

Prof. Dr. Volker Lüdemann, Manuel Christian Ortmann LL.M., Patrick Pokrant LL.M.

## Datenschutz beim Smart Metering – Das geplante Messstellenbetriebsgesetz (MsbG) auf dem Prüfstand

*Die Digitalisierung der Energiewende nimmt Fahrt auf. Ihre Umsetzung soll die Elektrizitätsversorgung effizienter machen und auch die Verbraucherseite aktiv am Strommarkt beteiligen. Ein wichtiger Baustein auf diesem Weg ist nach dem Willen des Gesetzgebers die Einführung einer neuen Mess- und Kommunikationsinfrastruktur. Mit dem Messstellenbetriebsgesetz (MsbG) wird die rechtliche Grundlage für*

*den verpflichtenden Einbau von intelligenten Messsystemen (sog. Smart Meter) gelegt. Das Gesetz soll noch in diesem Sommer in Kraft treten. Die Vorbehalte in der Bevölkerung sind jedoch groß. Grund hierfür sind vor allem Datenschutzbedenken. Der Beitrag zeigt die datenschutzrechtlichen Risiken auf und unterzieht den Gesetzentwurf auf dieser Grundlage einer ersten kritischen Würdigung.*

### I. Einleitung

Intelligente Messsysteme sind ein wichtiger Baustein für den Aufbau intelligenter Energieversorgungsnetze. Die bestehende Netzinfrastruktur ist auf den wachsenden Anteil erneuerbarer Energien nicht ausgelegt. Es fehlt vor allem an Flexibilität, um die wetterabhängige und dezentrale Einspeisung von Wind- und Sonnenenergie mit der Stromnachfrage in Einklang zu bringen. Intelligente Messsysteme bieten insoweit eine Lösung.<sup>1</sup> Mit ihrer Hilfe können vielfältige verbrauchsbezogene Messdaten generiert und über Kommunikationsschnittstellen für das Energieversorgungsnetz nutzbar gemacht werden.<sup>2</sup> Sie ermöglichen die kommunikative Vernetzung von Erzeugern, Verbrauchern und Speichern. Gleichzeitig bergen sie jedoch ein erhebliches Risikopotential für den Datenschutz. Dieses ergibt sich aus dem hohen Volumen an personenbezogenen Daten, das benötigt wird, um das Verhalten der Verbraucher und Energieerzeuger sinnvoll aufeinander abzustimmen. Zwischen einem möglichst umfassenden Datenschutz und der Generierung des vollen Nutzens aus dem Smart Metering bestehen insofern erhebliche Zielkonflikte.<sup>3</sup>

Heute erfolgt die Übermittlung der Messwerte in der Regel jährlich. Mit Einführung intelligenter Messsysteme steigt die Datenmenge und damit der Datenfluss aus dem Haushalt signifikant an. Die Daten geben nicht nur Auskunft über die Menge verbrauchter oder eingespeicherter Energie, sondern auch über den jeweiligen Zeitpunkt des Verbrauchs und der Einspeisung. Intelligente Messsysteme ermöglichen es damit in bisher unbekanntem Ausmaß, den Alltag der Verbraucher nachzuvollziehen, da ein Großteil der Alltagshandlungen mit Energieverbrauch verbunden ist.<sup>4</sup> Entsprechend groß ist die Skepsis in der Bevölkerung. Siebzig Prozent lehnt einen flächendeckenden Einsatz von Smart Metern ab, der Großteil hiervon wegen Datenschutzbedenken.<sup>5</sup> In den Niederlanden ist die Einführung von Smart Metern aufgrund ähnlicher Vorbehalte sogar zunächst gescheitert.<sup>6</sup> Der deutsche Gesetzgeber hat hieraus seine Schlüsse gezogen und den Aspekten des Datenschutzes und der Datensicherheit eine Schlüsselrolle im Messstellenbetriebsgesetz

zugedacht. Die Akzeptanz der Bevölkerung für den angestrebten flächendeckenden Einbau intelligenter Messsysteme soll damit erhöht werden.<sup>7</sup>

Der Beitrag analysiert nach einem kurzen Überblick über den Stand der Gesetzgebungsarbeiten (II.) und die Funktionsweise intelligenter Messsysteme (III.) die Herausforderungen für den Datenschutz (IV.). Auf dieser Grundlage wird anschließend untersucht, inwieweit die bestehenden Gefahren mit den Datenschutzbestimmungen des Messstellenbetriebsgesetzes aufgefangen werden können (V.). Ein Fazit schließt den Beitrag ab (VI.).

### II. Stand des Gesetzgebungsverfahrens

Die Einführung intelligenter Messsysteme geht auf die EU-Richtlinie 2009/72/EG<sup>8</sup> zurück. Als Teil des dritten Binnenmarktpaketes sieht sie die verpflichtende Ausstattung vor. Deutschland hat in Umsetzung der Richtlinie im Jahre 2011 gesetzliche Grundlagen für den Flächenausbau intelligenter Stromnetze und Stromzähler geschaffen.<sup>9</sup> Im Zuge der No-

1 BMWi, Pressemitteilung vom 17.01.2013: Smart Grids – Intelligenz entlastet Stromnetze; Roß, in: Servatius/Schneidewind/Rohlfing (Hrsg.), Smart Energy – Wandel zu einem nachhaltigen Energiesystem, S. 287 ff.; Seifert, ebd., S. 261; Pfändler, Smart Meter und Smart Grids, S. 4; Guckelberger, DÖV 2012, S. 613, 616.

2 Windoffer/Groß, VerwArch 2012, 491, 491 f.

3 BT-Drs. 18/5948, S. 97.

4 Art. 29-Datenschutzgruppe, Stellungnahme 4/2013, WP205, S. 5.

5 Die Befragung wurde im Oktober 2015 im Auftrag des Verbraucherzentrale Bundesverbands (vzbv) durch TNS Emnid durchgeführt. Die Ergebnisse können online abgerufen werden unter: <http://www.vzbv.de/pressemitteilung/smart-meter-verbraucher-lehnen-zwangsdigitalisierung-ab>.

6 Raabe/Lorenz/Pallas/Weis, in: Raabe/Pallas/Weis/Lorenz/Boesche (Hrsg.), Datenschutz in Smart Grids, 2011, S. 53; Raabe, DuD 2010, 379, 385.

7 So übereinstimmend BMWi, Strategie Intelligente Vernetzung, S. 24; Raabe, DuD 2010, 379, 379; Windoffer/Groß, VerwArch 2011, 491, 512.

8 Richtlinie 2009/72/EG des europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG (Elektrizitätsbinnenmarktrichtlinie).

9 Gesetz zur Neuregelung energiewirtschaftlicher Vorschriften, BGBl. I 2011, 1554.

vellierung des Energiewirtschaftsgesetzes<sup>10</sup> wurden neue Bestimmungen über den Messstellenbetrieb mitsamt einigen Bestimmungen zum Umgang mit personenbezogenen Daten eingefügt (§§ 21b-i EnWG). Der gesetzgeberische Ansatz sah sich von Anfang an der Kritik ausgesetzt, dass wesentliche Aspekte des Datenschutzes und der Datensicherheit nicht im EnWG selbst geregelt wurden.<sup>11</sup> Detaillierte Vorgaben waren einem Verordnungspaket vorbehalten.<sup>12</sup> Angesichts der geringen Regelungstiefe der EnWG-Normen stellte sich die Frage, ob sie hinreichend bestimmt und normenklar sind, um den verfassungsrechtlichen Anforderungen zu genügen. Da dem Recht auf informationelle Selbstbestimmung Grundrechtsstatus zukommt, vermag nur der Gesetzgeber, nicht der Ordnungsgeber, die Bedingungen einer möglichen Einschränkung festzulegen. Mit der Vorlage des Messstellenbetriebsgesetzes hat der Gesetzgeber auf die Kritik reagiert. Der bisherige Regelungsansatz über das EnWG in Verbindung mit einem Verordnungspaket wurde aufgegeben. Das federführende Ministerium für Wirtschaft und Energie hat sich im Hinblick auf die Grundrechtsrelevanz und zur Vermeidung einer weiteren Zersplitterung des Energierechts nunmehr dazu entschieden, die Regelungsmaterie in einem neuen Stammgesetz umfassend niederzulegen. Dies ist unter dem Gesichtspunkt der Rechtssicherheit uneingeschränkt zu begrüßen.

Der erste Entwurf für ein „Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG)“ wurde vom BMWi am 21. September 2015 vorgelegt.<sup>13</sup> Das Bundeskabinett nahm diesen im Anschluss an die öffentliche Anhörung mit geringfügigen Änderungen am 4. November 2015 an und leitete ihn dem Bundesrat zur Stellungnahme zu. Nachdem der Bundesrat am 18. Dezember 2015 umfangreich Stellung genommen hat,<sup>14</sup> liegt der Entwurf inzwischen in der Fassung vom 17. Februar 2016 vor, die nunmehr auch die Gegenäußerung der Bundesregierung enthält.<sup>15</sup> Nach derzeitigem Stand soll das Gesetzgebungsverfahren noch im Sommer 2016 abgeschlossen werden.

### III. Begriff und Funktionsweise intelligenter Messsysteme

Ein intelligentes Messsystem besteht nach § 2 Nr. 7 MsbG-E aus einer modernen Messeinrichtung zur Erfassung des tatsächlichen Energieverbrauchs und der Nutzungszeit sowie einer Kommunikationseinheit (Smart-Meter-Gateway) zur sicheren Einbindung der Messeinrichtung in ein Kommunikationsnetz.<sup>16</sup> Ein verpflichtender Einbau intelligenter Messsysteme ist im MsbG-E lediglich für größere Letztverbraucher und Anlagenbetreiber vorgesehen.<sup>17</sup> So statuiert § 29 Abs. 1 MsbG-E eine Einbaupflicht bei Letztverbrauchern mit einem Jahresstromverbrauch<sup>18</sup> über 6.000 kWh und Anlagenbetreibern mit einer installierten Leistung über 7 kW. Diese Verpflichtung besteht allerdings nur unter der Voraussetzung technischer Möglichkeit<sup>19</sup> und wirtschaftlicher Vertretbarkeit. Wann ein Einbau wirtschaftlich vertretbar ist,

wird in der zentralen Vorschrift des § 31 MsbG-E ausführlich für verschiedene Letztverbraucher- und Anlagenbetreibergruppen anhand von Preisobergrenzen festgelegt. Die Preisobergrenzen orientieren sich dabei an den Erkenntnissen und Annahmen einer Kosten-Nutzen-Analyse<sup>20</sup>. Können die Preisobergrenzen in der Praxis nicht eingehalten werden, besteht auch keine Einbaupflicht. Mit diesem Ansatz möchte der Gesetzgeber erreichen, dass nur diejenigen Letztverbraucher zum Einbau verpflichtet werden, die tatsächlich auch davon profitieren können.<sup>21</sup>

Für kleinere Letztverbraucher mit einem Jahresstromverbrauch bis einschließlich 6.000 kWh sieht § 29 Abs. 2 MsbG-E eine optionale Ausstattung vor. Die Optionalität bezieht sich hierbei aber nicht auf die freiwillige Entscheidung des Letztverbrauchers. Insofern ist der Gesetzeswortlaut hier missverständlich. Vielmehr obliegt es allein dem grundzuständigen Messstellenbetreiber, die Entscheidung über den Einbau zu treffen. Allerdings muss auch hier zunächst die wirtschaftliche Vertretbarkeit nach § 31 Abs. 3 MsbG-E gegeben sein. All diejenigen Letztverbraucher und Anlagenbetreiber, für die nach diesen Grundsätzen keine Pflicht zum Einbau eines intelligenten Messsystems besteht, sollen bis zum Jahr 2032 unter dem Stichwort der „nachhaltigen Komplettmodernisierung“<sup>22</sup> zumindest mit den nicht kommunikationsfähigen modernen Messeinrichtungen ausgestattet werden. Die wirtschaftliche Vertretbarkeit richtet sich hier nach § 32 MsbG-E und ist gegeben,

10 Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG) vom 7. Juli 2005 (BGBl. I S. 1970, 3621).

11 Dazu näher Karg, DuD 2010, 365, 368; Wiesemann, MMR 2011, 355, 357.

12 Vgl. BMWi, Baustein für die Energiewende: 7 Eckpunkte für das „Verordnungspaket Intelligente Netze“; abrufbar unter: <http://www.bmw.de/BMWi/Redaktion/PDF/E/eckpunkte-fuer-das-verordnungspaket-intelligente-netze,property=pdf,bereich=bmw2012,sprache=de,wb=true.pdf>.

13 Als Art. 4 bildet es den Kern des Gesetzes zur Digitalisierung der Energiewende, BMWi, Entwurf eines Gesetzes zur Digitalisierung der Energiewende, Referentenentwurf vom 21.09.2015, Art. 4.

14 BR-Drs. 543/15.

15 BT-Drs. 18/7555.

16 Definitionen zum Smart-Meter-Gateway und zur modernen Messeinrichtung finden sich in § 2 Nr. 19 MsbG-E und in § 2 Nr. 15 MsbG-E.

17 Insofern folgt der Gesetzentwurf den Empfehlungen der Kosten-Nutzen-Analyse und dem Grundsatz, dass es keinen Rollout „um jeden Preis“ geben sollte, vgl. BT-Drs. 18/7555, S. 2, 63 und 91.

18 Für die Berechnung des Jahresstromverbrauchs ist gem. § 31 Abs. 4 MsbG-E der Durchschnittswert der letzten drei Jahre maßgeblich.

19 Technisch möglich ist die Ausstattung einer Messstelle nach § 30 MsbG-E, wenn mindestens drei voneinander unabhängige Unternehmen intelligente Messsysteme, die die Voraussetzungen des MsbG erfüllen, anbieten.

20 Die Elektrizitätsbinnenmarkttrichtlinie eröffnet den Mitgliedstaaten die Möglichkeit, die Einführung von einer positiven gesamtwirtschaftlichen Bewertung abhängig zu machen. Das BMWi hat vor diesem Hintergrund eine Kosten-Nutzen-Analyse zur flächendeckenden Einführung intelligenter Messsysteme und Zähler in Deutschland in Auftrag gegeben. Der Endbericht wurde Ende Juli 2013 veröffentlicht, abrufbar unter: <http://www.bmw.de/DE/Mediathek/publikationen,did=586064.html>. Die von der EU angestrebte Rolloutquote i.H.v. 80% bis zum Jahr 2020 wurde darin für einen Großteil der Kunden unter den derzeit geltenden Rahmenbedingungen als wirtschaftlich nicht zumutbar bewertet.

21 BT-Drs. 18/7555, S. 91 ff.

22 BT-Drs. 18/7555, S. 90.

wenn die jährlichen Kosten für den Messstellenbetrieb 20 Euro brutto nicht übersteigen.<sup>23</sup> Auch hier besteht für Letztverbraucher keine Möglichkeit, sich einem Einbau zu entziehen.

Verantwortlich für den Einbau und den Betrieb der neuen Messinfrastruktur sind als grundzuständige Messstellenbetreiber die örtlichen Verteilnetzbetreiber, die bereits heute den Messstellenbetrieb verantworten, sofern der Anschlussnutzer keinen Dritten damit beauftragt hat. Das Recht des Anschlussnutzers, einen anderen Betreiber zu wählen, ist auch künftig gegeben. Neu ist allerdings, dass auch der Anschlussnehmer ein Wahlrecht erhalten soll.<sup>24</sup> Dem Messstellenbetreiber wird durch § 3 Abs. 1 S. 2 MsbG-E auch die Funktion des sog. Smart-Meter-Gateway-Administrators übertragen.<sup>25</sup> Diese Rolle ist neu und wurde eigens dafür geschaffen, die Verantwortlichkeit für den technischen Betrieb, auch im Hinblick auf die Einhaltung der Vorgaben zur Datensicherheit, klarzustellen. Als „vertrauenswürdige Instanz“<sup>26</sup> kann nur der Gateway Administrator einen direkten Zugriff auf die Daten ermöglichen.<sup>27</sup> Der grundzuständige Messstellenbetreiber hat nach § 41 MsbG-E die Möglichkeit, die Grundzuständigkeit auf ein anderes Unternehmen zu übertragen.<sup>28</sup> Dies gilt allerdings nur für den Messstellenbetrieb von modernen Messeinrichtungen und intelligenten Messsystemen. Für alle weiteren Messstellen verbleibt die Zuständigkeit bei ihm.<sup>29</sup>

Beim Messstellenbetrieb fallen grundsätzlich drei wesentliche Arten von Daten an: Messwerte, Netzzustandsdaten und Stammdaten. Messwerte sind Angaben über entnommene, erzeugte oder eingespeiste Energiemengen.<sup>30</sup> Stammdaten umfassen Informationen über Art, technische Ausstattung, Ort, Spannungsebene und kommunikative Anbindung von etwaigen Erzeugungsanlagen oder steuerbaren Verbrauchseinrichtungen, die an das Smart-Meter-Gateway angeschlossen sind.<sup>31</sup> Netzzustandsdaten betreffen vor allem Spannungs- und Stromwerte, die zur Ermittlung des Netzzustands verwendet werden.<sup>32</sup> Die Übermittlung der Daten soll zukünftig sternförmig erfolgen.<sup>33</sup> Hierbei werden die Daten nach Erhebung und Aufbereitung direkt an die zum Datenempfang berechtigten Stellen übermittelt. Die Daten laufen somit nicht mehr über mehrere Stationen zum Empfänger.<sup>34</sup>

Die Kommunikationseinheit ist bidirektional ausgelegt, d.h. Daten können sowohl übermittelt als auch empfangen werden.<sup>35</sup> Bei den zu empfangenden Informationen handelt es sich in erster Linie um Tarifinformationen. In Verbindung mit der sog. Zählerstandsgangmessung<sup>36</sup> ermöglicht dies dynamische variable Tarife. Der Anschlussnutzer wird hierdurch in die Lage versetzt, seinen Strombezug an Preissignale zu knüpfen. Er kann mehr beziehen, wenn der Preis niedrig ist und den Bezug verringern, wenn der Preis hoch ist. Dieser richtet sich vor allem nach dem Angebot elektrischer Energie. Auch entsprechende Steuerungssignale für Verbrauchsgeräte und Erzeugungsanlagen sind auf diesem Wege möglich.<sup>37</sup>

## IV. Herausforderungen für den Datenschutz

### 1. Personenbezug

Die datenschutzrechtliche Relevanz der intelligenten Messsysteme ergibt sich daraus, dass es sich bei den erhobenen Daten um personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG handelt.<sup>38</sup> Für Messwerte liegt dies auf der Hand. Bei den Verbrauchs-, Erzeugungs- und Einspeisungsdaten handelt es sich um Daten aus dem häuslichen Bereich. Diese können in vielfältige tatsächliche Zusammenhänge zum Anschlussnutzer und den weiteren Bewohnern gesetzt werden. Sie geben Aufschluss über Umfang, Art und Zeitraum des Energieverbrauchs der im Haushalt lebenden Personen. Personenbezug weisen aber auch die beim Smart Meter anfallenden Stamm- und Netzzustandsdaten auf.<sup>39</sup> Hierbei handelt es sich zwar überwiegend um technische Daten. Der Begriff der personenbezogenen Daten ist im Bereich des Messwesens allerdings weit auszulegen.<sup>40</sup> Auch technische Daten, die in Bezug zu einer natürlichen Person gesetzt werden können, sind hiervon erfasst.

23 § 32 MsbG-E.

24 Vgl. für das Wahlrecht des Anschlussnutzers § 5 sowie für das Wahlrecht des Anschlussnehmers und dessen Folgen für das Recht des Nutzers § 6 MsbG-E.

25 § 3 Abs. 1 S. 2 MsbG-E.

26 BT-Drs. 18/7555, S. 73.

27 BT-Drs. 18/7555, S. 84; Zur Verteilung der Daten sieht der Gesetzentwurf insofern noch zwei optionale Modelle vor: Der Gateway Administrator kann hierbei entweder als automatisierte „Datendrehscheibe“ dienen, oder es erfolgt eine direkte Verteilung durch das intelligente Messsystem. In beiden Fällen hat der Administrator selbst keinen Zugriff auf die unverschlüsselten Daten. Er kann den Zugriff lediglich ermöglichen, vgl. BT-Drs. 18/7555, S. 108.

28 Die Zuständigkeit für die Gateway Administration kann ebenfalls übertragen werden, § 2 Nr. 20 MsbG-E. Hierbei muss aber die Zertifizierung berücksichtigt werden.

29 § 43 Abs. 1 S. 2 MsbG-E.

30 Vgl. § 2 Nr. 14 MsbG-E.

31 Vgl. § 2 Nr. 22 MsbG-E sowie zum Anlagenbegriff BT-Drs. 18/7555, S. 75.

32 § 2 Nr. 16 MsbG-E.

33 Vgl. § 60 MsbG-E.

34 Besonders umstritten ist in diesem Zusammenhang die zukünftige Rolle der Verteilnetzbetreiber in diesem System. Einige Stimmen (so auch der Bundesrat, vgl. BT-Drs. 18/7555, S. 131 ff.) fordern, dass sie – abweichend vom Modell der sternförmigen Kommunikation – auch zukünftig als „Datendrehscheibe“ fungieren sollen.

35 Karsten/Leonhardt, RDV 2016, 22, 23.

36 Die Zählerstandsgangmessung beinhaltet nach § 2 Nr. 27 MsbG-E die Messung einer Reihe viertelstündig ermittelter Zählerstände. Im Gegensatz zur jährlichen Ablesung des Zählerstandes bei der Abrechnung von Standardlastprofilkunden kann so eine zeitlich differenzierte Abrechnung erfolgen.

37 Dinter, ER 2015, 229, 229 f.

38 Wann personenbezogene Daten vorliegen, richtet sich auch im MsbG-E nach § 3 Abs. 1 BDSG, vgl. §§ 59 Nr. 1, 65 Nr. 2, 70 Nr. 2 MsbG-E sowie die Begründung zu § 49 MsbG-E, BT-Drs. 18/7555, S. 105.

39 Für Stammdaten vgl. auch Schmelzer (o. Fn. 7), S. 119 f.

40 Konferenz der Datenschutzbeauftragten des Bundes und der Länder und Düsseldorf Kreis, Orientierungshilfe datenschutzgerechtes Smart Metering, Juni 2012, abrufbar unter: [http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschiessungssammlung/DS-BundLaender/Orientierungshilfe\\_SmartMeter.pdf?\\_\\_blob=publicationFile&v=1](http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschiessungssammlung/DS-BundLaender/Orientierungshilfe_SmartMeter.pdf?__blob=publicationFile&v=1), S. 8, 9 sowie 18. Für eine weite Auslegung des Begriffs ebenso Eßer, in: Auernhammer, BDSG, 4. Aufl. 2014, § 3 Rdnr. 8; Schild, in: Wolff/Brink, BDSG, 2013, § 3 Rdnr. 1; kritisch dagegen Wiesemann, ZD 2012, 447, 448.

Die unterschiedliche Sensitivität von Messdaten kann sich nicht in der Qualifizierung als personenbezogenes Datum niederschlagen, sondern allenfalls in der Beurteilung des Datenschutzbedarfs.<sup>41</sup> Für die Beurteilung des Personenbezugs kommt es auch nicht darauf an, ob tatsächlich eine Verknüpfung mit einer natürlichen Person erfolgt. Ausreichend ist vielmehr die Bestimmbarkeit der Identität einer Person auf Basis der Daten.<sup>42</sup> Die Personenbeziehbarkeit ergibt sich daraus, dass es objektiv für andere möglich ist, direkt oder indirekt einen Personenbezug herzustellen.<sup>43</sup> Das Datenschutzrecht stellt dabei auf den Zeitpunkt der Erhebung ab.<sup>44</sup> Besteht zu diesem Zeitpunkt objektiv die Gefahr eines Personenbezugs, ist das jeweilige Datum als personenbezogen zu qualifizieren, auch wenn sich die Gefahr später nicht realisiert. Andernfalls käme es zu Schutzlücken.<sup>45</sup> Mit entsprechendem Zusatzwissen lassen sich die Daten ebenso in Mehrpersonenhaushalten konkreten Bewohnern zuweisen.<sup>46</sup> Ein Personenbezug scheidet schließlich auch nicht daran, dass sich eine Zuordnung als schwierig oder unmöglich erweist. Für die Qualifizierung als personenbezogenes Datum reicht es aus, wenn überhaupt die Zuordnung zu einer natürlichen Person erfolgt, selbst wenn die Zuordnung im Ergebnis unzutreffend ist.<sup>47</sup>

## 2. Gefahr detaillierter Personen- und Verhaltensprofile

Die anfallenden personenbezogenen Daten sind kritisch, weil sie detaillierte Rückschlüsse auf die Lebensgewohnheiten und persönlichen Verhältnisse der Stromverbraucher ermöglichen. Ein Großteil der Alltagshandlungen ist mit Energieverbrauch verbunden.<sup>48</sup> Auf Grundlage des Energieverbrauchs lässt sich etwa feststellen, wann der Nutzer aufsteht oder zu Bett geht, zu welchen Zeiten er duscht oder badet, ob er zur Zubereitung der Mahlzeiten die Mikrowelle, den Herd oder den Backofen einsetzt und wie häufig die Waschmaschine oder sonstige Elektrogeräte laufen.<sup>49</sup> Studien zufolge ist es sogar möglich, anhand des Lastprofils zu ermitteln, welches Fernsehprogramm der Energienutzer wählt.<sup>50</sup> Tiefe und Aussagekraft der möglichen Profile sind zudem aufgrund der Datendichte, Datenqualität und Erhebungsdauer sehr hoch. Bei einer viertelstündlichen Auslesung liefert ein Smart Meter rund 35.000 Datensätze pro Jahr. Bei der technisch möglichen, wenn auch im MsBG-E derzeit nicht vorgesehenen sekundengenauen Auslesung steigt das Datenvolumen auf 31,5 Millionen Datensätze pro Smart Meter.<sup>51</sup> Die Daten werden zudem über einen langen Zeitraum erfasst. Zufällige Schwankungen werden über die Zeitleiste ausgeglichen. Der stete Datenstrom erlaubt mithin hochdetaillierte Einblicke in das Verhalten, die Vorlieben und die Persönlichkeitsstruktur der Stromverbraucher. Noch detailliertere Nutzerprofile ergeben sich, wenn die Messsysteme zur verbesserten Steuerung und Lastverschiebung den Verbrauch einzelner Hausgeräte mit einbeziehen.<sup>52</sup> Das Risiko der Profilbildung und der Aussagegehalt erhöhen sich weiter, wenn die Messdaten mit Daten aus anderen Quellen verknüpft werden.<sup>53</sup> Mit der Möglichkeit ein-

zelne Daten konkreten Personen zuzuordnen, lassen sich auch die Profile sehr genau individualisieren.

## 3. Unmerkliche Datenerhebung

Die datenschutzrechtliche Situation wird zudem dadurch verschärft, dass die Datenerhebung weitgehend unbemerkt vom Anschlussnutzer erfolgt. Intelligente Messsysteme erheben die Daten lautlos, unsichtbar und automatisch, das heißt, ohne aktive Beteiligung des Nutzers. Sie befinden sich außerhalb des Sichtbereichs des Nutzers, meist im Keller bzw. in einem Schaltschrank. Das Bewusstsein über die kontinuierliche Datenerhebung ist daher eher gering. Hinzu kommt, dass die Daten an Dritte übermittelt, dort weiter verarbeitet und genutzt werden, möglicherweise sogar zusätzlich durch zwischengeschaltete Dienstleister. Sie gelangen zudem in den Machtbereich verschiedener Empfänger. Der Weg der Daten ist intransparent.<sup>54</sup> Der Anschlussnutzer hat im Bereich der gesetzlich erlaubten Datenverwendungen praktisch keine Kenntnis darüber, wer wann welche Daten erhält und wofür diese Daten genau verwendet werden.<sup>55</sup>

## 4. Gefahr der Zweckentfremdung

Derart große Datenmengen unterliegen stets der Gefahr einer missbräuchlichen Verwendung. Wenn die Daten aus ihrem ursprünglichen Erhebungskontext herausgelöst werden, wird ein weiteres datenschutzrechtliches Prinzip verletzt: der Zweckbindungsgrundsatz. Personenbezogene Daten dürfen nur zu den Zwecken verwendet werden, zu denen sie erhoben worden sind.<sup>56</sup> Dieser Grundsatz ist mit den Möglichkeiten der Datenverwendung in und um intelligente Netze kaum in Einklang zu bringen. Durch technische Entwicklungen sowie die Kombination von Informationen im Sinne von „Big Data“ werden künftig vielfältige, derzeit

41 Orientierungshilfe (o. Fn. 42), S. 9, 18.

42 Schild, in: Wolff/Brink (o. Fn. 42), § 3 Rdnr. 17 ff.

43 Kremer, RDV 2014, 240, 244; Pohle/Zoch, CR 2014, 409, 410.

44 Zur Problematik des Erhebungszeitpunktes bei Messeinrichtungen Lüdemann/Sengstacken/Vogelpohl, ZD 2015, 55, 59.

45 Vgl. Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, ZD-Aktuell, 04363.

46 Hornung/Fuchs, DUD 2012, 20, 22 unter Verweis auf Raabe, DuD 2010, 379, 381.

47 Taeger, in: Taeger/Gabel, BDSG, 2. Aufl. 2013, § 3 Rdnr. 5.

48 Güneysu/Vetter/Wieser, DVBl 2011, 870, 872.

49 Hornung/Fuchs, DuD 2012, 20, 22; Müller, DuD 2012, 359, 360 f.

50 Greveler/Justus/Löhr, Hintergrund und experimentelle Ergebnisse zum Thema „Smart Meter und Datenschutz“, abrufbar unter: [http://1lab.de/pub/smartmeter\\_sep11\\_v06.pdf](http://1lab.de/pub/smartmeter_sep11_v06.pdf), S. 3.

51 Roßnagel/Jandt, Datenschutzfragen eines Energieinformationsnetzes, Alcatel-Lucent Stiftung für Kommunikationsforschung, SR 88, 2010, S. 8.

52 Wiesemann, ZD 2012, 447, 447.

53 BT-Drs. 18/5948, S. 94; Lüdemann, ZD 2015, 247, 250; Wiesemann, ZD 2012, 447, 447.

54 Hier entsteht ein Widerspruch zum Transparenzprinzip, vgl. Bizer, DuD 2007, 350, 353 f.

55 Karg, (o. Fn. 41), S. 4; Lüdemann/Jürgens/Sengstacken, ZNER 2013, 592, 593.

56 Zum Zweckbindungsgrundsatz: Bizer, DuD 2007, 350, 352.

nicht absehbare Verwendungszwecke möglich. Diese lassen sich im Vorhinein kaum mit der erforderlichen Genauigkeit eingrenzen.<sup>57</sup> Auf nationaler Ebene ist bereits geplant, die Smart-Meter-Daten mit Daten aus anderen Sparten, wie der Gas-, Wärme- und Wasserversorgung zu verknüpfen.<sup>58</sup> Auf europäischer Ebene gibt es Überlegungen, die Daten auch mit den Sektoren Verkehr und Telekommunikation zu verbinden.<sup>59</sup> Das Gefahrenpotenzial steigt zudem mit dem wirtschaftlichen Wert des häuslichen Datensatzes. Das Interesse hieran ist groß. Dies belegen nicht zuletzt Investitionen und Firmenübernahmen im Smart-Home-Bereich durch Konzerne mit originär datenbasierten Geschäftsmodellen, wie etwa Alphabet.<sup>60</sup> Die Einhaltung des Zweckbindungsgrundsatzes ist aber nicht nur durch die dynamische technische Entwicklung gefährdet. Verstöße gegen den Zweckbindungsgrundsatz drohen auch durch staatlichen Eingriff. Absehbar ist, dass Smart-Meter-Daten auch für Strafverfolgungs-<sup>61</sup> oder Finanzbehörden<sup>62</sup> interessant sind.

## 5. Datensicherheit

Die Einführung intelligenter Messsysteme stellt schließlich auch die Gewährleistung der Datensicherheit vor gewaltige Herausforderungen. Mit der umfassenden Vernetzung steigt die Vulnerabilität sowie die Gefahr, dass auch Kriminelle den Zugang suchen.<sup>63</sup> Die geplante Standardisierung der intelligenten Messsysteme erhöht die Verletzlichkeit zusätzlich.<sup>64</sup> Die Möglichkeit eines Stromdiebstahls, die Verfälschung von Daten oder die Infizierung von Messsystemen mit Schadsoftware wurden bereits nachgewiesen.<sup>65</sup> Bei manipulierten Verbrauchsdaten drohen dem Anschlussnutzer finanzielle Verluste.<sup>66</sup> Eine mutwillige Unterbrechung der Stromversorgung kann zum Ausfall lebenswichtiger Geräte führen.<sup>67</sup> Das Einbruch- und Diebstahlrisiko wird erhöht, wenn unberechtigte Dritte die Abwesenheit der Bewohner aus der Ferne feststellen können.<sup>68</sup> Der aktuelle Fall der Schadsoftware Locky zeigt mit dem Erpressungspotential weitere Risiken.<sup>69</sup>

## V. Datenschutzkonzept des MsbG

### 1. Bereichsspezifische Vorrangregelung

Mit Inkrafttreten des Messstellenbetriebsgesetzes werden die bisherigen datenschutzrechtlichen Regelungen über intelligente Messsysteme im EnWG abgelöst.<sup>70</sup> An deren Stelle treten die Bestimmungen des Messstellenbetriebsgesetzes zur Datenkommunikation in intelligenten Energienetzen. Diese sind in Teil 3 des Gesetzes enthalten (§§ 49–75 MsbG-E). Als bereichsspezifische Sonderregelungen gehen diese Vorschriften den allgemeinen Bestimmungen des BDSG vor.<sup>71</sup> Der Anwendungsvorrang ist im Gesetz ausdrücklich niedergelegt. Nach § 49 Abs. 1 S. 2 MsbG-E ist die „Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften unzulässig“. Der Gesetzgeber hat damit das lange geforderte<sup>72</sup> spezifische Datenschutzrecht für die Digitalisierung im Energiebereich geschaffen. Zu Recht. Mit der verpflichtenden Einführung von intelli-

genten Messsystemen werden die Letztverbraucher den mit dieser Technologie verbundenen Gefahren zwingend ausgesetzt. Es ist daher konsequent, dem damit staatlich gesetzten Risiko einen korrespondierenden Sicherungsauftrag für die informationelle Selbstbestimmung zur Seite zu stellen.<sup>73</sup> Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten in Zusammenhang mit dem Messstellenbetrieb ist daher künftig nur noch zulässig, soweit dies im Messstellenbetriebsgesetz ausdrücklich vorgesehen ist oder der Anschlussnutzer eingewilligt hat (§ 50 Abs. 1 MsbG-E).

## 2. Berechtigte und Zweckbindung

Da das Gesetz umfassende Einbaupflichten vorsieht, widmet sich der Großteil der Regelungen dem zulässigen Umgang mit den an der Messstelle erhobenen Daten. Hier setzt folgerichtig auch das gesetzliche Datenschutzkonzept an. Einen wesentlichen Baustein dieses Konzeptes bildet zunächst die abschließende Aufzählung der Stellen, die von Gesetzes wegen zum Datenumgang berechtigt sein sollen: Messstellenbetreiber, Netzbetreiber, Bilanzkoordinatoren, Bilanzkreisverantwortliche, Direktvermarktungsunternehmer nach dem EEG und Energielieferanten (§ 49 Abs. 2 MsbG-E). Nur die hier genannten Stellen sind von den gesetzlichen Erlaubnistatbeständen erfasst. Alle anderen Datenempfänger bedürfen der vorherigen schriftlichen Einwilligung des

57 In diese Richtung auch Roßnagel, Datenschutz in einem informatisierten Alltag, 2007, S. 139 m.w.N.

58 BT-Drs. 18/7555, S. 76.

59 Vgl. nur Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Leitlinien für transeuropäische Telekommunikationsnetze und zur Aufhebung der Entscheidung Nr. 1336/97/EG, KOM(2011) 657 endg. vom 19.10.2011, Erwägung 5.

60 So hat im Jahr 2014 etwa Google (heute Alphabet) das Unternehmen Nest, einen Hersteller von Thermostaten und Rauchmeldern, für mehrere Milliarden US-Dollar übernommen, vgl. <http://www.spiegel.de/netzwelt/gadgets/nest-uebernahme-google-will-in-ihr-schlafzimmer-a-943406.html>.

61 Eine hohe gleichförmige Stromabnahme kann beispielsweise ein Indiz für die Existenz einer Beleuchtungsanlage zur Aufzucht von illegalen Hanfpflanzen darstellen, vgl. Raabe/Lorenz/Pallas/Weis (o. Fn. 7), S. 33.

62 Die Identifikation bestimmter strombetriebener Geräte oder Einrichtungen könnte auf den Betrieb eines nicht angemeldeten Gewerbes hinweisen.

63 BMWi, Strategie Intelligente Vernetzung, S. 24.

64 Lüdemann, ZD 2015, 247, 251.

65 BT-Drs. 18/5948, S. 94 m.w.N.

66 Art. 29-Datenschutzgruppe, Stellungnahme 4/2013, WP205, S. 8, 13.

67 Art. 29-Datenschutzgruppe, Stellungnahme 7/2013, WP209, S. 6.

68 Art. 29-Datenschutzgruppe, Stellungnahme 4/2013, WP205, S. 12; in diese Richtung ebenso Hornung/Fuchs, DuD 2012, 20, 21.

69 Vgl. <http://www.faz.net/aktuell/technik-motor/computer-internet/erpresser-virus-locky-verbreitet-sich-rasant-in-deutschland-14080201.html>.

70 Vgl. Art. 3 Gesetzesentwurfs zur Digitalisierung der Energiewende.

71 Karsten/Leonhardt, RDV 2016, 22, 23. Zu den Anforderungen an bereichsspezifische Sonderregelungen vgl. nur Schmidt, in: Taeger/Gabel (o. Fn. 49), § 1 Rn. 33; Dix, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, § 1 Rn. 158, 170.

72 Vgl. dazu Kap. II sowie Lüdemann/Jürgens/Sengstacken, ZNER 2013, 592, 597.

73 Raabe/Lorenz/Pallas/Weis (o. Fn. 7), S. 53, Raabe, DuD 2010, 379, 384 f.

Anschlussnutzers. Dies gilt insbesondere für die Anbieter der unter Datenschutzgesichtspunkten kritischen Mehrwertdienste.<sup>74</sup> Da Mehrwertdienste für die Erreichung der energiewirtschaftlichen Ziele nicht erforderlich sind, ist eine Privilegierung über die gesetzlichen Erlaubnistatbestände nicht angezeigt.<sup>75</sup> Der Kreis der gesetzlich Berechtigten ist gegenüber dem EnWG zwar erweitert.<sup>76</sup> Dies ist aber vor allem der neu eingeführten sternförmigen Kommunikation direkt an die beteiligten Akteure bzw. im Falle des Direktvermarktungsunternehmers der noch jungen Marktrolle geschuldet. Unbefriedigend ist allerdings, dass die Berechtigten ihre Pflichten weiterhin im Wege der Auftragsverarbeitung an externe Dienstleister auslagern können.<sup>77</sup> Der „*numerus clausus*“ der Berechtigten wird hiermit in gewisser Weise wieder ausgehöhlt.<sup>78</sup>

Die gesetzlichen Erlaubnistatbestände zur Datenerhebung, -verarbeitung und -nutzung bauen auf den Kreis der berechtigten Stellen auf. So werden in den §§ 55 ff. in hoher Detailtiefe diejenigen Sachverhalte festgelegt, zu denen eine Erhebung, Übermittlung und Nutzung der Daten zulässig ist. Als Kriterien zur Differenzierung der Zulässigkeit dienen die Datenart, die Art der berechtigten Stelle und der Verwendungszweck. Hiernach bestimmt sich, wann welche Daten in welcher Taktung bzw. in welchem Detaillierungsgrad erhalten und weiter verwenden darf. Die gesetzlichen Vorgaben orientieren sich dabei an den energiewirtschaftlichen Aufgaben der Akteure.<sup>79</sup> Das Gesetz soll damit der Gefahr der Zweckentfremdung vorbeugen.<sup>80</sup>

Dieser kleinteilige legislative Ansatz ist grundsätzlich geeignet, die von intelligenten Messsystemen ausgehenden Gefahren für den Datenschutz wirksam zu minimieren. Der Preis ist allerdings eine hohe Komplexität der Regelungen. Das Messstellenbetriebsgesetz steht insoweit in der Tradition moderner Spezialgesetzgebung.

### 3. Datensparsamkeit

Der zweite zentrale Ansatz des Gesetzgebers ist die Betonung und gesetzliche Ausformulierung der Datensparsamkeit. Im Kontext intelligenter Mess- und Energiesysteme ist eine vollständige Vermeidung personenbezogener Daten nicht möglich. Andernfalls könnte weder die Verbrauchsabrechnung noch eine verbrauchsbezogene Steuerung umgesetzt werden. Angesichts der Gefahren für die informationelle Selbstbestimmung ist es deshalb von entscheidender Bedeutung, die Prozesse so zu gestalten, dass möglichst wenig kritische Daten entstehen bzw. in Umlauf kommen.<sup>81</sup> Das Gesetz orientiert sich zu diesem Zweck an dem allgemeinen Gebot der Datenvermeidung und Datensparsamkeit aus § 3a BDSG. Dies zeigt sich vor allem durch die Verpflichtung zur Anonymisierung und Pseudonymisierung in § 52 Abs. 3 MsbG-E.

Die wichtigste diesbezügliche Vorgabe betrifft die Datenübermittlung bei Anschlussnutzern mit einem Jahresstromverbrauch bis einschließlich 10.000 kWh. Hier dürfen lediglich die Jahresarbeitswerte übertragen werden.<sup>82</sup> Bei einem Durchschnittsverbrauch von 3.500 kWh pro Jahr und Haushalt ist damit zunächst der Großteil der Privathaushalte von

vornherein von einer Datenübermittlung ausgenommen.<sup>83</sup> Etwas anders gilt nur, wenn der Verbraucher sich freiwillig für einen variablen Tarif entscheidet. In diesem Fall ist nach § 35 Abs. 1 Nr. 2 MsbG-E die tägliche Bereitstellung der Zählerstandgänge des Vortages auch bei einem Jahresstromverbrauch unter 10.000 kWh vorgesehen.<sup>84</sup> Auch für Anschlussnutzer mit einem Jahresverbrauch über 10.000 kWh enthält § 60 Abs. 3 MsbG-E den Datenumgang beschränkende Bestimmungen. Die Zählerstände dürfen nur viertelstündlich ausgelesen werden. Außerdem darf die Übermittlung erst am Folgetag erfolgen. Dies erschwert eine mögliche Profilbildung.

Im bisherigen Gesetzgebungsverfahren wurde teils gefordert, die gesetzlichen Regelungen noch weiter zu untersetzen und auszudifferenzieren.<sup>85</sup> Der Gesetzgeber hat gut daran getan, diesen Vorschlägen nicht zu folgen. Die Regelungen weisen aufgrund ihrer Verknüpfung mit den Datenarten und Nutzungszwecken bereits jetzt eine außergewöhnlich hohe Komplexität auf. Abstrakten Normen ist immanent, dass nicht jeder denkbare Einzelfall abgebildet werden kann. Dies ist auch nicht notwendig. Entscheidend ist, dass die zentralen Anwendungsfälle erfasst sind. Die Randbereiche lassen sich hinreichend scharf über die Anwendung der allgemeinen Grundsätze der Datenvermeidung und Datensparsamkeit regeln.

Eine andere Frage ist allerdings, ob es zur Erreichung der gesetzgeberischen Ziele überhaupt erforderlich ist, personenbezogene Verbrauchsdaten aus dem Haushalt im geplanten Umfang zu übermitteln. Smart Meter verfügen über die Möglichkeit, einen Großteil der Datenverarbeitung im System selbst vorzunehmen, ohne dass hierzu weitere Stellen einbezogen werden müssen.<sup>86</sup> Dies gilt insbesondere für die

74 Mehrwertdienste sind definiert als energieverorgungsfremde Dienstleistungen, die als Kommunikationsinfrastruktur das Smart-Meter-Gateway nutzen, § 2 Nr. 9 MsbG-E.

75 BT-Drs. 18/7555, S. 107.

76 Vgl. § 21g Abs. 2 S. 1 EnWG mit § 49 Abs. 2 MsbG-E, wonach nun auch Bilanzkoordinatoren, Bilanzkreisverantwortliche und EEG-Direktvermarktungsunternehmer zu den berechtigten Stellen zählen.

77 § 49 Abs. 3 MsbG-E.

78 Karsten/Leonhardt, RDV 2016, S. 22, 23.

79 Dinter, ER 2015, 229, 234.

80 So zuvor gefordert durch Europäischer Datenschutzbeauftragter, Stellungnahme zur Empfehlung der Kommission zu Vorbereitungen für die Einführung intelligenter Messsysteme, abrufbar unter: [https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-06-08\\_Smart\\_metering\\_DE.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_DE.pdf), Ziff. 43.

81 Vgl. § 3a S. 2 BDSG; Europäischer Datenschutzbeauftragter (o. Fn. 82), Ziff. 43.

82 § 60 Abs. 3 MsbG-E.

83 Etwas anderes würde nur gelten, wenn mit dem Netzbetreiber die Steuerung von unterbrechbaren Verbrauchseinrichtungen gem. § 14a EnWG vertraglich vereinbart worden ist; vgl. BT-Drs. 18/7555, S. 110.

84 Hier entsteht ein Widerspruch zur Regelung der abschließenden Standardkommunikation nach § 60 Abs. 3 MsbG-E, wonach lediglich eine jährliche Übermittlung zulässig ist. Bei der Wahl eines variablen Tarifes wäre für kleinteiligere Übermittlungen wohl eine Einwilligung gemäß § 65 Nr. 1 MsbG-E erforderlich.

85 Vgl. Stellungnahme des Bundesrates in: BT-Drs. 18/7555, S. 135.

86 Die Ermöglichung datensparsamer Tarife sowie eine Messwertverarbeitung im Smart-Meter-Gateway gehören zu den durch die Technischen Richtlinien verbindlich vorgegebenen Mindestanforderungen, vgl. Kapitel 4 der Technischen Richtlinie BSI TR-03109-1 (S. 79 ff.).

Realisierung und Abrechnung zeitvariabler Tarife und damit gerade in den Bereichen, denen der Gesetzgeber eine große Bedeutung für die Sicherstellung einer nachhaltigen Energieversorgung beimisst. Für die Umsetzung der variablen Tarife erscheint es nach heutigem Stand der Technik ausreichend, wenn die Tarifinformationen an das intelligente Messsystem gesendet werden. Das Gerät berechnet dann aus Tarif und Verbrauch die Abrechnungsbeträge und meldet diese aggregiert an den Lieferanten.<sup>87</sup> Es verbleibt eine einseitige Kommunikation in Richtung des Verbrauchers. Nur zum Zeitpunkt und zum Zweck der Abrechnung wird einmalig ein (einzelner) Wert zurückgeliefert. Auch für das Netzmanagement und die Bilanzierung sind nach heutigem Stand keine personenbezogenen Daten erforderlich. Aggregierte Daten reichen hierfür aus.<sup>88</sup> Der Gesetzgeber sollte vor diesem Hintergrund die zusätzliche Anordnung in den Entwurf aufnehmen, dass überall dort, wo nach technischem Stand kein Personenbezug erforderlich ist, die Daten zwingend aggregiert werden müssen.<sup>89</sup> Eine derartige Regelung wurde im Vorfeld auch durch das BMWi angekündigt.<sup>90</sup> In den Entwurf hat diese aber bisher keinen Eingang gefunden.<sup>91</sup> Der allgemeine Grundsatz der Anonymisierung und Pseudonymisierung in Art. 52 Abs. 3 MsbG vermag das Fehlen einer solchen Vorgabe angesichts der ausdrücklichen Zulässigkeit der nichtaggregierten Datenübermittlung in den gesetzlichen Erlaubnistatbeständen nicht zu kompensieren.

#### 4. Anforderungen an die Einwilligung

Die Nutzer sollten auf Basis von Aufklärung und Partizipation selbstbestimmte, informierte Entscheidungen treffen können, die den Prinzipien der Freiwilligkeit und Souveränität entsprechen.<sup>92</sup> Um dies sicherzustellen sowie zur Gewährleistung eines ausreichenden Datenschutzes, werden bei der möglichen Einwilligung die hohen Anforderungen des § 4a BDSG übernommen. Bereits die geforderte Freiwilligkeit könnte fraglich sein, wenn etwa eine Inanspruchnahme von Mehrwertdiensten durch die Anschlussnutzer an die Preisgabe von Daten geknüpft wird, die zu diesem Zweck nicht erforderlich sind.<sup>93</sup> Notwendig ist darüber hinaus eine informierte Einwilligung. Der Betroffene muss wissen, worin er einwilligt, um die Tragweite seiner Entscheidung abzusehen.<sup>94</sup> Der Gesetzgeber flankiert dazu zwar bereits vertragliche Regelungen zur Datenkommunikation beim Smart Metering mit hohen Transparenzvorgaben durch ein standardisiertes Formblatt.<sup>95</sup> Ein Ansatz, der anzuerkennen ist. Allerdings stehen sich kurze, einfache Formblätter und die umfassenden Transparenzpflichten bei datenschutzrechtlichen Einwilligungserklärungen oftmals diametral gegenüber. Vor dem Hintergrund der möglichen Vielzahl von beteiligten Akteuren sowie Übermittlungs- und Verarbeitungsvorgängen innerhalb intelligenter Energienetze werden die zur Einwilligung erforderlichen Informationen sehr umfangreich sein. Insofern ist unter dem Stichwort des „information overload“ Skepsis angezeigt. Es besteht die Gefahr, dass die Nutzer mit Informationen überfrachtet werden.<sup>96</sup> Wie dieses Spannungsfeld, welches für sämtliche modernen Technologiean-

wendungen typisch ist, im Rahmen der intelligenten Messsysteme aufgelöst werden soll, bleibt abzuwarten.

Schwer umsetzbar sind die Formerfordernisse an die datenschutzrechtliche Einwilligung im Sinne des BDSG. Die Einwilligung in den Datenumgang ist höchstpersönlicher Natur. Da sie einen Grundrechtseingriff rechtfertigt, kann nur der Grundrechtsinhaber selbst die Einwilligung erklären; die Abgabe durch einen Bevollmächtigten scheidet aus.<sup>97</sup> Nach dem Messstellenbetriebsgesetz soll die Einwilligung aber lediglich durch den Anschlussnutzer erfolgen. Dabei wird ausgeblendet, dass in Mehrpersonenhaushalten personenbezogene Daten von sämtlichen Bewohnern erfasst, zugeordnet und zu Profilen zusammengefasst werden können.<sup>98</sup> Folglich wären regelmäßig Erklärungen aller Bewohner einzuholen. Aufgrund dieses weiten Kreises an Betroffenen, lässt sich auch die Schriftform des § 4a Abs. 1 S. 3 BDSG in der Praxis kaum erfüllen. Die elektronische Form ist nur mittels qualifizierter elektronischer Signatur zulässig, welche allerdings eine zu geringe Verbreitung gefunden hat, um praktische Relevanz zu genießen.<sup>99</sup> Zudem ist eine Einwilligung für jede einzelne Datenverwendung geboten.<sup>100</sup> Dies scheint mit Blick auf die Schriftform sowie den Kreis der potenziell im Haushalt betroffenen Personen undurchführbar.

#### 5. Organisatorische und technische Datensicherheit

Den datensicherheitsrechtlichen Gefahren begegnet der Entwurf schließlich durch die Aufstellung organisatorischer und technischer Mindestanforderungen für intelligente

87 In diese Richtung ebenso Schäfer-Stradowsky/Boldt, EnWZ 2015, 349, 351.

88 Raabe/Lorenz/Pallas/Weis (o. Fn. 7), S. 38; Orientierungshilfe (o. Fn. 42), S. 28; vzbv, Smart Meter Einbau: Zwangsdigitalisierung durch die Kellertür. Stellungnahme des Verbraucherzentrale Bundesverbandes zum Entwurf eines Gesetzes zur Digitalisierung der Energiewende, abrufbar unter: <http://www.bmw.de/BMWi/Redaktion/PDF/Stellungnahmen/Stellungnahmen-Gesetzentwurf-Digitalisierung-Energiewende/verbraucherzentrale-bundesverband,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf>, S. 5.

89 Schäfer-Stradowsky/Boldt, EnWZ 2015, 349, 351; Roßnagel, ZD 2013, 562, 563.

90 BMWi/BSI, Smart Metering – Datenschutz und Datensicherheit auf höchstem Niveau, abrufbar unter: [www.bmw.de/BMWi/Redaktion/PDF/S-T/smart-metering,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf](http://www.bmw.de/BMWi/Redaktion/PDF/S-T/smart-metering,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf), S. 2.

91 Die einzige Ausnahme bildet § 67 II Nr. 1 und 2 MsbG, in denen die Übermittlung aggregierter Last- und Einspeisegänge vom Übertragungsnetzbetreiber an den Verteilernetzbetreiber und den Bilanzkreisverantwortlichen geregelt ist.

92 BMWi, Strategie Intelligente Vernetzung, S. 5, 24.

93 Dies gilt insbesondere dann, wenn dem Nutzer bei einer Ablehnung der Datenverwendung die Leistung verwehrt wird. Vgl. insoweit das Kopplungsverbot, Däubler/Klebe/Wedde/Weichert, BDSG, 5. Aufl. 2016, § 4a Rdnr. 24.

94 Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 4a Rdnr. 25.

95 Dort müssen Angaben zu Art, Umfang, Häufigkeit und Zweck von Datenübermittlungen übersichtlich und verständlich niedergelegt und dem Anschlussnutzer zur Verfügung gestellt werden, § 54 MsbG-E.

96 Buchner, DuD 2010, 39, 40; Katko/Babaei-Beigi, MMR 2014, 360, 362 f.

97 Simitis, in: Simitis (Hrsg.) (o. Fn. 73), § 4a Rdnr. 30 f. m.w.N.

98 Vgl. Kap. IV 1 und 2.

99 Kühling, in: Wolff/Brink (o. Fn. 42), § 4a Rdnr. 48.

100 Simitis, in: Simitis (Hrsg.) (o. Fn. 73), § 4a Rdnr. 33.

101 § 1 Nr. 4, §§ 19 ff. MsbG-E.

Messsysteme.<sup>101</sup> In organisatorischer Hinsicht betont der Entwurf die Rolle des Smart-Meter-Gateway-Administrators und weist ihm die zentrale Verantwortung für die Einhaltung der datensicherheitsrechtlichen Bestimmungen zu. Allein der Gateway Administrator kann den Zugriff auf die Daten aus dem intelligenten Messsystem ermöglichen.<sup>102</sup> Jegliche Kommunikation mit dem intelligenten Messsystem muss durch ihn autorisiert werden. Er wacht darüber, dass Dritte zum Datenempfang tatsächlich berechtigt sind und hat sich entsprechende Berechtigungsnachweise vorlegen zu lassen. Entsprechend dieser zentralen Stellung im Sicherheitskonzept, stellt der Entwurf hohe Anforderungen an die Integrität und Fachkunde des Gateway Administrators. Die Übernahme dieser Funktion ist erst nach einer entsprechenden Zertifizierung möglich.<sup>103</sup> Ebenso unterliegt auch das Smart-Meter-Gateway selbst einer Zertifizierungspflicht.<sup>104</sup>

Die Sicherstellung der technischen Datensicherheit überträgt der Entwurf weitestgehend dem Bundesamt für Sicherheit in der Informationstechnik (BSI), das über den Umweg der Vermutungsregelung des § 22 Abs. 2 MsbG-E im Rahmen von Schutzprofilen und Technischen Richtlinien faktisch alle technischen Vorgaben für den Einsatz der intelligenten Messsysteme macht. Daneben wird die Bundesnetzagentur ermächtigt, im Einvernehmen mit dem BSI die erforderlichen Festlegungen im Verordnungswege zu treffen.<sup>105</sup>

Insgesamt sind die Datensicherheitsvorgaben stimmig. Dies gilt auch für die im Entwurf gewählte Lösung, die Detaillierung der technischen Vorgaben auf das flexible Instrument der Ausgestaltung durch das BSI und die Bundesnetzagentur zu stützen. In einem sich rasch ändernden Umfeld sichert dies die notwendige Innovationsoffenheit und Flexibilität. Positiv hervorzuheben ist auch die klare Zuweisung der Verantwortung an eine Stelle, hier den Gateway Administrator. Dies erleichtert die Prüfung durch die Aufsichtsbehörden. Kritisch ist jedoch, dass die Datensicherheitsanforderungen nach dem Entwurf nur die Kommunikationswege vom Messsystem zu den berechtigten Stellen abdecken. Nicht erfasst sind nachgelagerte Datenverarbeitungen. Vor allem neue, unregulierte Dienstleistungsanbieter, die auf Grundlage einer Einwilligung des Anschlussnutzers tätig werden, können hier zur Sicherheitslücke werden.<sup>106</sup>

## VI. Fazit

*Die Zusammenführung der gesamten Regelungsmaterie zum Messstellenbetrieb in einem neuen Stammgesetz ist zu begrüßen. Auch die Vorgabe umfangreicher Mindeststandards in den Bereichen Datenschutz, Datensicherheit und Interoperabilität ist ein wichtiger Schritt. Das Datenschutzkonzept des MsbG-E stellt insgesamt eine deutliche Verbesserung gegenüber den bisher geltenden Regelungen dar. Der Entwurf vermag in seiner jetzigen Fassung dennoch nicht die Bedenken zu zerstreuen, dass die „Zwangsdigitalisierung durch die Kellertür“<sup>107</sup> erhebliche Risiken für das Recht auf informationelle Selbstbestimmung mit sich bringt. Kritisch sind vor allem drei Punkte:*

- *Der Entwurf ermöglicht die Übermittlung personenbezogener Daten in einem Umfang, der weder technisch noch energiewirtschaftlich erforderlich ist. In vielen Fällen könnte die Verarbeitung der kritischen personenbezogenen Daten im intelligenten Messsystem selbst stattfinden. Übermittelt würden dann vorwiegend aggregierte Daten. Der das Haus verlassende Fluss sensibler Daten könnte so erheblich begrenzt werden. Zur Erreichung der energiewirtschaftlichen Ziele gibt es mithin weniger eingriffsintensive Alternativen. Es wäre daher – auch im Hinblick auf die Akzeptanz – zu wünschen, dass die Frage der Messwertverarbeitung im Smart-Meter-Gateway und weitere datensparsamere Alternativen im Gesetzgebungsverfahren nochmals vertieft behandelt werden.*
- *Problematisch ist zudem, dass der Entwurf bei Datenübermittlungen außerhalb der gesetzlichen Erlaubnistatbestände allein auf die Einwilligung des Anschlussnutzers abstellt, auch wenn die Daten mehrerer Haushaltsangehöriger erfasst werden. Für diesen Umstand bietet der Entwurf derzeit keine Lösung. Hier bedarf es auch angesichts der absehbaren Regelungen in der Datenschutz-Grundverordnung einer Klärung, um der Energiewirtschaft rechtssichere Lösungen anbieten zu können. Möglicherweise bietet eine Regelung wie im Telekommunikationsrecht zur Bekanntgabe des Einzelverbindungs nachweises einen Ausweg.<sup>108</sup> Für das Erfordernis der Schriftform zeichnet sich im Entwurf zur europäischen Datenschutz-Grundverordnung mit Art. 4 Nr. 11 in Verbindung mit Erwägungsgrund Nr. 32 eine Lockerung ab.<sup>109</sup>*
- *Kritisch ist zudem die zwangsweise Einführung von Smart Metern. Die Digitalisierung der eigenen vier Wände beruht bisher auf der freien Entscheidung der Wohnungsinhaber. Aus gutem Grund. Schließlich erlauben intelligente Messsysteme die Erhebung von Verbrauchsdaten in einem Umfang, durch den der Alltag der Menschen in der eigenen Wohnung in hoher*

102 BT-Drs. 18/7555, S. 84.

103 § 25 Abs. 5 MsbG-E.

104 § 24 MsbG-E

105 § 75 Nr. 1 MsbG-E.

106 Raabe/Lorenz/Pallas/Weis (o. Fn. 7), S. 49.

107 vzbv (o. Fn. 90), S. 5

108 Vgl. dazu auch Karsten/Leonhardt, RDV 2016, 22, 23 f.

109 Künftig soll eine „unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung“ ausreichend sein. Vgl. Standpunkt des Rates in erster Lesung im Hinblick auf den Erlass der Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aushebung der Richtlinie 95/46/EG, 5419/16 vom 6. April 2016, abrufbar unter: [http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST\\_5419\\_2016\\_INIT&from=DE](http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=DE).

Detailtiefe für Dritte nachvollziehbar ist.<sup>110</sup> Dementsprechend hat der Bundesrat für eine Opt-Out-Option votiert.<sup>111</sup> Für eine solche Lösung spricht auch, dass der Nachbarstaat Österreich diesen Weg bereits gegangen ist.<sup>112</sup> Die Position der Bundesregierung, wonach über reine Marktmechanismen keine ausreichende Durchsetzung intelligenter Messsysteme erfolgen kann, vermag nur bedingt zu überzeugen. Dabei kann dahingestellt bleiben, ob die Energiewirtschaft eines weiteren Subventionstatbestandes bedarf, dessen Finanzierung auf die Verbraucher umgelegt wird. Die Grenzen der Marktbeeinflussung sind jedenfalls dort erreicht, wo diese erheblich zu Lasten grundrechtsrelevanter Positionen der Endverbraucher gehen.

Es bleibt daher zu hoffen, dass der Gesetzgeber in diesen Punkten vor Inkraftsetzen des Messstellenbetriebsgesetzes nachsteuert.

110 Art. 29-Datenschutzgruppe, Stellungnahme 4/2013, WP205, S. 5.

111 Diese sollten sowohl in Bezug auf Ausstattung mit als auch auf die Verwendung von Daten aus intelligenten Messsystemen gelten, vgl. BT-Drs. 18/7555, S. 124 ff.

112 Vgl. § 83 Abs. 1 S. 4 ELWOG für den Strom- sowie § 128 Abs. 1 S. 4 GWG für den Gassektor.



### Prof. Dr. Volker Lüdemann

ist Professor für Wirtschafts- und Wettbewerbsrecht an der Hochschule Osnabrück und wissenschaftlicher Leiter des Niedersächsischen Datenschutzzentrums (NDZ).



### Manuel Christian Ortmann LL.M.

ist Doktorand im vom Land Niedersachsen sowie der VW-Stiftung geförderten Projekt „EOS-Energiespeicherlösungen in der Region Osnabrück-Steinfurt“ und beschäftigt sich mit aktuellen Fragen des Energierechts.



### Patrick Pokrant LL.M.

ist wissenschaftlicher Mitarbeiter im EOS-Projekt und beschäftigt sich mit aktuellen Fragen des Datenschutzrechts.

## Kurzbeiträge

### Aus den aktuellen Berichten der Aufsichtsbehörden (25): Unerwünschte Kunden/Mitarbeiter

Ausgewählt und kommentiert von Prof. Peter Gola, Königswinter\*

Es gibt Personen mit denen möchte man nichts oder nichts mehr zu tun haben, weil man selbst oder andere schlechte Erfahrungen mit ihnen gemacht haben. Ggf. helfen dann interne oder externe Wardateien.

#### Unerwünschte Hotelgäste

In einem zu einer großen Hotelkette gehörenden Haus wurden potentielle Hotelgäste am Empfang abgewiesen, weil sie laut Empfangspersonal auf einer „Schwarzen Liste“ stän-

den. Die Nachforschungen der BlnBDI (Jahresbericht 2015, Ziff. 5.8.2) ergaben, dass in der Liste unerwünschte frühere Gäste mit dem Ablehnungsgrund „Raucher“ bzw. „Schwarzschläfer“ aufgeführt werden. Die BlnBDI hat gegen eine solche Liste keine grundsätzlichen Bedenken, sofern die datenschutzrechtlichen Belange der betroffenen Gäste gewahrt bleiben. Dazu verweist sie auf die dem Hotelier zustehende

\* Der Autor ist Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn.