

A. Einführung

Der stetig weiterwachsende wirtschaftliche und technische Fortschritt sowie die zunehmende Digitalisierung im Bereich der Energiewirtschaft als Voraussetzung für einen einheitlichen und funktionierenden Energiemarkt führen auch zukünftig zu einem deutlichen Anstieg der Verarbeitung personenbezogener Daten. Während in der Vergangenheit Informationen über Stromflüsse noch sehr limitiert waren, wird heute das dezentrale Stromversorgungssystem durch bidirektionale Informations- und Stromflüsse gekennzeichnet.¹ Durch diese wechselseitige Übermittlung von Markt- und Verbrauchsdaten können Angebot und Nachfrage von Elektrizität besser in Einklang gebracht werden,² wodurch zum einen ein energiesparendes Verhalten³ des Letztverbrauchers⁴ und zum anderen eine effektivere Umstellung von konventionellen Energieträgern auf erneuerbare Energien erreicht werden soll.

Diese kommunikativen Veränderungen erhöhen die Anforderungen an die einzusetzenden Mess- und Kommunikationstechnologien und Datenverarbeitungssysteme. Um diesen Anforderungen gerecht zu werden, hat die Europäische Kommission, im Anhang der dritten Binnenmarktrichtlinie Strom⁵ und Gas⁶, den Mitgliedstaaten auferlegt, dass Letztverbraucher mit sogenannten „Smart Metern“, also intelligenten Messsystemen (iMS) auszustatten sind („Rollout“). Auf nationaler Ebene hat der Gesetzgeber diese Verpflichtung gegenüber dem Messstellenbetreiber (MSB) in § 29 Abs. 1 Messstellenbetriebsgesetz⁷ (MsbG) normiert.

¹ Art. 29-DSG, WP 183, S. 4.

² *Ringel*, in: Herbes/Friege Marketing Erneuerbarer Energien, S. 309.

³ BR-Drs. 568/08, Verordnung zum Erlass von Regelungen über Messeinrichtungen im Strom- und Gasbereich vom 8. 8. 2008, S. 1.

⁴ Letztverbraucher i. S. d. § 2 S. 1 Nr. 8 MsbG sind natürliche oder juristische Personen, die Energie für den eigenen Verbrauch oder für den Betrieb von Ladepunkten zur Versorgung von Elektrofahrzeugnutzern beziehen.

⁵ Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates v. 13. 7. 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG, ABl. EU L 211/55 v. 14. 8. 2009.

⁶ Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates v. 13. 7. 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG, ABl. EU L 211/94 v. 14. 8. 2009.

⁷ Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz - MsbG) vom 29. 8. 2016 (BGBl. I S. 2034), das durch Art. 15 des Gesetzes v. 22. 12. 2016 (BGBl. I S. 3106) geändert worden ist.

Ein iMS kann, je nach Ausstattung, für Energieerzeuger, Netzbetreiber⁸ und Letztverbraucher die notwendigen Energieverbrauchsdaten jederzeit bereitstellen⁹ und zur Übermittlung von beispielsweise Netzzustandsdaten i. S. d. § 2 S. 1 Nr. 16 MsbG verwendet werden. Zudem können iMS auch sichere und zuverlässige Steuerungsmaßnahmen von Erneuerbaren-Energien-Anlagen (EE-Anlagen) oder Kraft-Wärme-Kopplungs-Anlagen (KWK-Anlagen) unterstützen sowie als eine Art Kommunikationsplattform im intelligenten Energienetz¹⁰ (sog. „Smart Grid“) dienen.¹¹ Ein weiterer Vorteil liegt darin, dass der Letztverbraucher jederzeit sekundengenaue¹² und präzise Informationen über sein Verbrauchsverhalten, also seinen Energieverbrauch, erhalten und infolgedessen eine Umsetzung variabler Strom- oder Gastarife ermöglicht werden kann. Insofern beginnt mit dem Einsatz von iMS das Zeitalter des digitalen Messstellenbetriebs.

Allerdings haben iMS nicht nur Vorteile. Gerade in Bezug auf den Datenschutz sind iMS sehr bedenklich. Eine Anbringung erfolgt häufig in räumlich besonders geschützten Bereichen, so dass die Erhebung der entsprechenden Daten Aufschlüsse über persönliche Lebensumstände geben können sowie Rückschlüsse insbesondere auf An- und Abwesenheitszeiten der betroffenen Person im Haushalt, auf deren Gewohnheiten oder Vermögensverhältnisse sowie die Anzahl im Haushalt lebender Personen gezogen werden können.¹³ Von der betroffenen Person wird also, auch wenn zum Teil ungewollt, durch die sekundengenaue Erfassung, Erhebung, Verarbeitung, Protokollierung und

⁸ Ein Netzbetreiber ist gemäß der Legaldefinition des § 3 Nr. 27 EnWG der Netzbetreiber oder Anlagenbetreiber i. S. d. § 3 Nr. 2 bis 7 und 10 EnWG.

⁹ Richtlinie 2006/32/EG des Europäischen Parlaments und des Rates vom 5. 4. 2006 über Endenergieeffizienz und Energiedienstleistungen und zur Aufhebung der Richtlinie 93/76/ EWG des Rates, Art. 13 Abs. 1, ABl. EU L 114/64 v. 27. 4. 2006.

¹⁰ Ein intelligentes Netz ist ein Energieversorgungsnetz, welches durch informations- und regeltechnische Funktionen erweitert wurde, so die BNetzA, „Smart-Grid“ und „Smart Market“, Eckpunktepapier der Bundesnetzagentur zu den Aspekten des sich verändernden Energieversorgungssystems, 2011, S. 11.

¹¹ *Bartsch*, in: Theobald/Kühling, Energierecht Kommentar, 230. Datenschutz in Energieversorgungsunternehmen, Rn. 111; *Jandt/Roßnagel/Volland*, in ZD 2011, 99 (99 f); *Schäfer-Stradowsky/Boldt*, in: EnWZ 2015, 349 (349).

¹² Art. 29-DSG WP 183, S. 4: „Die Daten können in Echtzeit [...]“.

¹³ Art. 29-DSG, WP 205, S. 5; *Mitto*, in: Energierecht, Rn. 207; *Lüdemann/Pokrant*, in: DuD 2019, 365 (365); *Riemann*, in: TechDispatch Nr. 2 vom 16. 10. 2019; *Kühling/Rosbach/Busch* in: Kühling/Rosbach/Busch, Energierecht, S. 244, Rn. 55; *Lüdemann/Ortmann/Pokrant*, in: RDV 2016, 125 (128).

Speicherung ihrer (Energie-)Daten ein Verhaltensprofil erstellt. Hinzu kommt, dass der Letztverbraucher bzw. der Anschlussnutzer i. S. v. § 2 S. 1 Nr. 3 MsbG¹⁴ bei Vorliegen der gesetzlich normierten Voraussetzungen des § 29 MsbG den Einbau bzw. die Umrüstung seines herkömmlichen Messgerätes zu einem iMS zu dulden hat und sich insofern der Erstellung eines solchen Verhaltensprofils nicht entziehen kann. Dies ist auf nationaler Ebene betrachtet nicht nur in Hinblick auf den persönlich-sachlichen Privatsphärenschutz¹⁵ i. S. d. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz¹⁶ (GG), sondern auch auf räumliche Aspekte, wie die Unverletzlichkeit der Wohnung i. S. d. Art. 13 GG¹⁷, welche nicht Teil dieser Arbeit ist, bedenklich.¹⁸ Ein solches visualisiertes Profil bzw. solche gewonnenen Informationen sind nicht nur für den berechtigten Verwender- bzw. Adressatenkreis von Bedeutung, sondern beispielsweise auch für öffentliche Stellen, z. B. Ämter wie das Finanzamt, oder im schlimmsten Fall auch für Kriminelle, denen beispielsweise ein Einbruch aufgrund der nun bekannten Abwesenheitszeiten des betroffenen Anschlussnutzers erleichtert wird.¹⁹ Aus diesem Grund ist es essentiell wichtig, dass bei der Durchführung des zukünftig digitalen Messstellenbetriebs und einer damit verbundenen Verarbeitung personenbezogener Daten alle betroffenen natürlichen Personen geschützt werden. Zudem stellt der Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten auf europäischer Ebene nach Art. 7 und Art. 8²⁰ Charta der Grundrechte der Europäischen

¹⁴ Anschlussnutzer: der zur Nutzung des Netzanschlusses berechnete Letztverbraucher oder Betreiber von Erzeugungsanlagen nach dem Erneuerbare-Energien-Gesetz oder dem Kraft-Wärme-Kopplungsgesetz.

¹⁵ Art. 29-DSG, WP 183, S. 14.

¹⁶ Grundgesetz für die Bundesrepublik Deutschland in der im BGBl. Teil 3, Gliederungsnummer 100 - 1, veröffentlichten bereinigten Fassung, das zuletzt durch Art. 1 des Gesetzes v. 15. 11. 2019 (BGBl. I S. 1546) geändert worden ist.

¹⁷ *Brink/Schwab*, in: Wedde Handbuch Datenschutz und Mitbestimmung, S. 56, Rn. 14 f.; vertiefend zur Einbau- und Erneuerungspflicht i. S. d. § 29 Abs. 1 MsbG siehe *Hömke*, in: Elert Innovativ. Integrativ. Intelligent, S. 283 ff.

¹⁸ Nach Ansicht des BVerfG (NJW 2008, 822 (826)) schützt Art. 13 Abs. 1 GG nicht gegen die durch die Infiltration des Systems ermöglichte Erhebung von Daten, die sich im Arbeitsspeicher oder auf den Speichermedien eines informationstechnischen Systems befinden, das in einer Wohnung steht.

¹⁹ *Riemann*, in: TechDispatch Nr. 2 vom 16. 10. 2019.

²⁰ Der Europäische Gerichtshof (EuGH) wendet in eigentlich allen das Datenschutzrecht betreffenden Entscheidungen Art. 7 und Art. 8 GRCh parallel an, z. B. EuGH, Rs. C-291/12 NVwZ 2014, 435 (436); EuGH, Rs. C-131/12 EuZW 2014, 541 (548); EuGH, Rs. C-362/14 MMR 2015, 753 (758); hierzu *Guckelberger*, in: EuZW 2010, 939 (946); v. *Lewinski*, in: Auernhammer Kommentar zur DS-GVO; Art. 1, Rn. 5.

Union²¹ (GRCh) und Art. 16²² des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)²³ ein Grundrecht dar.²⁴ Ein solches Recht ergibt sich, auch wenn es nicht ausdrücklich genannt wird, aus Art. 8 der Konvention zum Schutz der Menschenrechte und Grundfreiheiten²⁵ (EMRK).²⁶ Wird dieses Grundrecht bei der Durchführung des digitalen Messstellenbetriebs missachtet, führt das unmittelbar dazu, dass betroffene, zunächst anonyme Personen identifizierbar werden und somit, wie oben bereits erwähnt, ein Rückschluss von der Information auf die dazugehörige Person gezogen werden kann. Damit es dazu nicht kommt, existieren zahlreiche primäre und sekundäre datenschutzrechtliche Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten. Diese sollten ausnahmslos für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, um ein Höchstmaß an Schutz zu gewährleisten. Zur Einhaltung dieser Grundsätze hat der Gesetzgeber mit der Verordnung (EU) 2016/679 vom 27. 4. 2016 - Datenschutz-Grundverordnung²⁷ (DS-GVO) – zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der

²¹ Charta der Grundrechte der Europäischen Union, ABl. EG C 364/1 v. 18. 12. 2000.

²² Nach EG 12 DS-GVO ist Art. 16 AEUV formelle Ermächtigungsgrundlage für die DS-GVO.

²³ Vertrag über die Arbeitsweise der Europäischen Union, ABl. EU L 112/21 v. 24. 4. 2012.

²⁴ EuGH, Rs. C-131/12 NJW 2014, 2257 (2264); *Diregger*, in: Handbuch Datenschutzrecht, S. 51; *Kühling/Klar/Sackmann*, in: Kühling/Klar/Sackmann Datenschutzrecht, Rn. 61; *Weichert*, in: Däubler/Wedde/Weichert/Sommer Kommentar zu DS-GVO, Art. 1 Rn. 12; *Albrecht/Jotzo*, in: Albrecht/Jotzo Das neue Datenschutzrecht der EU, S. 44, Rn. 20; a. A. *Schröder*, in: Streinz Kommentar zum EUV/ AEUV, Art. 16, Rn. 5, vor dem entstehungsgeschichtlichen Hintergrund überzeugt es nicht, Art. 16 Abs. 1 AEUV als Grundrecht auf Datenschutz zu qualifizieren.

²⁵ Konvention Nr. 005 des Europarats, Konvention zum Schutze der Menschenrechte und Grundfreiheiten in der Fassung der Protokolle Nr. 11 und 14, Rom/Rome, 4. XI. 1950; in Deutschland in Kraft getreten 3. 9. 1953 (BGBl. 1954 II S. 14).

²⁶ *Ernst*, in: Paal/Pauly Kommentar zur DS-GVO, Art. 1, Rn. 4; *Hornung/Spiecker gen. Döhmman*, in: Simitis Kommentar zur DS-GVO, Art. 1, Abs. 38; v. *Lewinski* (Fn. 20), Art. 1, Rn. 5; *Albrecht/Jotzo* (Fn. 24), S. 35, Rn. 1.

²⁷ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. EU L 119/11 v. 4. 5. 2016.

Richtlinie 95/46/EG²⁸ – einen EU-weiten, weitestgehend einheitlichen Rechtsrahmen geschaffen.

Mit der DS-GVO soll ein gleichmäßiges Datenschutzniveau für natürliche Personen in der Europäischen Union gewährleistet und sollen Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, beseitigt werden. Weitere Ziele dieser Verordnung sind zum einen die Schaffung von Rechtssicherheit und Transparenz für die Wirtschaftsteilnehmer, einschließlich Kleinunternehmen, sowie kleinere und mittlere Unternehmen und zum anderen die Schaffung gleichwertiger Sanktionen in allen Mitgliedstaaten. Neben der DS-GVO existieren zudem noch zahlreiche sektorenspezifische Datenschutzvorschriften, die bei der Verarbeitung personenbezogener Daten ergänzend beachtet werden müssen. Im Rahmen des digitalen Messstellenbetriebs sind neben der DS-GVO und dem Bundesdatenschutzgesetz²⁹ (BDSG) als allgemeines Datenschutzrecht auch die Vorschriften der §§ 49 ff. MsbG als sektorenspezifisches Datenschutzrecht zu beachten. Insofern steht der MSB zukünftig vor großen Herausforderungen bei der Durchführung eines datenschutzkonformen digitalen Messstellenbetriebs. Zum einen ist er der Pflicht³⁰ ausgesetzt, Anschlussnutzer mit iMS auszustatten³¹ und zum anderen dabei auch alle datenschutzrechtlich relevanten Grundsätze einzuhalten. Zudem muss der MSB gemäß § 45 Abs. 2 Nr. 1 MsbG innerhalb von drei Jahren nach Feststellung der technischen Möglichkeit durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach § 30 MsbG mindestens 10 % der nach § 31 Abs. 1 und 2 MsbG auszustattenden Messstellen mit iMS ausstatten und darf dem Anschlussnutzer für den Messstellenbetrieb insgesamt nicht mehr als die höchste fallbezogene Preisobergrenze dafür jährlich in Rechnung stellen (bezogen auf die Preisobergrenzen nach § 31 MsbG). In der Praxis führen auf der einen Seite die Erfüllung der gesetzlich normierten

²⁸ Richtlinien 95/46/EG des Europäischen Parlaments und des Rates v. 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG L 281/31 v. 23. 11. 1995.

²⁹ Bundesdatenschutzgesetz v. 30. 7. 2017 (BGBl. I S. 2097), das durch Art. 12 des Gesetzes v. 20. 11. 2019 (BGBl. I S. 1626) geändert worden ist.

³⁰ Ausführlich zur Ausstattungspflicht *Mühe*, in: vom Wege/Weise, Praxishandbuch MsbG, S. 41, Rn. 58 f.; *Mitto* (Fn. 13), Rn. 199 ff.

³¹ Die Ausstattungspflicht beschränkt sich auf ortsfeste Zählerpunkte, strombetriebene Fahrzeuge (Elektromobile, Triebfahrzeuge etc.) sind davon nicht betroffen, BT-Drs. 18/8919, S. 2.

Voraussetzungen bei der Umsetzung des Rollouts und der Durchführung des Messstellenbetriebs und auf der anderen Seite die dabei einzuhaltenden aktuell geltenden Datenschutzvorschriften zu erheblichen Problemen und zu großer Rechtsunsicherheit, sowohl auf der Seite des MSB als auch auf der Seite der Anschlussnutzer. Für diese sind insbesondere die Einhaltung von Datenschutz, die Daten- und Manipulationssicherheit sowie die Anonymisierung der Daten wichtige Aspekte bei der Messung unter Zuhilfenahme von iMS.³²

Aus diesem Grund ist das Ziel dieser Arbeit zu klären, inwieweit ein digitaler Messstellenbetrieb mit den aktuell geltenden allgemeinen und sektorenspezifischen Datenschutzgrundsätzen i. S. d. Art. 5 Abs. 1 DS-GVO und § 50 Abs. 1 MsbG vereinbar ist. Zum anderen ist das Ziel, die in der Praxis bestehenden Unsicherheiten zu beseitigen³³ und aufkommende Rechtsfragen zu beantworten, welche beim Einsatz mittels iMS entstehen. Des Weiteren soll dem MSB mit dieser Arbeit aufgezeigt werden, wie die Durchführung eines datenschutzkonformen Messstellenbetriebes zu erfolgen hat, damit das Risiko etwaiger Haftungsfolgen und Sanktionen verringert wird.

Vor diesem Hintergrund erfolgt im ersten Kapitel B dieser Arbeit eine Einführung in den Bereich Messstellenbetrieb sowie eine Erläuterung, was Messstellenbetrieb bedeutet, welche Aufgaben dem MSB obliegen und inwieweit der MSB als Verantwortlicher für den Messstellenbetrieb zugleich auch Verantwortlicher im datenschutzrechtlichen Sinne ist. Im zweiten Kapitel C wird untersucht, inwieweit die Durchführung des Messstellenbetriebs mit den allgemeinen und sektorenspezifischen Datenschutzvorschriften vereinbar ist. Anschließend wird im dritten Kapitel D untersucht, wann und in welchem Umfang der MSB haftbar gemacht werden kann, wenn er gegen aktuell geltende Datenschutzgrundsätze verstoßen hat. Im vierten Kapitel E werden die Rechtsbehelfe erläutert, welche dem MSB und dem Betroffenen bei einer nicht datenschutzkonformen Durchführung des Messstellenbetriebs aus dem allgemeinen Datenschutzrecht zustehen. Abgeschlossen wird die Arbeit mit einem Fazit sowie einem Ausblick, insbesondere im Hinblick bei der Durchführung von Zusatzleistungen beim Messstellenbetrieb.

³² *Hellmuth/Jakobs*, ZfE 2020, 15 (25).

³³ Hierzu zählt insbesondere die Unsicherheit, inwieweit ein datenschutzkonformer digitaler Messstellenbetrieb gewährleistet werden kann.