten zwischen den beteiligten Akteuren.

[113] Die Verwendung des einen oder des anderen Authentifizierungsmechanismus stellt aus datenschutzrechtlicher Perspektive allerdings zunächst keinen Unterschied dar und wird daher nicht näher betrachtet.

ANALYSE – ERHEBEN DER DATEN

Fraglich ist, wann die Messdaten im Sinne des § 3 Abs. 3 BDSG erhoben werden. Relevant ist dies, da der informatorische Pflichtenkanon des BDSG grundlegend an diesen Vorgang anknüpft. In Betracht kommt sowohl der Moment, in dem die Daten in der Ladesäule ankommen, als auch der Moment des Fernauslesens. Wie ausgeführt liegt ein Erheben nach § 3 Abs. 3 BDSG dann vor, wenn die Daten über den Betroffenen beschafft werden. Die Formulierung „beschaffen" legt nahe, dass ein aktives Element der datenerhebenden Stelle vorhanden sein muss. Ein solches aktives Element liegt in jedem Fall im Moment des Fernauslesens vor, da der MSB/MDL die Daten hierzu beim Zähler anfordern muss. Ein aktives Element des MSB/MDL beim Speichern der Daten im Zähler lässt sich hingegen nicht erkennen, da dieser Vorgang automatisiert durch den Zähler vorgenommen wird.

Auch die bereits veröffentlichten Gutachten zu Smart Metern knüpfen das Erheben der Daten an den Vorgang des Fernauslesens.[114] Zwar wurden diese Gutachten im Hinblick auf intelligente Haushaltszähler verfasst, doch stellt die reine Stromabnahme an einer Ladestation keinen anderen Vorgang dar als die Stromabnahme im Haushalt. Lediglich die Gefährdungslagen unterscheiden sich – wie geschildert –voneinander. Daher würde es, jedenfalls ohne explizite Regelung, konstruiert wirken, den Vorgang des Erhebens an andere Kriterien zu knüpfen, als dies bei Haushaltszählern der Fall ist.

Knüpft man im Fall der Elektromobilität, also der mobilen Stromabnahme, nun bezüglich der Datenerhebung an den Vorgang des Fernauslesens an, so stellt sich das Problem, wer für die im Zähler befindlichen Daten verantwortlich ist. Im Unterschied zur häuslichen Abnahme befindet sich dieser Zähler nämlich nicht in einem geschützten, sondern im öffentlichen Raum und ist dadurch naturgemäß einem höheren Gefahrenpotenzial ausgesetzt, als dies bei einem Haushaltszähler der Fall ist. Das BDSG wäre in Konsequenz einer Auslegung, die das Erheben an den Abruf durch den MSB/MDL anknüpfte aber im Moment der Speicherung der Messdaten auf dem Zähler noch nicht anwendbar.

Zudem stellt sich in diesem Fall das Problem der Mitwirkungspflicht bei der Erhebung der Daten in besonderem Maße. Zum Zeitpunkt des Fernauslesens der Daten dürfte der Betroffene regelmäßig die Ladesäule verlassen haben. Eine Mitwirkung bei der Erhebung, die an das Fernauslesen anknüpfte, wäre daher ausgeschlossen. Ob eine Mitwirkung zu einem früheren Zeitpunkt stattfindet und dies für § 4 Abs. 2 BDSG ausreicht, kann an dieser Stelle offen bleiben.

Insofern muss das Schutzregime des BDSG bereits dann eröffnet sein, wenn die Daten lediglich im Zähler gespeichert werden. Würde man den Vorgang des Erhebens hingegen an den Moment des Speicherns der Daten im Zähler anknüpfen, so stellen sich andere Probleme.

Die Vision des flächendeckenden Aufbaus einer Ladeinfrastruktur bezieht auch das Modell einer mobilen Steckdose mit ein. Hierbei soll der Kunde an jeder beliebigen Steckdose sein Fahrzeug auf seine eigene Rechnung beladen können. Der abgenommene Strom wird dabei am Zähler des Eigentümers der benutzten Steckdose registriert. Infolgedessen würden hier die Daten erst mit dem Fernauslesen erhoben.

Hieran zeigt sich, dass eine unterschiedliche Betrachtung der häuslichen und der mobilen Stromabnahme, wann ein Erheben der Daten vorliegt, nicht in Betracht kommen kann.

[114] ULD-SH, S. 5 ff; Roßnagel/Jandt, S. 36.

HANDLUNGSBEDARF

Es stellt sich folglich die Frage, wie die auf dem Zähler gespeicherten Daten behandelt werden sollen. Die Daten, welche sich auf dem Zähler befinden, müssen in jedem Fall geschützt werden. Da das BDSG in diesem Moment jedoch nach geltender Rechtslage noch nicht eingreift, besteht hier Handlungsbedarf.

> Es sollte bereichsspezifisch eine konkretisierende Regelung getroffen werden, wann in den Fällen der elektromobilen Nutzung von Ladestationen von einer Datenerhebung durch den MSB/MDL auszugehen ist. Im Hinblick auf die Folgepflichten (Information) sollte der maßgebliche Zeitpunkt schon mit dem Speichern der Daten auf dem Messgerät bestimmt sein.

ANALYSE – RECHTMÄßIGKEIT DER DATENERHEBUNG

Im Anschluss an das Fernauslesen der Messwerte durch den MSB/MDL verändert dieser die Daten sodann, indem er sie aggregiert um sie den anderen Beteiligten Akteuren zur Verfügung stellen zu können. Zudem werden die Daten auch vom MSB/MDL aus beweis- und eichrechtlichen Gründen gespeichert werden. Anschließend übermittelt er die Daten an den VNB, welcher sie ebenfalls speichert und dann über die Clearingstelle an den Lieferanten übermittelt.

Grundsätzlich stellt sich der Datenfluss im Szenario Elektromobilität bis auf die eventuell zwischengeschaltete Clearingstelle ähnlich wie im Szenario Smart Grid dar. Der Unterschied besteht jedoch darin, dass der Kunde im Referenzszenario Elektromobilität nur einen Vertrag mit dem Heimlieferanten hat. Keine Verträge bestehen hingegen in der Regel zwischen dem Nutzer und dem an der jeweiligen Ladestation zuständigen MSB/MDL beziehungsweise mit dem örtlichen VNB.

Als Rechtsgrundlage für die Erhebung der Messdaten durch den MSB/MDL kommt hier insbesondere § 4 Abs. 1 i. V. m. § 28 Abs. 1 BDSG in Betracht. Der MSB/MDL erhebt die Messdaten für die Erfüllung eigener Geschäftszwecke. Die Messung selbst ist nämlich gerade der primäre Geschäftszweck des MSB/MDL, (vgl. § 9 Abs. 1 MessZV).

Als vertragliche Basis zur Legitimation könnte angenommen werden, dass durch Nutzung der Ladesäule ein Vertrag konkludent zustande kommt und die Daten dementsprechend auf Grundlage von § 4 Abs. 1 i. V. m. § 28 Abs. 1 Nr. 1 1. Alt. BDSG erhoben werden dürfen. Bei heutigen SB-Tankstellen ist dies der Fall, das Aufstellen der zapfbereiten Säule stellt das Angebot und das Tanken des Kunden die Annahme dar, mithin wird bereits durch den Beginn des Tankens konkludent ein Kaufvertrag geschlossen. Jedoch ist das hier betrachtete Szenario anders zu bewerten. Der Kunde hat hier einen Vertrag mit einem Lieferanten und kauft von diesem Strom. Andere Vertragsbeziehungen möchte er hier nicht eingehen. Insbesondere, da er über sein Vertragsverhältnis mit dem Lieferanten hinaus keinerlei rechtliche Verpflichtungen auferlegt bekommen will. Der Abschluss eines konkludenten Vertrages zwischen MSB/MDL und Nutzer scheidet damit aus[115] und somit auch eine Legitimation der Datenerhebung über § 4 Abs. 1 i. V. m. § 28 Abs. 1 Nr.1 1. Alt. BDSG.

Auch eine Legitimation über § 4 Abs. 1 i. V. m. § 28 Abs. 1 Nr.1 2. Alt. BDSG scheidet in diesem Fall aus. Ein vertragsähnliches Vertrauensverhältnis kommt in Fällen von vorvertraglichen und nachver-

[115] Im Fall der Personalunion von MSB/MDL und Ladestationsbetreiber ergibt sich dieses Problem nicht.

traglichen Schuldverhältnissen sowie bei einem gestörten Vertragsschluss in Betracht.[116] Ein solcher Fall liegt hier zwischen dem Nutzer und dem MSB/MDL aber nicht vor. Die Parteien kennen sich im Zweifel noch nicht einmal, so dass ein vertragsähnliches Vertrauensverhältnis nicht bestehen kann.

Daneben könnte als Rechtsgrundlage für die Datenerhebung ein Anschlussnutzungsverhältnis gemäß § 3 NAV zwischen dem Nutzer und dem MSB/MDL bestehen. Ein solches Anschlussnutzungsverhältnis entsteht aber gemäß § 3 NAV nicht mit dem MSB/MDL, sondern mit dem VNB. Aber selbst wenn MSB/MDL und VNB hier aufgrund von § 21b Abs. 1 EnWG zusammenfallen sollten, ist es aufgrund der Rechtsfolgen, die die Einordnung des Kunden als Anschlussnutzer nach sich ziehen würde, ohnehin äußerst fraglich, ob dieser an einer Ladesäule überhaupt Anschlussnutzer sein kann.[117]

Letztendlich kommt noch eine Legitimation der Datenerhebung im Wege der Auftragsdatenverarbeitung gemäß § 11 BDSG in Betracht. Verantwortliche Stelle könnte hier der Lieferant sein, mit welchem ein Vertrag besteht, wodurch die Datenerhebung gemäß § 4 Abs. 1 i. V. m. § 28 Abs. 1 Nr.1 1. Alt. BDSG rechtmäßig wäre. Jedoch darf der Auftragnehmer, in diesem Fall der MSB/MDL, gemäß § 11 Abs. 3 BDSG die Daten nur nach Weisung des Auftraggebers, also des Lieferanten, erheben. Zudem ist der Bereich der Auftragsdatenverarbeitung dort zu Ende, wo dem „Auftragnehmer“ eine eigene rechtliche Zuständigkeit für die Aufgabe, deren Erfüllung die Datenverarbeitung oder Nutzung dient, zugewiesen wird.[118] Dies ist hier jedoch der Fall, da die Messung selbst das originäre Geschäftsinteresse des MSB/MDL ist. Dies ergibt sich bereits aus § 9 MessZV, so dass eine auch Legitimation im Wege der Auftragsdatenverarbeitung ausscheidet.

HANDLUNGSBEDARF

Da für das Referenzszenario der Elektromobilität in der Phase der Datenerhebung durch den MSB/MDL kein gesetzlicher oder vertraglicher Legitimationstatbestand ersichtlich ist, kommt einstweilen nur die Erteilung einer informierten Einwilligung nach § 4a BDSG in Betracht.[119] Im Hinblick auf das damit verbundene Schriftformerfordernis und die potentielle Vielzahl von Adressaten (MSB/MDL) scheidet diese Lösung im Praxiseinsatz jedoch ebenfalls aus.

Da nach der geltenden Rechtslage keine sinnvolle Rechtsgrundlage ersichtlich ist, welche die Datenerhebung des MSB/MDL bei der wechselnden Nutzung öffentlicher Ladestationen legitimieren kann, ist es notwendig, eine bereichsspezifische Legitimationsgrundlage oder eine vereinfachte elektronische Einwilligung nach dem Vorbild des TMG einzuführen.

[116] Gola/Schomerus, § 28 Rn. 26.

[117] Vgl. BNetzA, BK6-09-170, Konsultation eines Positionspapiers zu den Anforderungen an Messeinrichtungen im Sinne von § 21b Abs. 3a und 3b EnWG, Stand 06.11.2009, Online über http://www.bundesnetzagentur.de [12.05.2010].

[118] Gola/Schomerus, § 11 Rn. 9.

[119] Auf die Notwendigkeit der bereichsspezifischen Modifikation der Anforderungen an die datenschutzrechtliche Einwilligung ist schon oben hingewiesen worden.

ANALYSE – WEITERE DATENSCHUTZRELEVANTE VORGÄNGE (MESSDATEN)

Da eine Legitimation der Datenerhebung durch den MSB/MDL im geltenden Recht fehlt, muss hier zur weiteren Prüfung der Rechtmäßigkeit der sonstigen datenschutzrechtlich relevanten Vorgänge das Existieren einer solchen Regelung unterstellt werden.

Die Verarbeitung der Messdaten durch den MSB/MDL wird in Zukunft durch die gleiche Regelung legitimiert sein müssen, wie die Erhebung der Daten. Anderes gilt jedoch für die Übermittlung der Daten vom MSB/MDL an den VNB. Gemäß § 4 Abs. 3 MessZV ist der MSB/MDL verpflichtet, die von ihm ausgelesenen Messdaten an den VNB zu übermitteln. Da hier eine gesetzliche Pflicht zur Datenübermittlung besteht, muss diese Vorschrift auch als datenschutzrechtliche Erlaubnis herangezogen werden können, da das Gesetz nichts gesetzlich Verbotenes vom Adressaten der Vorschrift, hier der MSB/MDL, verlangen kann.[120]

Die Verarbeitung der Daten durch den VNB, also das Aggregieren (Verändern) lässt sich durch § 4 Abs. 4 Nr. 2 MessZV legitimieren. Hiernach ist der Netzbetreiber verpflichtet, durch ihn aufbereitete Messdaten an den Netznutzer zu übermitteln. Da er die Daten gemäß dieser Vorschrift aufbereiten muss, ist das Verändern der Daten datenschutzrechtlich zulässig, da auch hier gelten muss, dass dem Adressaten einer Norm nicht rechtswidriges abverlangt werden darf. Dasselbe gilt auch für die Speicherung der Messwerte durch den VNB. Dieser ist nämlich gemäß § 4 Abs. 4 Nr. 3 MessZV verpflichtet, die Messdaten für den im Rahmen des Netzzugangs erforderlichen Zeitraum zu archivieren.

Die Übermittlung der Daten an den Lieferanten kann entweder über eine Clearingstelle oder direkt vom VNB an den Lieferanten erfolgen. Sollte eine direkte Übermittlung zwischen VNB und jeweiligem Heimlieferanten stattfinden,[121] so ergibt sich die Legitimation ebenfalls aus § 4 Abs. 4 Nr. 2 MessZV. Hierin wird der VNB verpflichtet, abrechnungsrelevante Daten an den Netznutzer zu übermitteln. Der Begriff der Netznutzer wird in § 3 Nr. 28 EnWG definiert als „natürliche oder juristische Personen, die Energie in ein Elektrizitätsversorgungsnetz […] einspeisen oder daraus beziehen“. Netznutzer ist der Lieferant, welcher mit dem VNB einen Netznutzungsvertrag gemäß § 24 StromNZV bzw. einen Lieferantenrahmenvertrag gemäß § 25 StromNZV abgeschlossen hat.

Sollte die Variante der Datenübermittlung über eine Clearingstelle gewählt werden, so ist die Rechtsgrundlage fraglich. Eine Regelung, welche die Übermittlungen vom VNB zur Clearingstelle bzw. von der Clearingstelle zum Lieferanten legitimiert, existiert nach der geltenden Rechtslage nicht. Eine datenschutzrechtliche Einwilligung wäre beim Roaming nicht praktikabel. Eine Auftragsdatenverarbeitung kommt hier ebenfalls nicht in Betracht, da die Clearingstelle nicht weisungsgebunden agiert. Vielmehr erfüllt sie ihr zukünftig zukommende eigene Aufgaben.

HANDLUNGSBEDARF

Nach den bisherigen Sachgestaltungen in den Modellregionen wird jedenfalls in einem Teil der Modellregionen die Einführung einer Clearingstelle, insbesondere beim grenzüberschreitenden Roaming, vorgesehen. Insofern wird wie folgt empfohlen:

[120] Siehe auch Roßnagel/Jandt, S. 12.

[121] Die erscheint aber beim Roaming als die eher unwahrscheinliche Sachgestaltung.

Sollte durch das elektromobile Roaming die Notwendigkeit entstehen, eine Clearingstelle einzubeziehen, so müssten bereichsspezifische Regelungen geschaffen werden, welche die Datenübermittlung zwischen VNB, Clearingstelle und Lieferanten legitimieren. Zusätzlich müsste eine eventuelle Verarbeitung der Daten durch die Clearingstelle ebenfalls legitimiert werden.

ANALYSE – FAHRZEUGZUSTANDSINFORMATIONEN

Die als exemplarisches Beispiel für Fahrzeuginformationen im Referenzbeispiel gewählten Batteriezustandsdaten müssen ebenfalls vom MSB/MDL ausgelesen werden, da nur dieser Zugriff auf die Ladestation hat. In Betracht kommt, dass der MSB/MDL hier im Rahmen einer Auftragsdatenverarbeitung als Auftragnehmer gemäß § 11 BDSG tätig wird. Problematisch ist hier allerdings, dass wohl kaum davon ausgegangen werden kann, dass Verträge zwischen sämtlichen Fahrzeuginformationsprovidern und allen MSBs/MDLs bestehen. Insofern ist eine Legitimation im Wege der Auftragsdatenverarbeitung hier nicht praktikabel.

Die anschließende Übermittlung der Daten an den Fahrzeugsinformationsprovider müsste durch einen Vertrag zwischen diesem und dem Betroffen legitimiert werden. Ein solcher Vertrag müsste auch die Einwilligung des Betroffenen enthalten, welche diese Übermittlung dann gemäß § 4 Abs. 1 BDSG legitimiert. Die Verarbeitung der Daten beim Fahrzeugsinformationsprovider müsste ebenfalls durch eine Einwilligung des Betroffenen im Rahmen des Vertragsschlusses legitimiert werden.

Hinsichtlich der Übermittlung der Batteriezustandsdaten vom Fahrzeugsinformationsprovider zum Hersteller müsste ebenfalls eine Einwilligung des Kunden vorliegen, welche ebenfalls im Rahmen des Vertragsschlusses erteilt werden kann.

ZWECKBINDUNG

ANALYSE

Hinsichtlich der Zweckbindung der Daten ergeben sich im Szenario Elektromobilität keine nennenswerten Unterschiede zum Szenario Smart Grid. Die erhobenen Daten werden vorrangig zum Zweck der Vertragserfüllung, mithin zur Abrechnung, und zudem auch für andere Zwecke, wie beispielsweise das Energiemanagement, benötigt. Zur näheren Erläuterung kann daher an dieser Stelle auf die obigen Ausführungen verwiesen werden.

Hingewiesen sei hier allerdings noch auf mögliche Mehrwertdienste. So ist beispielsweise vorstellbar, dass die Zustandsinformationen des Fahrzeugs dazu verwendet werden, dem Fahrer mittels Navigationssystemen den Weg zur nächsten (freien) Ladestation zu zeigen. Für solche Dienste müsste allerdings eine explizite Einwilligung des Kunden in die Verwendung der Daten bzw. deren Übermittlung zu diesen Zwecken vorliegen.

Zudem ist geplant, dem Kunden an der Ladestation auch individualisierte Werbung anzuzeigen. Sollten die personenbezogenen Daten auch für diese Zwecke verwendet werden sollen, müsste auch hier eine explizite Einwilligung eingeholt werden.

ERFORDERLICHKEIT

ANALYSE

Auch im Elektromobilitätszenario stellt sich die Frage, welche Daten von den beteiligten Marktakteuren tatsächlich benötigt werden.

Der Lieferant benötigt die Daten zu Abrechnungszwecken. Folglich benötigt er die Messwerte in einer der Tarifierungangepassten Weise. Sollte ein Tarif vereinbart sein, welcher nur zwischen HT und NT unterscheidet, so reicht die Datenübermittlung an den Lieferanten zweimal am Tag. Der VNB benötigt die Messwerte hingegen für verschiedene Zwecke. Zum einen benötigt er sie für das Netzmanagement,hierzu muss er die jeweils aktuellen Einspeise- und Ausspeisewerte sehen (und auch erfassen?) können. Hierzu wäre es für den VNB von Vorteil, Messdaten nahezu in Echtzeit zu erhalten.

Bislang werden die Netze in Bezug auf Haushaltskunden ohne diese Daten stabil gehalten, indem auf sogenannten Standardlastprofils zurück gegriffen wird, die nach dem vermuteten regelmäßigen Verbrauch von Haushaltskunden erstellt wurden. Dem lag das Prinzip zugrunde, dass stets so viel Strom produziert bzw. vorgehalten wurde, wie die Kunden benötigten. In Zukunft soll jedoch verstärkt die aktuelle Stromproduktion (dayahead-Prognose z. B. des erwarteten Windstroms) bestimmen, wann wie viel Strom von welchen Kunden abgenommen wird/werden sollte. Auf diese Weise könnten Lastspitzen aufgrund einer hohen Windproduktion effektiver abgefedert werden als dies heute möglich ist. Dadurch soll zugleich das Entstehen von wastedgreen Energy vermieden oder doch zumindest gemindert werden. Zugleich soll im stärkeren Maße aus Gründen des Klimaschutzes Strom aus Erneuerbaren Energien in die Netze aufgenommen werden und auch beim Kunden ankommen.

Zum anderen benötigt der VNB die Messwerte auch zur Abrechnung der angefallenen Netzentgelte. Hierbei würden jedoch ebenfalls wie im Falle des Lieferanten Messdaten in der Granularität des jeweiligen Tarifes ausreichen. Sollten die Netzentgelte nicht variabel sein, so würden hierzu wohl auch aggregierte Werte ausreichen.[122]

Der MSB/MDL ist vertraglich verpflichtet, die Messwerte auszulesen. Dies ist der Hauptzweck des Messvertrages gemäß § 3 MessZV. Die einzelnen Messwerte selbst benötigt er hingegen nicht. Zu Abrechnungszwecken reicht es ihm aus, wenn er weiß und belegen kann, wie oft eine Messung durchgeführt wurde. Eine Verwendung der Inhaltsdaten zu eigenen Zwecken ist nicht erforderlich.

Welche Datenverwendung für die Aufgabenerfüllung der Clearingstelle erforderlich ist, muss an dieser Stelle noch offen bleiben, da noch nicht hinreichend geklärt ist, welche Aufgaben ihr in der Prozesskette zukommen sollen. So könnte es möglich sein, dass die Clearingstelle lediglich Routingfunktionen erfüllt und somit überhaupt keine einzelnen Messwerte benötigt, sondern nur wissen muss, wer Empfänger der Daten ist. Sollte sie allerdings auch Abrechnungsaufgaben wahrnehmen, so benötigt sie natürlich die zur Abrechnung jeweils erforderlichen Messwerte.

[122] I.Ü. wird auf die Ausführungen im ersten Teil verwiesen.

Aus der Perspektive der eichrechtlichen Nachvollziehbarkeit ergeben sich im Rahmen der Abrechnung besondere Herausforderungen an die Erforderlichkeit von Datenverwendungen. Das Eichrecht fordert, dass die Abrechnung für den Kunden rückverfolgbar und nachvollziehbar sein muss.[123] Dies ergibt sich schon aus § 1 EichG sowie aus den PTB-A 50.7. Diese vom Eichrecht geforderte Nachvollziehbarkeit durch den Kunden ist allerdings im Bereich der Elektromobilität schwieriger zu erreichen als dies heute üblich ist. Derzeit hat jeder Kunde einen Heimzähler, der auf seinem eichpflichtigen Display[124] die Messwerte anzeigt. Im Bereich der Elektromobilitätsszenarien an öffentlichen Ladestationen besitzt der Kunde allerdings keinen Zähler mehr, an dem er seine Rechnung vergleichen kann. Es wird deshalb zu fordern sein, dass er seine Messergebnisse und gegebenenfalls vorhandene Anreiztarife in eichrechtlich sicherer, mit heutigen Hauszählern vergleichbarer Weise auch unter Nutzung von IKT einsehen kann. Dies ist einer der zentralen Unterschiede zwischen den derzeit in Einführung befindlichen Smart Metern und dem hier zugrunde gelegten Fall der Elektromobilität. Die einem bestimmten Vertrag zuzuordnende Energieentnahme wird nun nicht mehr über eine bestimmte, sondern prinzipiell über eine Vielzahl verschiedener Mess- und Zähleinrichtungen erfolgen.[125]

HANDLUNGSBEDARF

Sofern sich die Elektromobilitätszenarien verfestigen, wäre eine bereichsspezifische Festlegung der Granularität und zulässigen Empfänger der elektromobilitätsbezogenen Abrechnungsdaten sinnvoll.

DATENSPARSAMKEIT

Auch im Rahmen von Elektromobilitätsszenarien ist das datenschutzrechtliche Gebot von Datenvermeidung und Datensparsamkeit zu beachten. Demnach gilt es auch hier, die Erhebung, Verarbeitung etc. personenbezogener Daten je nach funktionaler Anforderung so weit wie möglich zu vermeiden bzw. die personenbezogenen Daten zu anonymisieren oder zumindest zu pseudonymisieren.

Aus dem Gesichtspunkt der Datensparsamkeit würde eine optimale Gestaltung von öffentlichen Ladestationen die Möglichkeit der Barzahlung oder auch aus der Telekommunikation bekannte Prepaid-Modelle unterstützen. Gleichwohl werden sich auch Sachgestaltungen finden, wo die Nutzerinteressen an einer bargeldlosen Abrechnung aus einer Hand überwiegen.

Für die letztgenannte Sachgestaltung ist daher zu klären, inwiefern sich die Mechanismen von Datenvermeidung, Anonymisierung und Pseudonymisierung auch im Rahmen des „bequemen“ Elektromobilitätszenarios anwenden lassen. Über das bereits oben betrachtete Szenario der elektronischen

[123] Bericht BNetzA, S. 64.

[124] § 7j Abs. 1 Nr. 1 EO in Verbindung mit MID RL. 2004/22/EG Anhang I 10.5; PTB-A 50.7 3.1.1.1.

[125] Zu diesen Fragestellungen siehe auch: Pallas/Raabe/Weis, CR Juni 2010 (im Erscheinen)

Haushaltszähler hinaus sind hier insbesondere diejenigen für die Elektromobilität spezifischen Fragen zu betrachten, die

- sich aus der Tatsache ergeben, dass spätestens im Zuge des Roamings personenbezogene Messdaten durch viele verschiedene MSBs/MDLs erhoben und explizit mit einer ID attributiert werden müssen,
- sich aus der Existenz neuer Marktrollen wie LSB oder Clearingstelle ergeben und die
- im Zusammenhang mit dem Ortsbezug der Messdaten und der sich daraus ergebenden Möglichkeit der Bildung von Bewegungsprofilen entstehen.

ANALYSE

Im Referenzszenario würden sowohl Identifikations- als auch aus der Stations- bzw. Zählernummer ableitbare Standortdaten vom jeweiligen MSB/MDL abgerufen und an den Lieferanten übermittelt. Dieser wäre damit in der Lage, detaillierte Bewegungsprofile seiner Elektromobilitätskunden zu erstellen. Spätestens nach Abschluss der Messung müssen zudem Zeit- und ID-attributierte Messwerte zur Stromentnahme an den Lieferanten übermittelt werden, aus denen dieser wiederum nicht nur ablesen kann, wann ein bestimmter Kunde sein Fahrzeug an eine Ladestation angeschlossen hat, sondern auch, wie lange das Fahrzeug an der gleichen Stelle stehen geblieben ist.

Betrachtet man nun das Szenario des Roamings zwischen unterschiedlichen Ladestationsbetreibern, so stellen sich die resultierenden Datenschutzrisiken noch umfangreicher dar. In der derzeitigen Pilotphase wird hier davon ausgegangen, dass dem Betreiber der im Rahmen des Roamings zu nutzenden Ladestation grundsätzlich immer die vollständige, aus Länderkennung, Anbieterkennung, Vertrags-ID und Prüfziffer bestehende ID des Kunden übermittelt wird.

Die vollständige Klartext-ID des Kunden stellt in diesem Zusammenhang mangels expliziten Personenbezugs ein Pseudonym dar, welches der LSB nicht ohne weiteres auflösen kann.[126] Andererseits bleibt eine Kunden-ID aber für einen vergleichsweise langen Zeitraum unverändert. Hieraus wiederum resultieren zumindest ein latentes Risiko der nachträglichen Auflösung des Pseudonyms und damit auch das Risiko der Erstellung personenbezogener Bewegungsprofile durch den LSB. Ähnliches gilt auch für die zukünftig zu berücksichtigenden, fluktuierend eingeschalteten MSBs/MDLs, welche die Zeit- und ID-attributierten Messwerte aus den Ladestationen auslesen und weiterleiten, sowie für die zukünftig zu erwartenden Regelenergie-Aggregatoren und Zusatzdienste-Anbieter.

HANDLUNGSBEDARF

Angesichts der besonderen Aussagekraft der zumindest implizit ortsbezogenen Messdaten und der gegenüber dem Szenario der elektronischen Hauszähler nochmals signifikant vergrößerten Anzahl potentiell beteiligter Akteure sind im Bereich der Elektromobilität zusätzliche Maßnahmen zur

[126] Es wird hier davon ausgegangen, dass unter keinen Umständen zur Auflösung notwendige Angaben wie beispielsweise komplette Vertragsdatensätze zwischen den unterschiedlichen Akteuren ausgetauscht werden.

Datenvermeidung und Datensparsamkeit unverzichtbar.[127] Der Verwendung einer Klartext-ID deutlich vorzuziehen wäre daher die bereits oben skizzierte Verwendung temporärer, beispielsweise täglich wechselnder Pseudonyme, die ausschließlich durch den Heimlieferanten aufgelöst und somit einem bestimmten Kunden zugeordnet werden können. Würden diese Pseudonyme im Zuge fortgeschrittener Kommunikationsmodelle zwischen Fahrzeug und Ladestation bereits im Fahrzeug generiert und in der Ladestation zur ID-Attributierung der Messwerte verwendet, dann wäre sowohl für den LSB als auch für den auslesenden MSB/MDL keine Bildung langfristiger Bewegungsprofile mehr möglich. Eine Profilbildung durch eine eventuell zu etablierende Clearingstelle wäre ebenfalls ausgeschlossen. Die Autorisierung durch den Heimlieferanten ließe sich ebenfalls auf Basis solcher temporärer Pseudonyme realisieren, indem der Heimlieferant dem LSB „Übernahmeerklärungen" in Form kryptographisch signierter Tickets ausstellt.

Anstatt mit einer Klartext-ID sollte die Anmeldung an der Ladestation und die ID-Attributierung von Messdaten auf Basis temporärer, nur durch den Heimlieferanten des jeweiligen Kunden auflösbarer Pseudonyme realisiert werden. Für die Autorisierung durch den Heimlieferanten sollten auf solchen temporären Pseudonymen aufbauende Ticketing-Verfahren zum Einsatz kommen.

Auch bei Verwendung der so skizzierten Pseudonyme muss der Heimlieferant in jedem Fall in der Lage sein, die Pseudonyme aufzulösen und die entsprechenden (Mess-) Datensätze seinen Kunden zuzuordnen. Anders als im Kontext der Hauszähler sind diese Daten jedoch zumindest mittelbar ortsbezogen und würden es dem Heimlieferanten ermöglichen, Bewegungs- oder Nutzungsprofile seiner Kunden zu erstellen. Eine Datenübermittlung vom LSB oder MSB/MDL ohne Zählernummer und damit ohne Ortsbezug scheidet jedoch aus eichrechtlichen Gründen kategorisch aus.

Eine grundsätzlich denkbare Möglichkeit bestünde jedoch in der Etablierung einer zusätzlichen Instanz, die den Ortsbezug (die Zählernummer) aus den mit Pseudonym-IDs versehenen (Mess-) Daten herauslöst und archiviert und die Daten daraufhin ohne Ortsbezug neu signiert und an den Heimlieferanten weiterleitet. Beides müsste selbstverständlich in eichrechtlich sicherer Form, also durch eine diesbezüglich geprüfte und zugelassene Software, geschehen. Da eine solche Instanz lediglich auf mit temporären Pseudonymen attributierten Daten arbeiten würde, wäre eine Profilbildung auch hier ausgeschlossen. Eine Zusammenführung von entpseudonymisierten Daten und Ortsangaben dürfte dann lediglich in bereits vorab klar definierten Ausnahmefällen wie zur Validierung einer durch den Kunden angezweifelten Abrechnung geschehen. Eine solche Instanz könnte beispielsweise bei einer zu etablierenden Clearingstelle angesiedelt sein.[128] Weniger viel versprechend erscheinen hingegen Modelle der getrennten Speicherung, die komplett innerhalb des Einflussbereiches des Heimlieferanten realisiert werden.

[127] Die für den Bereich der elektronischen Haushaltszähler formulierten Empfehlungen zur aggregierten und damit anonymisierten Übertragung von Messdaten an den Netzbetreiber, zur Integration von Vorgaben zur datenschutzfreundlichen Technikgestaltung in den eichrechtlichen Rahmen und zur kritischen Diskussion der derzeitigen Vorgaben der BNetzA zu Prozessen und Datenformaten gelten selbstverständlich auch für den Bereich der Elektromobilität.

[128] Siehe auch Raabe/Lorenz/Schmelzer, it-Information Technology, 2010, 107 ff.

Bezüglich der Integration von Zusatzdienste-Anbietern oder Regelenergie-Aggregatoren stellt sich mittelfristig zudem die Frage nach der datensparsamen – also möglichst pseudonymen – und dennoch rechtssicheren Realisierung bidirektionaler Kommunikation. Sollen Fahrzeuge am Markt für Regelenergiedienstleistungen auftreten können, so muss einerseits Datensparsamkeit gegenüber den jeweiligen Vertragspartnern gewährleistet sein, andererseits muss es im Fall der Nichterbringung einer zugesagten Regelenergieleistung möglich sein, eine solche Nichterbringung auch zu sanktionieren. Erbrachte Leistungen müssen wiederum auch vergütet werden können. Moderne Verfahren, die auf der Ausstellung temporärer beglaubigter Pseudonyme (Pseudonymzertifikate) durch eine vertrauenswürdige dritte Instanz[129] basieren, erscheinen hierfür durchaus geeignet und könnten die Grundlage für datenschutzfreundliche und gleichzeitig sichere Aktivitäten auf dem elektronischen Energiemarktplatz bilden.

Zur Vermeidung der Bildung von Bewegungsprofilen durch den Heimlieferanten sollten die an ihn übermittelten Daten keinen (mittelbaren) Ortsbezug enthalten. Eichrechtlich relevante Verpflichtungen an die Nachvollziehbarkeit und das Gebot der Datensparsamkeit sollten durch die Etablierung von temporären Pseudonymen, die durch eine vertrauenswürdige dritte Instanz (TrustedThird Party) beglaubigt sind, zum Ausgleich gebracht werden.

NUTZERRECHTE

Die bereits für das erste Referenzszenario diskutierten, aus § 35 BDSG erwachsenden Ansprüche auf Berichtigung, Löschung und Sperrung von Daten sind auch für Szenarien der Elektromobilität zu gewährleisten. Die obigen Ausführungen zur Löschung bzw. Sperrung nebst expliziter Fristen, zur Übermittlung in Drittstaaten und zur regelbasierten Repräsentation der Nutzerrechte behalten somit auch im Kontext der Elektromobilität ihre Gültigkeit.

ANALYSE

Die besonderen Gegebenheiten der Elektromobilität unterstreichen die Notwendigkeit der skizzierten Maßnahmen zum regelbasierten Zugriffsschutz[130] nochmals. Angesichts der Tatsache, dass im Rahmen von Elektromobilität die Anzahl relevanter Akteure mit diversen, ständig wechselnden LSBs und MSBs/MDLs, Aggregatoren, Zusatzdienste-Anbietern, etc. signifikant steigen wird, werden klassische Mechanismen zur Wahrnehmung von Nutzerrechten kaum mehr praktikabel sein. Diesem Umstand muss durch eine geeignete Ausgestaltung des technischen und rechtlichen Rahmens Rechnung getragen werden.

[129] Zum grundsätzlichen Ansatz der Verwendung solcher Pseudonymzertifikate im Rahmen der Verkehrstelematik, siehe beispielsweise Sichere Intelligente Mobilität Testfeld Deutschland : Deliverable D21.5 – Spezifikation der IT -Sicherheitslösung, S. 127 ff. Online unter http://www.simtd.de/news/publications [11.05.2010]

[130] Vgl. auch Raabe in Fischer/Maehle/Reischuk, S. 191.

HANDLUNGSBEDARF

Um den Nutzern auch in einem so komplexen Umfeld wie der Elektromobilität die Möglichkeit zu geben, in effektiver und effizienter Art und Weise von Ihren Rechten Gebrauch zu machen, sind die bereits oben skizzierten Maßnahmen auch auf die im Rahmen der Elektromobilität hinzukommenden Akteure und Prozesse auszuweiten.

Die explizite Statuierung bereichsspezifischer Lösch- und Sperrfristen ist auch auf die im Rahmen von Elektromobilität hinzukommenden Akteure (LSB, Aggregatoren, Zusatzdienste-Anbieter sowie ggfs. eine Clearingstelle) auszuweiten. Angesichts der nochmals signifikant erhöhten Komplexität erscheinen zudem regelbasierte technische Systeme für eine effektive und effiziente Wahrnehmung von Nutzerrechten unverzichtbar.

TRANSPARENZ

ANALYSE

Bereits diskutiert wurde die Frage, ob das Auslesen eines Zählers noch dem Grundsatz der Direkterhebung entspricht, da hierbei grundsätzlich keine Beteiligung des Kunden erfolgt. Im Rahmen der Elektromobilität stellt sich dieses Problem jedoch noch einmal anders da. Im Gegensatz zum Haushaltszähler hat der Kunde an einer öffentlichen Ladestation keinerlei Rechte an dem dort verwendeten Zählern. Er übt mithin nicht die Sachherrschaft über das Messgerät aus. Allerdings wurde bereits festgestellt, dass der datenschutzrechtliche Schutz im Szenario Elektromobilität bereits mit dem Auflaufen der Daten auf dem Zähler beginnen muss. Die Daten können aber erst dann auf den Zähler auflaufen, wenn der Kunde aktiv sein Fahrzeug an die Ladestation angeschlossen und sich angemeldet hat. Eine Mitwirkung des Betroffenen liegt zweifelsfrei in den Fällen vor, in denen der Kunde sich selbst mittels einer RFID-Karte identifiziert. Durch das Benutzen der Karte an der Ladestation ist der Mitwirkungspflicht Genüge getan.

Davon zu unterscheiden ist die Mitwirkung des Kunden in den Fällen, in denen sich wie zukünftig vorgesehen, das Fahrzeug selbsttätig identifiziert. Der Betroffene kennt die Identifikation des Fahrzeugs. Zudem wird diese erst durch das Anschließen an der Ladestation ausgelöst. Das Anschließen reicht hierbei aus, um dem Erfordernis des § 4 Abs. 2 BDSG gerecht zu werden.

Problematisch ist dann jedoch, dass hier personenbezogene Daten zwar unter Mitwirkung des Fahrzeugnutzers erhoben werden, diese Daten möglicherweise jedoch den Personenbezug zu jemand anderem, dem Fahrzeughalter herstellen.[131] § 4 Abs. 2 BDSG verlangt die Mitwirkung des Betroffenen. Betroffener ist nach § 3 Abs. 1 BDSG eine bestimmte oder bestimmbare natürliche Person. In diesem Fall ist die bestimmbare Person der Fahrzeughalter.

[131] Es wird hier davon ausgegangen, dass sich, wie von diversen Akteuren derzeit vorgesehen, ein Fahrstrom-Vertrag auf eine Fahrzeug-ID bezieht. Die alternative Möglichkeit der Nutzeridentifikation beispielsweise auf Basis personengebundener und vom Fahrzeug zu Identifikationszwecken ausgelesener Smart Cards würde zwar u.a. das im Folgenden dargestellte Problem entschärfen, ist aber noch nicht ausreichend diskutiert.

Allerdings stellt sich die Situation ähnlich dar wie im Telekommunikationsmarkt. Sollte jemand anderes als der Anschlussinhaber das Telefon benutzen, so werden die Verbindungsdaten dennoch mit der Person des Anschlussinhabers verknüpft. Das Mitwirken des Anschlussinhabers bei jedem Telefonat stellt sich allerdings als unverhältnismäßig im Sinne von § 4 Abs. 2 Nr. 2 b) BDSG dar. Zudem liegen keinerlei Anhaltspunkte für ein schutzwürdiges Interesse des Betroffenen, der Vertragsinhaber ist, vor. Im Bereich der Elektromobilität würde insofern das Mitwirken des Vertragsinhabers bei jedem Vorgang der Erhebung ebenfalls einen unverhältnismäßigen Aufwand im Sinne dieser Vorschrift darstellen.

HANDLUNGSBEDARF

Da dem Betroffenen gegenüber die Struktur und die Schritte der Datenverwendungen gleichwohl auch bei der Nutzung von öffentlichen Ladestationen zugänglich gemacht werden müssen, stellt sich die Frage nach dem Adressaten dieser Pflicht. Insofern wäre auch hier eine bereichsspezifische Bestimmung des insofern Verantwortlichen sinnvoll. Anders als im Referenzszenario Smart Meter ist eine Verantwortlichkeit der wechselnden Ladestationsbetreiber und MSB/MDL nicht praktikabel.

Es sollte bereichsspezifisch bestimmt werden, dass der Vertragspartner des Kunden, mithin im Szenario der Heimlieferant, Verantwortlicher für datenschutzrechtliche Informationen in den Elektromobilitätszenarien des Roaming ist.

TEIL III : REGULIERUNGSTHEORETISCHE FRAGEN

Auf Basis der in Teil I und Teil II vorgenommen Analysen im Hinblick auf die geltende Rechtslage sollen nun noch die regulierungstheoretischen Implikationen in den Blick genommen werden. In dieser Sicht ist damit die Frage nach dem systematisch richtigen normativen Rahmen der Datenschutzregelungen zum Smart Grid gemeint. Es kommt insofern grundsätzlich in Betracht es bei den allgemeinen Regelungen des BDSG zu belassen, oder ein neues bereichsspezifisches Schutzprogramm z. B. nach telekommunikationsrechtlichem Vorbild, im Energiewirtschaftsrecht zu verankern.

Im Spannungsfeld von Datenschutz, Rechtssicherheit für die Marktakteure und Innovationsoffenheit zur bestmöglichen Erreichung der Effizienzziele, stellt sich zudem noch die Frage nach der Ausgestaltung der positiven Regulierungstiefe im Optionenraum von ordnungspolitischen bis zu kooperativen, selbstregulierenden Maßnahmen. Diese Fragen unterscheiden sich insofern nur unwesentlich von den zuletzt in den Szenarien der Nutzung von RFID angeführten Problemlagen. Dies gilt insbesondere unter der Prämisse der in den Beispielen gezeigten unsicheren Arbeitshypothesen zur tatsächlichen Entwicklung des Smart Grid. Mit den im Fragenkreis des Einsatzes von RFID und anderen komplexen Informationssystemen gewonnenen datenschutzrechtlichen Erfahrungen können sich aber Anhaltspunkte für eine sinnvolle Ausgestaltung im Hinblick auf die neue Herausforderung gewinnen lassen.[132]

[132] Siehe auch Raabe, DuD 2010 (im Erscheinen)

BEREICHSSPEZIFISCHE REGELUNG

Einer bereichsspezifische Anreicherung des Energiewirtschaftsrechts um Datenschutzaspekte könnte, wie es sich schon jüngst bei der vergleichbaren Diskussion um die datenschutzrechtliche Beurteilung von RFID-Technologien angedeutet hat, grundsätzlich entgegengehalten werden, dass die Flexibilität von Selbstverpflichtungen im Bereich moderner Technikgestaltung im Gegensatz zu starren gesetzlichen Regelungen differenziertere Lösungen ermöglicht. Für den Verzicht auf ordnungsrechtliche Eingriffe könnte auch hier ins Feld geführt werden, dass die Selbstverpflichtung offener für neue datenschutzrelevante Entwicklungen sei und dadurch die Wettbewerbsfähigkeit und das Innovationspotential der betroffenen Unternehmen weniger einschränke.[133]

Dieser pauschalen Aussage kann allerdings nicht gefolgt werden. Es ist das Wesen moderner Technikgestaltung, dass sie mit prognostischen Unsicherheiten belastet ist. Damit wird die gesetzliche Ex-Ante-Steuerung der Datenverarbeitung angesichts der dynamischen Entwicklung von Technik und Anwendungen zunehmend schwierig.[134] Eine mit einem umfassenden Verweis auf eine wie auch immer geartete Selbstverpflichtung einhergehende, pauschale Verlagerung der Prognoserisiken auf den Grundrechtsträger der Informationellen Selbstbestimmung, durch eine totale Verweigerung normativer Grundsatzentscheidungen, ist aus verfassungsrechtlicher Sicht unzulässig.

Auf der anderen Seite ist im Bereich des Energiewirtschaftsrechts das marktliche Wissen um notwendige Geschäftsprozesse des Kernmarktes schon im bestehenden Rechtsrahmen verankert. So sind im Bereich des Messwesens die damit verbunden Verarbeitungsschritte und Legitimationstatbestände schon heute weitgehend energiewirtschaftsrechtlich normiert. Auch wenn die Komplexität der Marktprozesse zukünftig deutlich steigen wird, handelt es sich gleichwohl um ein auch zukünftig einheitlich zu betrachtendes Marktsystem, bei dem aus Gründen der Versorgungssicherheit eine enge normative Verortung neuer Marktakteure und Prozesse zu erwarten steht. Zudem zeigt die Gesamtschau der vorliegenden Szenarioanalysen im 1. und 2. Teil dieser Empfehlungen, dass an vielen Stellen eine Beurteilung allein nach den Vorgaben des BDSG nicht zu Ergebnissen führt, die den hier notwendigen Interessenausgleich sachgerecht abbildet. Insofern bietet es sich an, bei der notwendigen Anreicherung des materiellen Rechts auch zugleich die datenschutzrechtlichen Implikationen zu gestalten. Daraus leitet sich folgende grundsätzliche Empfehlung ab:

> Das Energiewirtschaftsrecht sollte nach dem Vorbild des vergleichbaren Telekommunikationsrechts grundsätzlich um einen Abschnitt „Datenschutz“ bereichsspezifisch angereichert werden.

In der Literatur wird darüber hinaus auch noch die Einführung eines Energiegeheimnisses nach dem Vorbild der besonderen Geheimhaltungsverpflichtungen für Telekommunikationsdiensteanbieter,

[133] So für RFID, Bundesregierung, Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie. Deutscher Bundestag, Drucksache 16/789, S. 13.

[134] Ladeur, DuD 2000, 12, 16.

Ärzte oder Rechtsanwälte vorgeschlagen. Da Energieversorger, Netzbetreiber und Messstellenbetreiber je nach Ausgestaltung des Energieinformationsnetzes in eine ähnliche Rolle wie die genannten Berufsträger hineinwachsen können, sei der Betroffene auch bei den Energiedaten auf eine vergleichbare Vertrauensbeziehung angewiesen.[135]

Im Ergebnis erreicht die Statuierung einer solchen besonderen Pflicht im Verhältnis zum bestehenden allgemeinen Datengeheimnis aus § 5 Abs. 1 BDSG über die Strafbewährung des § 203 StGB bzw. 206 StGB eine Verstärkung durch den ausgeprägteren Sanktionsrahmen. Es stellt sich allerdings die Frage, ob in einem entwicklungsoffenen System wie dem SmartGrid, welches aus Gründen der Enegieeffizienzsteigerung durch Verbesserung der informatorischen Basis gerade auf die zugleich zu verwirklichende Innovationsfreundlichkeit des gesetzlichen Rahmens angewiesen ist, die Statuierung eines solchen in erheblichem Maße strafbewehrten Sanktionsmechanismus den Zielkonflikt zwischen informatorisch gefördertem Klimaschutz und erforderlicher Grundrechtssicherung sinnvoll auflösen kann. Dies wird einerseits der historischen Entwicklung der einzelnen adressierten Tatbestände des besonderen Geheimnisschutzes nicht gerecht. Auf der anderen Seite würden lediglich die Akteure des Energiekernmarktes im Hinblick auf die bei Strafbewehrung notwendige Bestimmtheit adressiert, wohingegen, wie das Beispiel von zukünftigen Energieeffiziendiensten und Mehrwertleistungen im Markt der Elektromobilität zeigt, die eigentlichen datenschutzrechtlichen Gefahrenlagen des Smart Grid gerade in diesen Folgeszenarien entstehen.

REGULIERUNGSINSTRUMENTE

Auf einem anderen Blatt steht allerdings die Frage nach den dann sinnvoll zu verwendenden verfahrensrechtlichen und materiellen datenschutzrechtlichen Regulierungsinstrumenten. Es steht also in Frage, was in datenschutzrechtlicher Hinsicht bzgl. des Smart Grid wie geregelt werden soll. Im Gegensatz zu der vorhandenen gesetzlichen Marktgestaltung, welche einen überschaubaren Kreis von Akteuren mit klaren Rollenzuweisungen und Kommunikationsbedürfnissen abbildet, ist die Prognose im Hinblick auf die zur Energieeffizienzsteigerung notwendige Öffnung des Marktes und mithin datenschutzrelevanter neuer Rollen, Kommunikationsbeziehungen und Verarbeitungsschritten nur schwer vorhersagbar. Da die diesbezügliche rechtswissenschaftliche Diskussion um die Realisierung von regulierter Selbstregulierung im Datenschutz[136] bislang keine konkrete Ausgestaltung oder gar eine gesetzliche Normierung erfahren hat, kann insofern nicht auf Erfahrungswissen zurückgegriffen werden. **Als Besonderheit für die hier gegenständliche Sachgestaltung ist festzuhalten, dass der Begriff der Innovationsoffenheit für zukünftige Technikgestaltungen nicht nur abstrakte Dimension besitzt, sondern im Hinblick auf die Effektivierung von Klimaschutzaspekten eine auch legislativ zwingende Größe darstellt**. So ist z. B. im Smart Grid davon auszugehen, dass entsprechend den neueren Trends zu Service-orientierten Architekturen auch innovative Modelle kombinatorischer Energieeffizienzdienstleistungen kostengünstig zu gestalten sein werden[137] und einen erheblichen Beitrag zum Klimaschutz leisten können.

[135] Vgl. Roßnagel/Jandt, S. 39.

[136] Siehe nur: Hoffmann-Riem, S. 513 ff.; Roßnagel in Roßnagel, S. 387 ff.

[137] Dies deutet sich beispielsweise beim Google PowerMeter an. Siehe http://www.google.org/powermeter/ [11.05.2010]

ORDNUNGSRECHT

Für die Absicherung der datenschutzrechtlichen Prinzipien ist deshalb zukünftig von einem Maßnahmenbündel auszugehen, welches einerseits im sicher erschlossenen Bereich der energiewirtschaftsrechtlichen Kernmärkte einen unbedingten, ordnungsrechtlich normierten Bestand an materiellen Vorgaben zur Datenverarbeitung enthält. Auf der anderen Seite dürfte im Bereich der prognostisch nicht sicher erfassbaren System- und Technikgestaltungen ein Ansatz Erfolg versprechend sein, der auf kooperative Gestaltung setzt.

In der klassischen Diskussion um Selbstregulierung im Datenschutz zeigt sich ein immanenter Fehler zum einen der Abwesenheit von Sanktionsmechanismen bei Verweigerung des privaten Tätigwerdens. Auf der anderen Seite bedarf es einer Neubewertung des Verständnisses, dass selbstregulative Maßnahmen lediglich dann greifen können, wenn sie über das bestehende Schutzprogramm hinausgehen.[138] Die Frage nach sinnvollen Datenschutzmechanismen in zukünftigen Sachgestaltungen der Technikentwicklung im Smart Grid sollte aber, wegen der größeren Nähe der betroffenen Kreise zur Technik, gleichwohl Gegenstand von kooperativ gestalteten Erkenntnisprozessen sein.

Dazu bedarf es zu einer sinnvollen Durchsetzung der kooperativ gewonnen Vorgaben eines imperativ wirkenden und ordnungsrechtlich sanktionierten Befehls. Die insofern bislang gelegentlich im Bereich der datenschutzrechtlichen Selbstregulierung angestrebte Verweisung auf eine privatrechtliche Durchsetzung der Sanktionsmechanismen muss im Rahmen der sich aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG ergebenden Schutzpflichten, gerade im Bereich unsicherer Prognoselagen, im Kern beim Staatssouverän verbleiben, weil er ansonsten das Risiko, welches mit solchen Prognosen verbunden ist, auf den sachunkundigen Bürger abwälzte. Die in der Diskussion um die Selbstregulierung vertretene, zivilistisch geprägte Position, welche aus Gründen einer eigentumsrechtlich motivierten Betrachtung[139] des Gegenstandes „Information“ eine durch Art. 14 GG (analog)[140] terminierte Betrachtung aller diesbezüglichen Sachgestaltungen in den Markt weisen will, verkennt die Reichweite dieser auch bei privatem Handeln bestehenden Prognoseverantwortung des Staates. Dies zeigt sich gerade bei der Entwicklung komplexer, die Daseinsvorsorge stützender, privater Informationssysteme wie dem Smart Grid.

Auf der anderen Seite erfordert die Ausgestaltung von Kommunikationsinfrastrukturen des Energiemarktes erhebliche Investitionen, die letztlich auch aus Gründen der Rechtssicherheit eine verbindliche staatliche Abschlussentscheidung verlangen.

KOOPERATIVE VERFAHREN

Um die vorgenannte Anforderung zu erfüllen, muss damit im Hinblick auf die einzelnen normierungsbedürftigen materiellen Tatbestände einerseits das Wissen aller betroffenen Kreise bestmöglich in den Prozess der legislativen Erkenntnisgewinnung eingebracht werden. Auf der anderen Seite ist aus **Gründen des notwendigen Investitionsschutzes und der im Energiesektor**

[138] Bizer, DuD 2003, 394.

[139] Vgl. Kilian in Bizer/Lutterbeck/Rieß, S. 152.

[140] Vesting, S. 189.

grundlegenden Gewährleistung von Versorgungssicherheit ein Höchstmaß an Rechtssicherheit bei hinreichender Flexibilität zur Anpassung an zukünftige Technik- und Geschäftsmodell-entwicklungen, mithin Innovationsoffenheit, zu realisieren.

Im einschlägigen Sachbereich der Energiewirtschaft liegt es insofern nahe, sich methodisch am Rechtsgedanken des Festlegungsverfahrens (§§ 21b i. V. m. §29 EnWG) als Schema auch für die Auflösung der hier adressierten Zielkonflikte zu orientieren.

Das nach §§ 21b Abs. 4 i. V. m. 29 EnWG eingeführte Festlegungsverfahren im Messwesen ist so ausgestaltet, dass die Bundesnetzagentur im Rahmen von Konsultationen der betroffenen Kreise gesetzlich geforderte Zielvorgaben formuliert. Von den Verbänden der Marktakteure werden sodann konkrete technische Spezifikationen erarbeitet, welche nach weitergehenden Konsultationen von den Beschlusskammern der BNetzA als allgemeinverbindlich erklärt werden. Rechtstechnisch handelt es sich bei der Festlegung um einen allgemeinverfügenden Verwaltungsakt. Dieser Akt steht allerdings unter der Prämisse eines gesetzlich angeordneten Änderungsvorbehaltes. Durch diese Verfahrensgestaltung können also die Kenntnisse der betroffenen Kreise um eine sinnvolle Sachgestaltung sehr frühzeitig in den Entscheidungsprozess eingebracht werden und gleichzeitig unter der Ägide der sachgerechten Ermessensausübung eine im Vergleich zur unmittelbaren gesetzlichen Normierung flexible Änderung herbeigeführt werden, wenn sich innovationshemmende Wirkungen der Festlegungen zeigen. Gleichzeitig verbleiben die Sanktionsmechanismen und die Bestimmung der Umsetzungsfristen allein beim staatlichen Souverän. Im Hinblick auf das weitgehend zu konstatierende Versagen der bisherigen ordnungsrechtlichen Ansätze des Datenschutzes in Bereichen weniger komplexer Technikgestaltungen dürfte diesem Ansatz aus Gründen der Effektivierung des Grundrechtsschutzes auch nicht das Wesentlichkeitsprinzip entgegenzuhalten sein, als die Formulierung der (neutral formulierten) Zielvorgaben beim Gesetzgeber verbleiben kann.

Der ordnungsrechtliche Rahmen eines zukünftigen Datenschutzrechts für personenbezogene Energiedaten sollte zwischen klar definierten Vorgaben für die Akteure der Energiekernmarktes und flexibleren Vorgaben für die Randbereiche von Energieeffizienzdienstleistungen differenzieren. Im Rahmen von gesetzlich strukturierten Mitwirkungsverfahren nach dem Vorbild des Festlegungsverfahrens nach § 21b EnWG sollte von der Möglichkeit der Integration des Sachverstandes der Marktakteure des Energiemarktes Gebrauch gemacht werden.

FAZIT

Bei der datenschutzrechtlichen Bewertung von Aspekten des Smart Grid ist zu beachten, dass es sich um ein entwicklungsoffenes System handelt, welches dem gesamtgesellschaftlich relevanten Ziel der Verbesserung des Klimaschutzes dient.

Die Analyse der Referenzszenarien hat gezeigt, dass eine abschließende datenschutzrechtliche Bewertung der Herausforderungen des Smart Grid und mithin diesbezügliche Empfehlungen zum derzeitigen Zeitpunkt nicht möglich sind. Auf der anderen Seite ist es zwingend geboten, schon bei der beginnenden Entwicklung der technischen Infrastruktur für das Smart Grid wesentliche Weichen zu stellen.

Neben einer notwendigen Verbesserung der Faktenbasis für die rechtliche Bewertung durch Modellierung von datenschutzrelevanten Sachverhalten sind nach dem Paradigma des „Privacy by Design“ schon heute Entwurfsmuster für technisch wirkende, flexible und entwicklungsoffene Schutzmechanismen in der Systemarchitektur zu entwickeln. Aus Gründen der Rechtssicherheit und des Investitionsschutzes sollte dies regulativ begleitet werden. Diese Herausforderung stellt sich als Querschnittsaufgabe dar, die alle Ebenen der zukünftigen Marktkommunikation betrifft.

Für die Architekten der zukünftigen IT-Infrastrukturen und der Geschäftsmodelle sollten die Begriffe „Datensparsamkeit“ und „Datensicherheit“ das Leitmotiv auch im Hinblick auf die notwendige Nutzerakzeptanz der Systeme sein.

Die Chancen des begonnenen Diskurses von Marktakteuren, Regulierung und Datenschutzaufsicht sollten auch zukünftig in legislativen Verfahren genutzt werden, die allen Aspekten von Klima- und Datenschutz zu einem bestmöglichen Ausgleich verhelfen.

Schließlich müssen die bestehenden gesetzlichen Verfahrensregelungen zur Transparenzsicherung für den Betroffenen im Hinblick auf die hohen Transaktionsfrequenzen, die Komplexität der Infrastrukturen und die Praktikabilität einer sinnerhaltenden bereichsspezifischen Revision unterzogen werden.

LITERATUR

Albrecht ,Astrid, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, 2003, Baden-Baden.
(zitiert: Albrecht)

Benz, Steffen, Energieeffizienz durch intelligente Stromzähler, ZUR 2008, 457.

Bericht BNetzA: Wettbewerbliche Entwicklungen und Handlungsoptionenim Bereich Zähl- und Messwesen und bei variablen Tarifen, 2010, online über www.bundesnetzagentur.de. [12.05.2010].
(zitiert: Bericht BNetzA)

Bizer, Johann, Mut zur Selbstregulierung, DuD 2003, 394.

Bizer, Johann, Sieben Goldene Regeln des Datenschutzes, DuD 2007, 350.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo, Bundesdatenschutzgesetz, 3. Auflage 2010, Frankfurt am Main.
(zitiert: Bearbeiter in Däubler/Klebe/Wedde/Weichert)

Danner, Wolfgang/Theobald, Christian ,Energierecht Kommentar, Stand: März 2009, München.
(zitiert: Bearbeiter in Danner/Theobald)

Fest, Claus/Franz, Oliver/Gaul, Armin, Energiewirtschaftliche und energiewirtschaftsrechtliche Fragen der Elektromobilität – Teil 2, Energiewirtschaftliche Tagesfragen Heft 5/2010.

Friedewald, Michael/Raabe, Oliver/Koch, Daniel J./Georgieff, Peter/Neuhäusler, Peter, UbiquitäresComputing - Zukunftsreport für das Büro für Technikfolgenabschätzung beim Deutschen Bundestag, Berlin 2010.
(zitiert: Friedewald/Raabe/Koch/Georgieff).

Göge, Marc-Stefan/Boers, Stefanie, Gläserne Kunden durch Smart Metering, ZNER 2009, 368.

Gola, Peter/Schomerus, Rudolf, Bundesdatenschutzgesetz Kommentar, 9. Auflage, 2007, München.
(zitiert: Gola/Schomerus)

Grabitz, Eberhard /Hilf, Meinhard, Das Recht der europäischen Union, Band IV, Stand: Oktober 2009, München.
(zitiert: Bearbeiter in Grabitz/Hilf)

Hoffmann-Riem, Wolfgang, Informationelle Selbstbestimmung in der Informationsgesellschaft – auf dem Wege zu einem neuen Konzept des Datenschutzes, In: Archiv des öffentlichen Rechts 123(4), 1998, S. 513.
(zitiert: Hoffmann-Riem)

Kilian, Wolfgang, Rekonzeptualisierung des Datenschutzrechts durch Technisierung und Selbstregulierung? In: Bizer/Lutterbeck/Rieß (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft – Freundesgabe für Alfred Büllesbach, 2002, S.151.
(zitiert: Kilian in Bizer/Lutterbeck/Rieß)

Ladeur, Karl-Heinz, Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken: Zur „objektiv-rechtlichen Dimension" des Datenschutzes, DuD2000, 12.

Pallas, Frank/Raabe, Oliver/Weis, Eva, Beweis- und eichrechtliche Aspekte der Elektromobilität, CR Juni 2010 (im Erscheinen).

Raabe, Oliver, Datenschutz im Internet der Energie, In:Fischer/Maehle/Reischuk (Hrsg.): Im Fokus das Leben, Proceedings zur Informatik 2009, GI-Edition-Lecture Notes in Informatics (LNI), S.191.
(zitiert: Raabe in Fischer/Maehle/Reischuk)

Raabe, Oliver, Datenschutz im Smart Grid – Anpassungsbedarf des Rechts und des Systemdatenschutzes, DuD 2010 (im Erscheinen).

Raabe, Oliver/Lorenz, Mieke/Schmelzer, Knut, Generic Legal Aspects of E-Energy, it-Information Technology, 2010, 107.

Roßnagel, Alexander, Das rechtliche Konzept der Selbstbestimmung in der mobilen Gesellschaft, In: Taeger/Wiebe (Hrsg.), Mobilität - Telematik – Recht, 2005, Köln.
(zitiert: Roßnagel in Taeger/Wiebe)

Roßnagel, Alexander, Datenschutz in einem informatisierten Alltag, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, 2007, Berlin, http://library.fes.de/pdf-files/stabsabteilung/04548.pdf [12.06.2010]
(zitiert: Roßnagel, Datenschutz in einem informatisierten Alltag)

Roßnagel, Alexander, Datenschutzaudit – Konzeption, Durchführung, gesetzliche Regelung, Braunschweig,Wiesbaden 2000.
(zitiert: Roßnagel, Datenschutzaudit)

Roßnagel, Alexander, Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, München.
(zitiert: Bearbeiter in Roßnagel, Handbuch Datenschutzrecht)

Roßnagel, Alexander/Jandt, Silke, Datenschutzfragen eines Energieinformationsnetzes, Rechtsgutachten im Auftrag der Alcatel-LucentStiftung für Kommunikationsforschung, Stand 26. März 2010, Kassel.
(zitiert: Roßnagel/Jandt)

Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen, Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministers des Innern, 2002, http://www.dud.de/dud/documents/modernisierung-dsrecht.pdf [12.05.2010].
(zitiert: Roßnagel/Pfitzmann/Garstka)

Schaffland, Hans-Jürgen/Wiltfang, Noeme, Bundesdatenschutzgesetz, Stand: März 2010, Berlin.
(zitiert: Schaffland/Wiltfang)

Simitis, Spiros, Bundesdatenschutzgesetz, 6. Auflage 2006, Baden-Baden.
(zitiert: Bearbeiter in Simitis)

Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein: Datenschutzrechtliche Bewertung desEinsatzes von „intelligenten“ Messeinrichtungen für die Messung von gelieferter Energie (SmartMeter),https://www.datenschutzzentrum.de/smartmeter/20090925-smartmeter.html[12.05.2010].
(zitiert: ULD-SH)

Vesting, Thomas, Das Internet und die Notwendigkeit der Transformation des Datenschutzes, In: Ladeur (Hrsg.): Innovationsoffene Regulierung des Internet, 2003, S. 155, Baden-Baden.
(zitiert: Vesting)

Wybitul, Tim, Wie viel Arbeitnehmerdatenschutz ist „erforderlich“?, BB 2010, 1085.