

Daniel Ennöckl
Universität Wien, Institut für Staats- und Verwaltungsrecht

SMART METER

Anrechnung der digitalen Standardzähler (DSZ) an die
Einführungsquote der intelligenten Messgeräte zur Schaffung
einer konsumentinnenfreundlicheren Lösung

Juli 2017



GERECHTIGKEIT MUSS SEIN

Gutachten

SMART METER

Anrechnung der digitalen Standardzähler (DSZ) an die Einführungsquote
der intelligenten Messgeräte zur Schaffung einer
konsumentenfreundlicheren Lösung

DANIEL ENNÖCKL

Universität Wien, Institut für Staats- und Verwaltungsrecht

Juli 2017

I. Fragestellung

Das Elektrizitätswirtschafts- und -organisationsgesetz 2010 ermächtigt den Bundesminister für Wirtschaft, Familie und Jugend per Verordnung die Einführung intelligenter Messeinrichtungen festzulegen. Im Fall der Verordnungserlassung sind die Netzbetreiber dazu verpflichtet, EndverbraucherInnen mit intelligenten Messgeräten auszustatten. Im Rahmen dieser Verordnung hat der Netzbetreiber aber auch den Wunsch der EndverbraucherInnen, kein intelligentes Messgerät zu erhalten, zu berücksichtigen.

In der Intelligenten Messgeräte-Einführungsverordnung 2014 (IME-VO 2014) wird vorgegeben, dass die Netzbetreiber bis Ende 2019 mindestens 95 % der an das Netz angeschlossenen Zählpunkte als intelligente Messpunkte gemäß der Intelligenten Messgeräte-Anforderungs-Verordnung der E-Control 2011 (IMA-VO 2011) auszustatten haben.

Nach der Regelung der IME-VO müssen die Netzbetreiber 95 % der Haushalte mit einem Smart Meter ausrüsten. Demgegenüber steht § 83 Abs. 1 EIWOG, wonach die Netzbetreiber den Wunsch der EndverbraucherInnen berücksichtigen müssen, kein intelligentes Messgerät zu erhalten. Die vorliegende Studie untersucht, wie diese Diskrepanz aufgelöst und eine konsumentenfreundliche Lösung implementiert werden kann. Insbesondere wird geprüft, ob eine Nutzung von intelligenten Messgeräten durch die Netzbetreiber gegen den Willen der betroffenen KonsumentInnen mit dem Datenschutzgesetz 2000 (DSG 2000) vereinbar ist, sowie ob die Bereitstellung sogenannter Digitaler Standardzähler (DSZ), also von Messgeräten, die keine Viertelstundenwerte speichern und über keine Abschaltfunktion bzw. Leistungsbegrenzungsfunktion verfügen, in die 95 %-Quoten eingerechnet werden können.

II. Rechtsrahmen für intelligente Messgeräte

A. Unionsrechtlicher Rahmen

Die Verpflichtung, Haushalte weitestgehend flächendeckend mit intelligenten Messgeräten auszustatten, geht auf die EU-Elektrizitätsbinnenmarkt-RL 2009/72/EG¹ zurück. Die Richtlinie ordnet in Art. 3 Abs. 11 an, dass, um die Energieeffizienz zu fördern, die Mitgliedstaaten, **oder wenn dies von einem Mitgliedstaat vorgesehen ist, die Regulierungsbehörden nachdrücklich empfehlen, dass die Elektrizitätsunternehmen den Stromverbrauch optimieren, indem sie beispielsweise Energiemanagementdienstleistungen anbieten, neuartige Preismodelle entwickeln oder gegebenenfalls intelligente Messsysteme oder intelligente Netze einführen.**

Für die Auslegung dieser Bestimmung und die Beurteilung ihrer Datenschutzkonformität ist zu beachten, dass Art. 3 EU-Elektrizitätsbinnenmarkt-RL die Überschrift **„Gemeinwirtschaftliche Verpflichtungen und Schutz der Kunden“** trägt. Der Einbau intelligenter Messgeräte wird vom europäischen Gesetzgeber somit eindeutig als Maßnahme des KonsumentInnenschutzes verstanden.

Darauf aufbauend normiert der Anhang I der EU-Elektrizitätsbinnenmarkt-RL (Überschrift: *„Maßnahmen zum Schutz der Kunden“*) in seinem Abs. 2, dass die Mitgliedstaaten gewährleisten, dass intelligente Messsysteme eingeführt werden, durch die die aktive Beteiligung der VerbraucherInnen am Stromversorgungsmarkt unterstützt wird. **Die Einführung dieser Messsysteme kann einer wirtschaftlichen Bewertung unterliegen, bei der alle langfristigen Kosten und Vorteile für den Markt und die einzelnen VerbraucherInnen geprüft werden sowie untersucht wird, welche Art des intelligenten Messens wirtschaftlich vertretbar und kostengünstig ist und in welchem zeitlichen Rahmen die Einführung praktisch möglich ist.** Entsprechende Bewertungen haben bis 03.09.2017 stattzufinden. Anhand dieser Bewertung erstellen die Mitgliedstaaten oder eine von ihnen benannte zuständige Behörde einen Zeitplan mit einem Planungsziel von 10 Jahren für die Einführung der intelligenten Messsysteme. **Wird die Einführung intelligenter Zähler positiv bewertet, so werden mindestens 80 % der VerbraucherInnen bis 2020 mit intelligenten Messsystemen ausgestattet.** Die Mitgliedstaaten oder die von ihnen benannten zuständigen Behörden sorgen für die Interoperabilität der Messsysteme, die in ihrem Hoheitsgebiet eingesetzt werden und tragen der Anwendung der entsprechenden Normen und bewährten Verfahren sowie der großen Bedeutung, die dem Ausbau des Elektrizitätsbinnenmarkts zukommt, gebührend Rechnung.

¹ Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates vom 13.07.2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG (Elektrizitätsbinnenmarkt-RL), ABL vom 14. .2009, L 211, 55.

B. Nationale Umsetzungsregelungen

Die Umsetzung der Verpflichtung zur Bereitstellung von intelligenten Messgeräten im österreichischen Recht erfolgte zunächst mit dem Elektrizitätswirtschafts- und -organisationsgesetz 2010, BGBl I 110/2010.² Das Gesetz in dieser Fassung trat am 03.03.2011 in Kraft und normiert in § 7 Abs. 1 Z 31 eine Legaldefinition des Begriffs; demnach ist unter einem „intelligenten Messgerät“ eine „technische Einrichtung, die den tatsächlichen Energieverbrauch und Nutzungszeitraum zeitnah misst, und die über eine fernauslesbare, bidirektionale Datenübertragung verfügt“ zu verstehen.

Darüber hinaus ordnete § 83 EIWOG i.d.F. BGBl I 110/2010 an, dass der Bundesminister für Wirtschaft, Familie und Jugend nach Durchführung einer Kosten/Nutzanalyse die Einführung intelligenter Messeinrichtungen festlegen kann. Dies hat nach Anhörung der Regulierungsbehörde und der Vertreter des KonsumentInnen schutzes durch Verordnung zu erfolgen. Die Netzbetreiber sind im Fall der Erlassung dieser Verordnung zu verpflichten, jene EndverbraucherInnen, deren Verbrauch nicht über einen Lastprofilzähler gemessen wird, mit intelligenten Messgeräten auszustatten. Nach Abs. 2 hat der Betrieb von intelligenten Messgeräten unter Wahrung des Daten- und KonsumentInnen schutzes zu erfolgen; die Regulierungsbehörde hat die Vertreter des KonsumentInnen schutzes sowie die Datenschutzkommission weitestmöglich einzubinden.

In jene Fassung, in der die Bestimmungen betreffend intelligente Messgeräte noch heute im EIWOG normiert sind, wurden die Regelungen der §§ 83 ff EIWOG mit dem Bundesgesetz, mit dem das Elektrizitätswirtschafts- und -organisationsgesetz 2010, das Gaswirtschaftsgesetz 2011 und das Energie-Control-Gesetz geändert werden, BGBl I 174/2013 gebracht. Die vom Nationalrat beschlossene Fassung der genannten Regelungen geht auf einen Abänderungsantrag der Abgeordneten Peter Haubner, Wolfgang Katzian, Mag. Christiane Brunner, Mag. Rainer Widmann, Ing. Robert Lugar, Kolleginnen und Kollegen zu dem Antrag 2323/A der Abgeordneten Peter Haubner, Wolfgang Katzian, Kolleginnen und Kollegen (AA-345) zurück. § 83 EIWOG sieht demnach ergänzend zur Regelung i.d.F. BGBl I 110/2010 (unter anderem) vor, dass die Netzbetreiber zu verpflichten sind, „jene Endverbraucher, deren Verbrauch nicht über einen Lastprofilzähler gemessen wird, mit intelligenten Messgeräten auszustatten, über die Einführung, insbesondere auch über die Kostensituation, die Netzsituation, Datenschutz und Datensicherheit und Verbrauchsentwicklung bei den Endverbrauchern, Bericht zu erstatten und die Endverbraucher zeitnah über den Einbau eines intelligenten Messgeräts sowie die damit verbundenen Rahmenbedingungen zu informieren. Im Rahmen der durch die Verordnung bestimmten Vorgaben für die Installation intelligenter Messgeräte hat der Netzbetreiber den Wunsch eines Endverbrauchers, kein intelligentes Messgerät zu erhalten, zu berücksichtigen.“

² Bundesgesetz, mit dem das Elektrizitätswirtschafts- und -organisationsgesetz 2010 und das Energie-Control-Gesetz erlassen werden, BGBl I Nr. 110/2010.

Das Gesetz ordnet somit an, dass die KonsumentInnen das Recht haben, mittels einseitiger Erklärung den Einbau eines Smart Meters abzulehnen. Der Netzbetreiber hat diesem Wunsch zu entsprechen. Dieses Opt-out-Recht kommt den KonsumentInnen dem Wortlaut der Bestimmung allerdings nur insoweit entgegen, als dadurch die Vorgaben der IME-VO³ nicht beeinträchtigt werden (so auch die Begründung des Abänderungsantrags AA-345).

Aufgrund des § 83 Abs. 1 EIWOG wurde die soeben erwähnte IME-VO erlassen. Diese normiert in ihrer derzeit geltenden Fassung, dass jeder Netzbetreiber bis Ende 2017 mindestens 70 % und im Rahmen der technischen Machbarkeit, bis Ende 2019 mindestens 95 % der an sein Netz angeschlossenen Zählpunkte als intelligente Messgeräte (§ 7 Abs. 1 Z 31 EIWOG) gemäß den Vorgaben der Verordnung der E-Control, mit der die Anforderungen an intelligente Messgeräte bestimmt werden (Intelligente Messgeräte-AnforderungsVO 2011), auszustatten hat (§ 1 Abs. 1 Z 2 und 3 IME-VO). Die Entscheidung, welche EndverbraucherInnen mit welcher Art von intelligenten Messgeräten ausgestattet werden, liegt dabei im Ermessen des jeweiligen Netzbetreibers.

Gemäß § 83 Abs. 2 EIWOG hat die Regulierungsbehörde jene Anforderungen durch Verordnung zu bestimmen, denen diese intelligenten Messgeräte zu entsprechen haben. Dementsprechend wurde im BGBl II 339/2011 die Verordnung der E-Control, mit der die Anforderungen an intelligente Messgeräte bestimmt werden (Intelligente Messgeräte-AnforderungsVO 2011 – IMA-VO 2011), kundgemacht.

Schließlich sieht § 83 Abs. 6 EIWOG vor, dass, sofern es die Gewährleistung von Datenschutz und Datensicherheit im Zusammenhang mit dem Betrieb von intelligenten Messsystemen erfordert, der Bundesminister für Wirtschaft, Familie und Jugend im Einvernehmen mit dem Bundeskanzler mit Verordnung, unter Bedachtnahme auf die relevanten internationalen Vorschriften sowie die technische und wirtschaftlich vertretbare Umsetzbarkeit, nähere Bestimmungen zum Stand der Technik festlegen kann, welchen ein Netzbetreiber zu entsprechen hat. Dabei sind insbesondere die jährlichen Berichte der Regulierungsbehörde sowie internationale Sicherheitsstandards zu berücksichtigen. Eine solche Verordnung wurde aber bislang nicht erlassen.

³ Verordnung des Bundesministers für Wirtschaft, Familie und Jugend, mit der die Einführung intelligenter Messgeräte festgelegt wird (Intelligente Messgeräte-Einführungsverordnung – IME-VO), BGBl 138/2012 i.d.F. BGBl II 323/2014.

III. Grundrecht auf Datenschutz und intelligente Messgeräte

A. Vorliegen personenbezogener Daten

Der Terminus „*personenbezogene Daten*“ ist der zentrale Begriff des DSG 2000, weil das Gesetz nur dann auf eine Informationsverarbeitung anwendbar ist, wenn sie sich auf solche Daten bezieht. Nach § 4 Z 1 DSG 2000 sind unter dem Begriff *personenbezogene Daten* „Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist“ zu verstehen. Aus dieser Definition folgt, dass der Datenbegriff des DSG 2000 in seinem Kern zwei Elemente aufweist. Er verlangt einerseits einen bestimmten Informationsgehalt über eine individuelle Person sowie andererseits dessen Zuordnung oder Zuordenbarkeit zum Betroffenen.⁴

Das Kriterium, dass eine „Angabe“ über einen Betroffenen vorliegen muss, umfasst sämtliche Arten von Informationen, die über eine individuelle Person gegeben werden können. Eine inhaltliche Einschränkung nimmt das DSG 2000 nicht vor. Daher gelten alle Aussagen über die Bezugsperson als Daten, egal auf welchen Aspekt ihres Lebens sie sich beziehen.⁵

Das zweite Element eines Datums ist sein Personenbezug, also die Möglichkeit der Zuordnung der Angabe zu einer individuellen Person. Damit eine Information als Datum i.S.d. DSG 2000 qualifiziert werden kann, muss die Identität desjenigen, über den Angaben gemacht werden, entweder „bestimmt“ oder „bestimmbar“ und damit die Information mit der Person des Betroffenen verknüpfbar sein.

Die Begriffe „bestimmt“ und „bestimmbar“ – aus denen sich der sachliche Anwendungsbereich sämtlicher datenschutzrechtlicher Regelungen ergibt – sind im DSG 2000 weder definiert, noch wird sonst präzisiert, wie eine Angabe formuliert sein muss, damit sie einen Personenbezug aufweist. Auch die Datenschutz-Richtlinie (DSRL⁶) und die Datenschutzgrundverordnung (DSGVO⁷) differenzieren nicht zwischen diesen beiden Termini. Die Abgrenzung, ob der Betroffene „bestimmt“ oder lediglich „bestimmbar“ ist, ergibt sich aus der Informationsquelle, anhand derer der Personenbezug hergestellt werden kann.⁸ Als „bestimmt“ gilt der Betroffene demnach, wenn sich seine Identität aus der Angabe selbst ergibt oder aufgrund ihres Inhaltes und der Umstände der Aussage feststeht, dass sich die darin enthaltenen Informationen ausschließlich auf ihn beziehen können. Dies ist insbesondere dann der Fall, wenn das Datum den Namen des Betroffenen umfasst.⁹ Der Personenbezug ist darüber hinaus dann

⁴ Ennöckl, Der Schutz der Privatsphäre [2014] 107.

⁵ Jahnel, Datenschutzrecht [2010] 127.

⁶ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl vom 23.11.1995, L. 281, S. 31.

⁷ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl vom 04.05.2016, L 119, 1.

⁸ Ähnlich Dohr/Pollirer/Weiss/Knyrim, Kommentar DSG, § 4, Anm. 2.

⁹ Stelzer/A. Lehner, Datenschutz in Biobanken, ZfV 2008, 742f.

bestimmt, wenn die Angabe zwar nicht den Namen, jedoch andere Merkmale enthält, die in Summe nur eine einzige Person erfüllt, sodass es möglich ist, die Identität des Betroffenen zu bestimmen.¹⁰

In Abgrenzung dazu ist der Personenbezug einer Angabe lediglich „bestimmbar“, wenn aus ihr alleine der Betroffene nicht zwingend ermittelt werden kann und seine Identität in der Angabe daher nicht exklusiv determiniert ist. Mit Hilfe zusätzlicher Informationen, die im betreffenden Datum nicht enthalten sind, besteht hinsichtlich bestimmbarer personenbezogener Daten aber dennoch die Möglichkeit, den Betroffenen zu identifizieren.¹¹ Es reicht dabei aus, wenn der Personenbezug nicht unmittelbar zum Zeitpunkt der Datenerhebung oder Speicherung, sondern erst nachträglich hergestellt werden kann. Ob die Identifizierung des Betroffenen tatsächlich erfolgt oder regelmäßig unterbleibt, ist für die Anwendbarkeit des Datenschutzrechts unerheblich.¹²

Hinter dieser Einbeziehung bestimmbarer personenbezogener Daten steckt der Anspruch, den Datenschutz nicht auf Angaben zu beschränken, die in einem direkten Kontext mit Identifizierungsmerkmalen stehen und den Personenbezug zum Betroffenen unmittelbar enthalten. Es sollen auch solche Daten erfasst werden, bei denen die Zurechnung zu einer bestimmten Person erst mittelbar durch die Inanspruchnahme „externer“ Angaben erfolgen kann.

Unstrittig ist, dass die Information über den Energieverbrauch in einem bestimmten Haushalt eine Angabe i.S.d. § 4 Z 1 DSGVO 2000 darstellt. Zu prüfen ist allerdings, ob diese Information einem individuellen und damit bestimmbareren Betroffenen zugerechnet werden kann. Dies vor dem Hintergrund, dass in einem Haushalt regelmäßig nicht nur eine einzelne Person, sondern mehrere Menschen leben und daher keine exakte Zuordnung der Gesamtmenge auf die einzelnen BewohnerInnen möglich ist.

In diesem Zusammenhang ist die Legaldefinition des Begriffs des *Betroffenen* in § 4 Z 3 DSGVO 2000 maßgeblich; demnach ist der Betroffene „jede vom Auftraggeber verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden.“ Unter der Betroffenenkategorie der „Personengemeinschaft“ fallen nicht nur handelsrechtliche Personengesellschaften ohne Rechtspersönlichkeit,¹³ sondern auch Personengruppen, die „infolge eines die Mitglieder verbindenden Objektbezuges eine unterscheidbare Entität darstellen.“¹⁴ Ein solcher gemeinsamer Objektbezug verbindet etwa die Mitglieder einer Hauseigentümergeinschaft oder die Angehörigen eines Haushaltes. „Daher stellen die Angaben über den Stromverbrauch eines von

¹⁰ Vgl. EuGH 6.11.2003, Rs C-101/01, *Lindqvist*, Slg 2003, I-12971, Rz 27.

¹¹ Stellungnahme der Art.-29-Datenschutzgruppe 4/2007 zum Begriff „personenbezogenes Datum“, 01248/07/DE, 14; *Jahnel*, Begriff und Arten von personenbezogenen Daten, in: *Jahnel* (Hrsg.), *Datenschutzrecht und E-Government Jahrbuch 2008* (2008) 32.

¹² *Jahnel*, Das Grundrecht auf Datenschutz, in: *Akyürek/Baumgartner/Jahnel/Lienbacher/Stolzlechner* (Hrsg.), *Staat und Recht in europäischer Perspektive, Festschrift für Heinz Schäffer* (2006) 319.

¹³ *Jahnel*, *Datenschutzrecht* 123.

¹⁴ *Ennöckl*, *Privatsphäre* 146.

*mehreren Personen benützten Hauses oder einer Wohnung zwar keine personenbezogenen Daten über die einzelnen Bewohner dar, weil sich aus der Gesamtmenge nicht der Einzelenergieverbrauch dieser Personen ableiten lässt. Dem Haushalt bzw. der Eigentümergemeinschaft als solcher kommt zu einer derartigen Information aber die Stellung als Betroffener in Form einer Personengemeinschaft i.S.d. § 4 Z 3 DSG 2000 zu.*¹⁵

Das DSG 2000 differenziert – den Vorgaben der DSRL und der DSGVO entsprechend – darüber hinaus zwischen sensiblen und nicht sensiblen Daten. Auch wenn der Energieverbrauch eines Haushaltes sehr weitreichende Rückschlüsse auf die Nutzung einer Wohnung oder eines Hauses und die Lebensgewohnheiten der BewohnerInnen zulässt, so sind diese Angaben dennoch als nicht sensibel anzusehen. Als sensibel gelten gemäß § 4 Z 2 DSG 2000 nämlich nur Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben. Diese Voraussetzungen erfüllen die Angaben über den Energieverbrauch nicht. Die (strengerer) Regelungen¹⁶ über die Verarbeitung sensibler Daten sind daher bei der Anwendung intelligenter Messgeräte nicht anzuwenden.

B. Automationsunterstützte Datenverarbeitung

Der Regelungszweck des Datenschutzrechts liegt primär im Schutz der Persönlichkeitssphäre der BürgerInnen vor dem zunehmenden Einsatz moderner Informationstechnologien.¹⁷ Daher fallen automationsunterstützt verarbeitete Daten uneingeschränkt in den Anwendungsbereich des DSG 2000. Sämtliche Formen digitaler Informationsaufzeichnung im Rahmen von elektronischen Datenverarbeitungssystemen sind daher anhand der Vorgaben des DSG 2000 auf ihre Zulässigkeit zu prüfen.

Um den Datenschutz umfassend zu gewährleisten und um zu verhindern, dass dieser durch die Wahl der technischen Form der Datenaufzeichnung umgangen werden kann, ist das Datenschutzrecht seit dem Jahr 2000 (in Umsetzung der DSRL) darüber hinaus auch für manuelle (im Sinne von konventionell, also nicht automationsunterstützt verarbeitete) Daten maßgeblich. Voraussetzung dafür ist, dass die Daten Teil einer „Datei“ sind. Darunter wird eine „strukturierte Sammlung von Daten“ verstanden, „die nach mindestens einem Suchkriterium zugänglich sind“.

Da im Fall der Smart Meter die Datenermittlung und -übertragung vollständig digitalisiert erfolgt, ist das DSG 2000 zur Gänze auf die in diesem Rahmen erfolgende Verarbeitung von Energieverbrauchsdaten durch intelligente Messgeräte anzuwenden. Es liegt eine durchgehende automationsunterstützte

¹⁵ Ennöckl, Privatsphäre 147.

¹⁶ Für die Verwendung sensibler Daten müssen strengere Voraussetzungen (§§ 9, 46 Abs. 3 DSG 2000) erfüllt sein, sie ist der Vorabkontrolle bei der Registrierung unterworfen (§ 18 Abs. 2 Z 1 DSG 2000) und es besteht eine jederzeitige Überprüfungsmöglichkeit durch die DSB (§ 30 Abs. 3 DSG 2000).

¹⁷ Vgl. AB zum DSG 1978 1024 BlgNR 14. GP.

Datenverarbeitung vor, die insbesondere dem Grundrecht auf Datenschutz gemäß § 1 DSG 2000 zu entsprechen hat.

C. Grundrecht auf Geheimhaltung personenbezogener Daten

Nach § 1 Abs. 1 DSG 2000 hat jedermann, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen schutzwürdigen Geheimhaltungsinteresses ist nur dann ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind. Dies ist in Bezug auf den Energieverbrauch eines Haushaltes nicht der Fall. Weder sind diese Informationen frei zugänglich (im Sinne einer allgemeinen Verfügbarkeit) noch ist es ausgeschlossen, dass der Netzbetreiber diese Daten einer bestimmten Adresse und damit einem konkreten Betroffenen zuordnen kann.

Das Recht auf Geheimhaltung personenbezogener Daten schützt den Betroffenen nicht nur vor einer Weitergabe von Daten an Dritte; in das Grundrecht wird vielmehr bereits dann eingegriffen, wenn personenbezogene Daten ermittelt und aufgezeichnet werden.¹⁸ Jede Verwendung von personenbezogenen Daten ist ein Informationseingriff und bedarf als solcher einer Rechtfertigung.¹⁹ Auch die strukturierte Evidenzhaltung personenbezogener Daten greift in den Schutzbereich des Grundrechts auf Geheimhaltung ein.²⁰

Unbedeutend ist die Art und Weise, auf die die Daten verarbeitet werden und in welchem technischen Verfahren die Speicherung vorgenommen wird. Auf elektronischen Speichermedien festgehaltene Angaben sind daher ebenso grundrechtsrelevant wie solche, die auf konventionellen Datenträgern aufgezeichnet werden.

Für den Einsatz von Smart Metern folgt daraus, dass bereits das Aufzeichnen und Speichern des Stromverbrauchs eines Haushaltes einen (rechtfertigungsbedürftigen) Grundrechtseingriff darstellt, selbst wenn die Daten nicht (täglich oder im 15-Minuten-Intervall) an den Netzbetreiber übermittelt, sondern lediglich (als Monatsverbrauchswert) „vor Ort“ im Messgerät gespeichert werden.

D. Beschränkungen des Grundrechts

Der Anspruch des Betroffenen auf Geheimhaltung seiner personenbezogenen Daten steht in ständigem Konflikt mit gegenläufigen Interessen anderer – sei es staatlicher Behörden, sei es Privater – an der

¹⁸ VfSlg 12.880/1991, 16.369/2001.

¹⁹ *Öhlinger/Eberhard*, Verfassungsrecht ¹¹ (2016) Rz 830.

²⁰ DSK 21.1.2003, K120.757/001-DSK/2003; *Lehner/Lachmayer*, Datenschutz im Verfassungsrecht, in: Bauer/Reimer (Hrsg.), Handbuch Datenschutzrecht (2009) 95 (99).

Erhebung und (sonstigen) Verwendung von Daten. Da sich in einer Informationsgesellschaft niemand der automationsunterstützten Verarbeitung von Angaben zu seiner Person entziehen kann, wirkt das Grundrecht auf Datenschutz nicht absolut, sondern darf unter den in § 1 Abs. 2 DSG 2000 genannten Gründen beschränkt werden.

Die Ermächtigung des § 1 Abs. 2 DSG 2000 weist eine denkbar komplizierte Struktur von verschiedenen Eingriffstypen auf und unterscheidet sich grundlegend von den Vorbehalten anderer Grundrechte: Während die Gesetzesvorbehalte anderer grundrechtlicher Gewährleistungen regeln, inwieweit der einfache Gesetzgeber in den Schutzbereich des Grundrechts eingreifen kann, sieht § 1 Abs. 2 DSG 2000 u.a. vor, dass gewisse Beschränkungen des Rechts auf Datenschutz auch dann zulässig sind, wenn sie sich auf keine gesetzliche Grundlage stützen können, sofern sie bestimmten materiellen Anforderungen entsprechen. Dies ist Folge der Horizontalwirkung des Grundrechts.²¹ Da die datenschutzrechtlichen Ansprüche auch gegenüber Privaten geltend gemacht werden können, wird bei den Bedingungen für Beschränkungen des Grundrechts je nach Grundrechtsverpflichteten unterschieden und es werden für Grundrechtseingriffe staatlicher Behörden andere Anforderungen aufgestellt als für solche Privater oder privatwirtschaftlich handelnder Auftraggeber.

Dem Gedanken der informationellen Selbstbestimmung folgend sieht § 1 Abs. 2 DSG 2000 zunächst vor, dass die datenschutzrechtlichen Gewährleistungen aufgrund der höchstpersönlichen, individuellen Interessenlage des Betroffenen selbst beschränkt werden können; zulässig sind Eingriffe in den Geheimhaltungsanspruch demnach, wenn sie im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgen.

Liegen diese Voraussetzungen nicht vor, muss sich eine Grundrechtsbeschränkung auf überwiegende berechnete Interessen eines anderen stützen können; darunter können sowohl die Interessen Privater als auch öffentliche Interessen fallen. In beiden Varianten ist zwingend eine Abwägung mit den Geheimhaltungsinteressen des Betroffenen vorzunehmen. Erfolgt der Eingriff durch staatliche Behörden, so bedarf dieser zusätzlich einer gesetzlichen Grundlage, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sein muss.

Schließlich enthält § 1 Abs. 2 letzter Satz DSG 2000 den sogenannten Grundsatz der Datensparsamkeit, wonach alle Grundrechtseingriffe – unabhängig vom Eingriffssubjekt – nur in der jeweils gelindesten zielführenden Art erfolgen dürfen und damit einer Verhältnismäßigkeitsprüfung unterliegen.

²¹ *Jahnel*, Grundrecht 337; *Berka*, Die Grundrechte (1999) Rz 224; *Öhlinger/Eberhard*, Verfassungsrecht, Rz 833; *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht¹¹ (2015) Rz 1492; *Wiederin*, Schutz der Privatsphäre,

a) Lebenswichtige Interessen des Betroffenen

Als ersten Fall einer zulässigen Beschränkung des Anspruchs auf Geheimhaltung sieht § 1 Abs. 2 DSG 2000 die Verwendung von personenbezogenen Daten im lebenswichtigen Interesse des Betroffenen vor. Lebenswichtige Interessen des Betroffenen sind berührt, wenn für diesen eine Lebensgefahr oder eine akute ernste Gefährdung seiner Gesundheit besteht, die nur durch die beabsichtigte Datenverwendung abgewendet werden kann. Die betreffenden Daten können, müssen aber nicht zwingend (notfall-)medizinische Daten sein; auch die Ermittlung von Standortdaten der Telekommunikation zum Auffinden von Verunglückten kann etwa eine Datenverwendung im lebenswichtigen Interesse des Betroffenen darstellen, ohne dass die dabei eingesetzten Daten einen medizinischen Konnex aufweisen.

Für die Ermittlung von Energieverbrauchsdaten mittels intelligenter Messgeräte kann ausgeschlossen werden, dass diese im lebenswichtigen Interesse des Betroffenen erfolgt. Es ist mir keine Fallkonstellation ersichtlich, in denen die Energieverbrauchsdaten verwendet werden müssen, um eine Lebensgefahr oder eine akute ernste Gefährdung der Gesundheit des Betroffenen abzuwehren. Die Datenverarbeitung durch Smart Meter kann sich daher nicht auf diesen Rechtfertigungstatbestand stützen.

b) Zustimmung des Betroffenen

Die Aufnahme der Zustimmung als zusätzliche Eingriffsermächtigung im DSG 2000 wurde damit begründet, dass mit ihr anerkannt werden sollte, dass „*in erster Linie der Betroffene selbst über das Schicksal der ihn betreffenden Daten zu entscheiden hat*“.²² Mit diesem Rechtfertigungsgrund kommt – dem Gedanken der informationellen Selbstbestimmung folgend – zum Ausdruck, dass der Einzelne selbst darüber disponieren darf, ob und welche Angaben zu seiner Person verwendet werden.²³

Das DSG 2000 enthält in § 4 Z 11 DSG 2000 eine Legaldefinition des Begriffs der Zustimmung. Demnach ist darunter „*die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt*“, zu verstehen. Diese Legaldefinition wirkt, da sich das dem Grundrecht auf Datenschutz in seiner Gesamtheit innewohnende Begriffsverständnis an jenem des § 4 DSG 2000 orientiert, auch auf die Eingriffsermächtigung des § 1 Abs. 2 DSG 2000 ein.²⁴ In materieller Hinsicht folgt aus ihr, dass das

²² EBRV 1613 BlgNR 20. GP zu § 1 DSG 2000.

²³ Siehe auch *Kopetzki*, Einwilligung und Einwilligungsfähigkeit, in: *Kopetzki* (Hrsg), *Einwilligung und Einwilligungsfähigkeit* (2002)1.

²⁴ *Jahnel*, Grundrecht 330; a.A. *Reimer*, Verfassungs- und europarechtliche Überlegungen zur datenschutzrechtlichen Zustimmung, in: *Jahnel/Siegwart/Fercher* (Hrsg), *Aktuelle Fragen des Datenschutzrechts* (2007) 199, der von einem eigenen verfassungsrechtlichen Begriffsverständnis ausgeht; meines Erachtens nicht schlüssig die Argumentation *Dohr/Pollirer/Weiss/Knyrim*, DSG, § 1, Anmerkung 12, wonach dies nur für sensible Daten gelten soll.

Vorliegen einer wirksamen datenschutzrechtlichen Zustimmung voraussetzt, dass der Betroffene in Kenntnis der Sachlage und freiwillig in eine Datenverwendung einwilligt. Das bedeutet, dass er volle Kenntnis davon haben muss, in welchem Umfang und zu welcher Art von Angaben zu seiner Person er zustimmt, an wen die Daten übermittelt werden dürfen und zu welchem Zweck dies erfolgt, sowie dass die Willenserklärung ohne Drohung oder Zwang und außerhalb von Abhängigkeitsverhältnissen erteilt wird.²⁵ Die Schriftlichkeit der Erklärung ist hingegen keine Voraussetzung für eine gültige Zustimmung (mehr²⁶). Eine ausdrückliche Einwilligung zur Datenverwendung wird nur hinsichtlich sensibler Daten verlangt.²⁷ Da eine solche aber nicht für den Rechtfertigungstatbestand des § 1 Abs. 2 DSG 2000 vorausgesetzt wird, können auch konkludente Willenserklärungen einen Grundrechtseingriff in Form der Verwendung nicht sensibler Daten rechtfertigen.²⁸

Die Möglichkeit, die datenschutzrechtliche Zustimmung jederzeit widerrufen zu können, ist weder in der Verfassungsbestimmung des § 1 DSG 2000 noch in der Legaldefinition des § 4 Z 11 DSG 2000 als Voraussetzung für eine wirksame Einwilligung vorgesehen. In den einfachgesetzlichen Regelungen zur Datenverwendung der §§ 8 Abs. 1 Z 2 und 9 Z 6 DSG 2000 wird die jederzeitige Widerrufsmöglichkeit allerdings als Tatbestandselement normiert.

Nicht relevant ist im Fall einer datenschutzrechtlichen Zustimmung das Gebot des gelindesten Mittels (Gebot der Datensparsamkeit), weil sich im Fall der Einwilligung der Umfang der zulässigen Datenverwendung nicht allein aus ihrem Zweck, sondern primär aus der Erklärung des Betroffenen ergibt. Ihm obliegt es, durch seine Willenserklärung zu bestimmen, für welche Aufgabe und in welchem Umfang Angaben zu seiner Person verwendet werden dürfen. Stimmt er zu, dass eine bestimmte ihn betreffende Information genutzt werden darf, so ist die darauf gestützte Datenverwendung selbst dann zulässig, wenn der mit ihr verfolgte Zweck auch mit Daten in einem geringeren Umfang erreicht werden könnte.²⁹

²⁵ Vgl. OGH 27.1.1999, 7 Ob 170/98w; 22.3.2001, 4 Ob 28/01y = ecolex 2001, 147 mit Glosse *Rabl*, 13.9.2001, 6 Ob 16/01y = ecolex 2002, 86 mit Anmerkung *Leitner*, 19.11.2002, 4 Ob 179/02f; dazu *Iro*, OGH: Unwirksame Klauseln in den Allgemeinen Geschäftsbedingungen der Banken, RdW 2003, 66; zur Zustimmung im Rahmen von AGBs siehe *Knyrim*, Datenschutzrecht 165 ff. Die zum DSG 1978 ergangene Rechtsprechung zu den Zustimmungserfordernissen kann angesichts der umfassenden Formulierung des § 4 Z 14 DSG 2000 meines Erachtens auf die Bestimmung des § 4 Z 14 DSG 2000 unmittelbar übertragen werden; ebenso *Duschanek*, § 1 DSG 2000, Rz 47.

²⁶ Vgl. demgegenüber §§ 7 Abs. 1 Z 2, 18 Abs. 1 Z 1 DSG 1978.

²⁷ *Dammann/Simitis*, EG-Datenschutzrichtlinie (1997) Art. 8, Anm. 9; *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000) 52.

²⁸ *Lehner*, Recht auf Datenschutz, in: Heißl (Hrsg.), Handbuch Menschenrechte (2009) Rz 11/28; *Jahnel*, Grundrecht 330; *Grabenwarter*, Datenschutzrechtliche Anforderungen an den Umgang mit Kundendaten im Versandhandel, ÖJZ 2000, 867.

²⁹ AA *Reimer*, Zustimmung 189.

c) Zustimmung und Opt-out-Regelung

§ 83 EIWOG normiert, dass im Rahmen der durch die IME-VO bestimmten Vorgaben für die Installation intelligenter Messgeräte der Netzbetreiber den Wunsch der EndverbraucherInnen, kein intelligentes Messgerät zu erhalten, zu berücksichtigen hat. Die in dieser Regelung eingeräumte Datenverwendungsbefugnis kann sich somit nicht auf eine Zustimmung der Betroffenen im Sinne des § 4 Z 11 DSG 2000 stützen, sondern räumt den Netzbetreibern das Recht auf Datenverarbeitung bereits dann ein, solange ein ausdrücklicher Widerspruch der Betroffenen unterbleibt.

Eine ähnliche Regelung findet sich in den Regelungen zur Elektronischen Gesundheitsakte (ELGA).³⁰ Auch in diesem Rahmen wurde ein „Opt-out-Modell“ implementiert, demzufolge der Teilnahme am ELGA-System jederzeit widersprochen werden kann. Die Datenschutzrechtskonformität dieses Modells wurde bislang nicht ausjudiziert. Vor dem Hintergrund, dass es aber in der Praxis unmöglich wäre, von allen Betroffenen Zustimmungserklärungen einzuholen, wird es in der Literatur aber als verhältnismäßige Ausgestaltung einer Datenverwendungsbefugnis angesehen.³¹ Zu beachten ist in diesem Zusammenhang allerdings, dass das ELGA-System keine Quote betreffend das Opt-out-Recht kennt; vielmehr kann jede/r Betroffene die Teilnahme unbeschränkt verweigern.

Folgt man dieser Ansicht, bedeutet dies, dass die Datenverwendung in Bezug auf jene KonsumentInnen, die sich nicht gegen den Einbau eines intelligenten Messgerätes ausgesprochen haben, mit dem Grundrecht auf Datenschutz nach § 1 Abs. 1 DSG 2000 vereinbar ist. Zu untersuchen ist daher, ob die Ermittlung der Energieverbrauchsdaten mittels Smart Metern auch in jenen Fällen zulässig sein kann, in denen sich die VerbraucherInnen nach § 83 Abs. 1 EIWOG dagegen ausgesprochen haben, diesem Wunsch infolge der Quotenvorgaben der §§ 1 Abs. 1 Z 2 und 3 IME-VO aber nicht entsprochen werden kann.

d) Eingriffe wegen überwiegender berechtigter Interessen anderer

Können sich Eingriffe in das Grundrecht auf Datenschutz durch den Gesetzgeber nicht auf lebenswichtige Interessen oder die Zustimmung des Betroffenen stützen, sind sie nur dann gerechtfertigt, wenn sie in Wahrung überwiegender Interessen anderer erfolgen. Für den dabei anzulegenden Maßstab kommt es darauf an, ob die vom Gesetz vorgesehene Datenverwendung durch Private oder eine staatliche Behörde erfolgt.

§ 1 Abs. 2 DSG 2000 enthält nämlich durch seinen Verweis auf Art. 8 Abs. 2 EMRK einen materiellen Gesetzesvorbehalt, der allerdings nur für Grundrechtseingriffe „staatlicher Behörden“ einschlägig ist. Dieser Begriff wird im DSG 2000 nicht definiert; die Gesetzesmaterialien zum DSG 2000 führen aus,

³⁰ Elektronische Gesundheitsakte-Gesetz – ELGA-G, BGBl I 111/2012; § 15 Abs. 2 GTelG 2012.

³¹ Eberhard, § 1 DSG, in: Korinek/Holoubek (Hrsg), Österreichisches Bundesverfassungsrecht (Loseblatt, 12. Lfg. 2016) Rz 67.

dass darunter ein „*hoheitlich handelndes staatliches Organ*“ verstanden werden soll.³² Aus dieser Erläuterung folgt, dass es für das Vorliegen einer staatlichen Behörde – anders als etwa hinsichtlich der Differenzierung zwischen Datenanwendungen im privaten und jenen im öffentlichen Bereich gemäß § 5 Abs. 2, 1. Fall DSG 2000 – nicht auf organisationsrechtliche, sondern auf rein funktionale Aspekte ankommt. Unter staatlichen Behörden sind demnach zunächst jene Organe eines Rechtsträgers zu verstehen, denen allgemein die Befugnis zukommt, Hoheitsakte zu setzen. Dies sind im Bereich der Verwaltung jene Organe, die zur Erlassung von Bescheiden, VO oder zur Setzung von Akten verwaltungsbehördlicher Befehls- und Zwangsgewalt berufen sind.³³ Da die organisationsrechtliche Ausgestaltung unerheblich ist, fallen auch Hoheitsakte Privater in Form der Beleihung unter diesen Begriff.³⁴

Neben den klassischen Formen hoheitlichen Handelns wird auch die Datenverwendung im Rahmen der schlichten Hoheitsverwaltung von § 1 Abs. 2 DSG 2000 erfasst – also faktisches Verwaltungshandeln, das selbst nicht normativer Art ist und daher nicht als Rechtsakt im eigentlichen Sinn qualifiziert werden kann, das aber im Zusammenhang mit der Hoheitsverwaltung erfolgt.³⁵ Wird eine Datenverwendung nicht per Verordnung oder durch Bescheid angeordnet oder zwangsweise durchgesetzt, sondern nur faktisch vorgenommen, ist daher zu prüfen, ob diese Handlung zur Erledigung einer Materie erfolgt, die hoheitlich geprägt ist.³⁶ Ist dies zu bejahen, liegt schlichtes Hoheitshandeln vor, auf das der materielle Gesetzesvorbehalt des § 1 Abs. 2 DSG 2000 anzuwenden ist.³⁷

In diesem Zusammenhang ist maßgeblich, dass die in § 83 EIWOG angeordnete Verarbeitung (und Auslesung) der Energieverbrauchsdaten ausschließlich durch die Netzbetreiber erfolgt. Diese können nicht als hoheitlich handelnde staatliche Organe qualifiziert werden. Das Rechtsverhältnis zwischen ihnen und den KonsumentInnen ist ein zivilrechtliches und kein öffentlich-rechtliches Verhältnis. Der für staatliche Behörden maßgebliche materielle Vorbehalt des § 1 Abs. 2 DSG 2000 i.V.m. Art. 8 EMRK ist daher für die Beurteilung des § 83 EIWOG nicht einschlägig.

Für eine gesetzlich angeordnete Datenverwendung durch Private verlangt § 1 Abs. 2 DSG 2000 hingegen lediglich, dass überwiegende berechnete Interessen den Grundrechtseingriff rechtfertigen. Die Interessen des Privaten, die einen Informationseingriff rechtfertigen können, werden demnach nicht nach materiellen Gesichtspunkten bestimmt, sondern nur nach formalrechtlichen Kriterien. Akte Privater müssen daher nicht wie bei staatlichen Behörden im öffentlichen Interesse gelegen sein; es muss sich

³² EBRV 1613 BlgNR 20. GP zu § 1 DSG 2000; ähnlich *Kotschy*, Grundrechte und staatliche EDV-Register, in: Österreichische Juristenkommission (Hrsg.), Grundrechte in der Informationsgesellschaft (2001) 88 (89 [FN 2]), nach der darunter Eingriffe „*in der Ausübung staatlicher Hoheitsgewalt*“ fallen.

³³ *B. Raschauer*, Allgemeines Verwaltungsrecht⁵ (2017) Rz 136.

³⁴ *Jahnel*, Grundrecht 331; *Pürgy/Zavadil*, Die „staatliche Behörde“ im Sinne des § 1 Abs. 2 DSG 2000, in: Bauer/Reimer (Hrsg.), Handbuch Datenschutzrecht (2009) 141 (145).

³⁵ *B. Raschauer*, Allgemeines Verwaltungsrecht, Rz 699.

³⁶ VwGH 8.9.2009, 2008/17/0152.

³⁷ *Jahnel*, Grundrecht 331.

aber um „*berechtigte*“ Interessen, also um von der Rechtsordnung anerkannte Interessen handeln.³⁸ Dies setzt voraus, dass die Datenverwendung rechtlich angeordnet oder anerkannt ist, eine (verfassungs-, einfachgesetzliche oder auf vertraglicher Vereinbarung beruhende) rechtliche Basis aufweisen kann oder für die Durchsetzung von Rechtspositionen erforderlich ist.³⁹ Innerhalb dieses rechtlichen Rahmens kommen grundsätzlich sämtliche private Interessen (insbesondere auch wirtschaftliche) in Betracht.

Auch bei Grundrechtseingriffen Privater muss – im Sinne der Judikatur des EGMR zu den aus Art. 8 EMRK resultierenden positiven Schutzpflichten – zwischen den konkurrierenden Interessen ein fairer Ausgleich hergestellt werden. Daher sind Grundrechtsbeschränkungen zugunsten privater Auftraggeber ebenfalls einer Verhältnismäßigkeitsprüfung zu unterziehen. Wie im Fall von Eingriffen staatlicher Behörden in das Recht auf Datenschutz muss eine Abwägung zwischen den Interessen des Auftraggebers und jenen des Betroffenen vorgenommen werden und haben die Eingriffsinteressen gegenüber dem Geheimhaltungsanspruch zu überwiegen. Der Schutz der Interessen des einen endet dort, wo er mit einem überwiegenden berechtigten Interesse des anderen kollidiert. Dies gilt selbst für jene Fälle, in denen sich die Datenverwendung auf eine grundrechtlich geschützte Rechtsposition des Auftraggebers stützen kann.⁴⁰ Auch hier sind wiederum der Zweck der Datenverwendung einerseits und der konkrete Dateninhalt andererseits zu berücksichtigen; auf diese bezogen ist zu prüfen, ob aus objektiver Sicht das Interesse an der Verwendung der Daten als schwerwiegender einzustufen ist, als das Geheimhaltungsinteresse des Betroffenen.⁴¹

Schließlich sieht § 1 Abs. 2 letzter Satz DSG 2000 in einem dritten Schritt ausdrücklich das Gebot des gelindesten Mittels vor. Unter mehreren grundsätzlich geeigneten und erforderlichen Beschränkungen des Grundrechts auf Datenschutz ist nur jenes mit der geringsten Eingriffsintensität verfassungsrechtlich zulässig (sogenannter Grundsatz der Datensparsamkeit). Das Gebot bezieht sich sowohl auf Art. und Umfang der verarbeiteten Daten⁴² als auch auf die zeitlichen Grenzen zulässiger Datennutzungen und die Form der Datenverwendung.⁴³ Eine Datenverwendung, die dieses Übermaßverbot missachtet, stellt eine Grundrechtsverletzung dar.⁴⁴

Prüft man vor dem Hintergrund dieser Vorgaben des § 1 Abs. 2 DSG 2000 die Zulässigkeit der Datenverarbeitung mittels Smart Meter gegen den Willen des Betroffenen, so stellt sich zunächst die Frage, worin das überwiegende Interesse an der digitalen Datenverarbeitung liegen könnte. Dabei kommen zum einen die Interessen der Netzbetreiber sowie zum anderen öffentliche Interessen in Betracht.

³⁸ *Lehner*, Datenschutz, Rz 11/36.

³⁹ *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 99; OGH 27.9.2988, 4 Ob581/88.

⁴⁰ *Lehner*, Datenschutz, Rz 11/36.

⁴¹ *Ennöckl*, Privatssphäre 201.

⁴² Vgl. § 6 Abs. 1 Z 2 und 3 DSG 2000.

⁴³ Vgl. § 6 Abs. 1 Z 5 DSG 2000.

⁴⁴ VfSlg 17.065/2003.

In Bezug auf die Netzbetreiber ist zu beachten, dass diese insoweit ein Interesse an der Ermittlung der Energieverbrauchsdaten haben, als diese die Voraussetzung für die Erfüllung der vertraglichen Vereinbarungen mit den KonsumentInnen darstellen. In diesem Sinne normiert § 8 Abs. 3 Z 4 DSG 2000, dass schutzwürdige Geheimhaltungsinteressen nicht verletzt sind, wenn die Verwendung der Daten zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich ist. Aus dem Gebot der Datensparsamkeit folgt aber, dass dies nur in jenem Ausmaß erfolgen darf, das aufgrund der vertraglichen Vereinbarung unbedingt notwendig ist. Diesbezüglich wäre eine Auslesung folglich einmal pro Jahr gestattet; eine Auslesung in kürzeren Intervallen allerdings nur dann, wenn im Vertrag mit dem Stromlieferanten ein anderer Abrechnungszeitraum vertraglich vereinbart ist oder eine ausdrückliche Zustimmung vorliegt. Das Ermitteln täglicher Verbrauchswerte gegen den Willen des Betroffenen ist daher nicht nach § 8 Abs. 3 Z 4 DSG 2000 sowie nicht durch überwiegende berechtigte Interessen eines anderen gerechtfertigt.

Im Hinblick auf überwiegende öffentliche Interessen könnte geltend gemacht werden, dass der Einsatz von Smart Metern eine effiziente Energienutzung unterstützen, zu Energieeinsparungen führen und damit dem Umweltschutz dienen soll.⁴⁵ Die 2010 von PwC Österreich im Auftrag der E-Control verfasste „*Studie zur Analyse der Kosten-Nutzen einer österreichweiten Einführung von Smart Metering*“⁴⁶ prognostiziert etwa eine jährliche Energieeinsparung von ca. 0,7 TWh Strom, sollte der Smart Meter in 95 % der Haushalte bereitgestellt werden.

Dazu ist allerdings anzumerken, dass dieses (prognostizierte) Einsparungspotential vor allem daraus resultieren soll, dass *„der Kunde nun die Möglichkeit [hat], den Energieverbrauch regelmäßig (und vor allem zeitnahe) zu kontrollieren.“* Dadurch könne er *„sein Verbrauchsverhalten entsprechend anpassen. Auf Basis dieser Verhaltensänderung kann der Stromverbrauch zumindest um 3,5 % (...) reduziert werden.“*⁴⁷ Die erhoffte Energieeinsparung ergibt sich also ausschließlich daraus, dass die KonsumentInnen den Smart Meter nutzen und infolgedessen ihr Konsumverhalten anpassen.

Spricht sich ein/e KonsumentIn allerdings dezidiert gegen den Einsatz eines Smart Meters in seinem/ihrem Haushalt aus, wird diese Einsparungsmöglichkeit mit an Sicherheit grenzender Wahrscheinlichkeit nicht eintreten. Eine Person, die eine solche tägliche digitale Auslesung des Stromverbrauchs ablehnt, wird diesen weder laufend kontrollieren noch die persönliche Lebensweise anpassen. Der Einsatz intelligenter Messgeräte mag zwar insgesamt einem öffentlichen Interesse dienen; für die Datenverarbeitung gegen den Willen der Betroffenen trifft dies meines Erachtens aber nicht zu. Man wird die KonsumentInnen nicht gegen ihren Willen „zu ihrem Glück zwingen“ können. Eine solches Verständnis der Regelung des § 83 EIWOG wäre weder mit Art. 8 EMRK noch mit § 1 Abs. 1 DSG 2000 vereinbar.

⁴⁵ Pirstner-Ebner, Rechtsprobleme intelligenter Systeme, in: Storr (Hrsg.), Neue Impulse für die Energiewirtschaft (2012) 167 f.

⁴⁶ Abrufbar unter <https://www.e-control.at/documents/20903/-/-/cf11cc28-2826-4bf8-95e1-59ba8c75dac3>

⁴⁷ Seite 9 der Studie.

Zwischenergebnis

Die Bereitstellung von intelligenten Messgeräten gegen den Willen der Betroffenen wäre als Verletzung des Grundrechts auf Geheimhaltung personenbezogener Daten gemäß § 1 Abs. 1 DSG 2000 zu qualifizieren.

E. Rechtsfolgen

Das soeben dargestellte Zwischenergebnis bedeutet, dass jede/r KonsumentIn die Möglichkeit haben muss, den Einsatz eines intelligenten Stromzählers in seinem/ihrem Haushalt abzulehnen. Dies ist mit den unionsrechtlichen Vorgaben auch so lange vereinbar, als die von der Richtlinie geforderte Abdeckungsquote von 80 % nicht unterschritten wird – was aufgrund der bisherigen Erfahrungen in der Praxis ohnedies nicht zu erwarten ist.

Als problematisch erweist sich nunmehr allerdings, dass das nationale österreichische Recht (in Form der IME-VO) eine 95 %ige Abdeckungsquote mit Smart Metern verlangt. Hätte diese Regelung zur Folge, dass KonsumentInnen das gesetzlich (bedingt) eingeräumte Opt-out-Recht nicht in Anspruch nehmen können, müsste die IME-VO als datenschutzrechtswidrig qualifiziert werden. Dies vor allem vor dem Hintergrund, dass es keinerlei Regelungen gibt, die einen Rechtsrahmen vorgeben, nach welchen Kriterien die Netzbetreiber bestimmen müssten, wer seinen Grundrechtsanspruch ausüben kann und wer nicht. Ein rein zeitliches „first come, first served“-System bzw. ein Lossystem wären zweifelsohne gleichheitswidrig. Das rein zeitliche Element stellt kein sachlich gerechtfertigtes Differenzierungskriterium im Sinne des Art. 7 B-VG dar, zumal es im Ermessen der Netzbetreiber liegt, wem zuerst ein intelligentes Messgerät angeboten und damit das Opt-out-Recht ermöglicht wird.

F. Verfassungskonforme Auslegung des EIWOG sowie der IME-VO?

Zu prüfen ist daher, ob die Regelungen des EIWOG sowie die IME-VO verfassungskonform ausgelegt werden können. Dies erscheint in Bezug auf § 83 EIWOG problemlos, weil dieser das Recht der KonsumentInnen, einen Smart Meter ablehnen zu dürfen, grundsätzlich anerkennt. Die Regelung selbst enthält keine Quote, bis zu der das Opt-out-Recht in Anspruch genommen werden kann und ist folglich mit § 1 Abs. 2 DSG 2000 vereinbar.

Demgegenüber verlangt § 1 Abs. 1 Z 3 IME-VO explizit, dass bis Ende 2019 mindestens 95 % der Zählpunkte als intelligente Messgeräte im Sinne des § 7 Abs. 1 Z 3 EIWOG auszustatten sind. Liest man diese Bestimmung derart, dass in diesem Ausmaß Smart Meter vorhanden sein müssen, die den Energieverbrauch täglich ermitteln, wäre sie – wie oben dargestellt – verfassungswidrig, sobald einem einzelnen Konsumenten/einer einzelnen Konsumentin das Opt-out-Recht verweigert wird.

Zu beachten sind in diesem Zusammenhang die „Sonstigen Marktregeln Strom“ der E-Control gemäß § 22 1 Z 1 E-ControlG. Diese sehen den Begriff des *Digitalen Standardzählers (DSZ)* vor. Dabei handelt es sich um „ein elektronisches Messgerät, das keine Viertelstundenwerte speichert und über keine Abschaltfunktion bzw. Leistungsbegrenzungsfunktion verfügt und daher kein intelligentes Messgerät ist. Eine regelmäßige Auslesung und Übertragung des monatlichen Zählerstandes ist möglich. Darüber hinaus ist für Verbrauchsabgrenzungen eine Übermittlung des Zählerstandes vorzusehen, wobei der Netzbetreiber rechtzeitig davon in Kenntnis zu setzen ist.“ Anders formuliert: **Der Digitale**

Standardzähler ist ein intelligentes Messgerät, bei dem aber datenschutzrechtlich problematische Funktionen (insbesondere auf Wunsch der KonsumentInnen) deaktiviert sind. Ihr Einsatz ist daher grundsätzlich mit dem DSG 2000 vereinbar. Festzuhalten ist allerdings, dass eine Übertragung des monatlichen Zählerstandes im Falle des Opt-outs des Kunden/der Kundin – ohne ausdrückliche Zustimmung durch den Kunden/die Kundin – nicht mit dem DSG 2000 vereinbar ist. In diesem Punkt müssen die „Sonstigen Marktregeln Strom“ der E-Control, die den „Digitalen Standardzähler“ definieren, meines Erachtens geändert werden, um mit dem DSG 2000 vereinbar zu sein. Zu beachten ist dabei, dass eine allfällige (unzulässige) Übertragung des monatlichen Zählerstandes (ungeachtet der Regelungen der „Sonstigen Marktregeln Strom“ der E-Control) dem Netzbetreiber zuzurechnen ist und dieser dafür gerichtlich verantwortlich gemacht werden kann (siehe unten Kapitel G.)

Es stellt sich daher die Frage, ob intelligente Messgeräte, die derart deaktiviert werden, dass sie aus datenschutzrechtlicher Sicht als (grundrechtskonformer) digitaler Standardzähler anzusehen sind, in die 95 %ige Quote des § 1 Abs. 1 Z 3 IME-VO eingerechnet werden können.

Dies ist meines Erachtens zu bejahen: Die technischen Anforderungen, die ein *intelligentes Messgerät* im Sinne des § 7 Abs. 1 Z 31 EIWOG erfüllen muss, werden nämlich in der IMA-VO 2011 – konkret in § 3 der VO – festgelegt. Dort wird aber keineswegs verlangt, dass die Geräte tatsächlich zeitnahe die Energieverbrauchswerte messen, sondern nur, dass dies mit einem solchen Gerät „möglich ist“. Die Kriterien des § 3 IMA-VO sind nahezu alle derart formuliert, dass die *Möglichkeit* bestehen muss, eine bestimmte Funktion zu nutzen. Dies ist aber auch bei der Bereitstellung von Digitalen Standardzählern der Fall; auch solche Geräte sind grundsätzlich in der Lage, die Funktionen eines intelligenten Messgerätes zu erfüllen, weil diese kurzfristig reaktiviert werden können. Es spricht infolge der Formulierung des § 3 IMA-VO 2011 daher aus meiner Sicht nichts dagegen, Digitale Standardzähler in die 95 %ige Quote der IME-VO miteinzuberechnen und so § 83 EIWOG verfassungskonform auszulegen.

Als Alternative zu dieser Vorgehensweise käme eine Novelle des EIWOG (konkret der Formulierung der Regelung des § 83 Abs. 1) in Betracht. Es müsste diesfalls die Wendung „Im Rahmen der durch die Verordnung bestimmten Vorgaben für die Installation intelligenter Messgeräte“ aus dem Gesetzestext gestrichen werden. Die Bestimmung müsste dann wie folgt lauten:

§ 83 (1) Der Bundesminister für Wirtschaft, Familie und Jugend kann nach Durchführung einer Kosten/Nutzanalyse die Einführung intelligenter Messeinrichtungen festlegen. Dies hat nach Anhörung der Regulierungsbehörde und der Vertreter des Konsumentenschutzes durch Verordnung zu erfolgen. Die Netzbetreiber sind im Fall der Erlassung dieser Verordnung zu verpflichten, jene Endverbraucher, deren Verbrauch nicht über einen Lastprofilzähler erfasst wird, mit intelligenten Messgeräten auszustatten, über die Einführung, insbesondere auch über die Kostensituation, die Netzsituation, Datenschutz und Datensicherheit und Verbrauchsentwicklung bei den Endverbrauchern, Bericht zu erstatten und die Endverbraucher zeitnah über den Einbau eines intelligenten Messgeräts sowie die damit verbundenen Rahmenbedingungen zu informieren. ~~Im Rahmen der durch die Verordnung~~

~~bestimmten Vorgaben für die Installation intelligenter Messgeräte hat~~ Der Netzbetreiber hat den Wunsch eines Endverbrauchers, kein intelligentes Messgerät zu erhalten, zu berücksichtigen. Die Regulierungsbehörde hat die Aufgabe, die Endverbraucher über allgemeine Aspekte der Einführung von intelligenten Messgeräten zu informieren und über die Einführung von intelligenten Messgeräten, insbesondere auch über die Kostensituation, die Netzsituation, Datenschutz und Datensicherheit, soweit bekannt, den Stand der Entwicklungen auf europäischer Ebene und über die Verbrauchsentwicklung bei den Endverbrauchern, jährlich einen Bericht zu erstatten.

Darüber hinaus wäre eine Änderung der Legaldefinition des § 7 Abs. 1 Z 31 EIWOG anzudenken. Die Bestimmung sollte wie folgt lauten:

„intelligentes Messgerät“ eine technische Einrichtung die den tatsächlichen Energieverbrauch und Nutzungszeitraum zeitnah messen kann, und die über eine fernauslesbare, bidirektionale Datenübertragung verfügt;

G. Datenermittlung trotz Opt-out

Macht ein/e KonsumentIn von ihrem Recht, den Einsatz eines intelligenten Messgerätes abzulehnen, Gebrauch und werden vom Netzbetreiber dennoch Daten über den im Vertrag vereinbarten Abrechnungsintervall hinaus abgelesen und übermittelt, so ist das als eine rechtswidrige Datenverwendung anzusehen. Das bedeutet, dass im Falle der Deaktivierung der Funktionen eines intelligenten Stromzählers infolge des Opt-outs des Betroffenen eine Ablesung und Übertragung des Zählerstandes nur noch einmal pro Jahr erfolgen darf, es sei denn es wurde im Vertrag mit dem/der Kunden/Kundin ausdrücklich ein anderes Abrechnungsintervall vereinbart. Eine monatliche Datenübertragung mittels digitalen Standardzählers ist im Fall einer vertraglich vereinbarten einjährigen Verrechnungsperiode nicht mit dem DSG 2000 vereinbar. In diesem Punkt entsprechen die „*Sonstigen Marktregeln Strom*“ der E-Control nicht den Vorgaben des DSG 2000.

Eine solche Datenschutzverletzung fällt allerdings (nach der derzeit geltenden Rechtslage) weder unter die in § 51 DSG 2000 normierte gerichtliche Strafbestimmung noch unter die Verwaltungsstrafbestimmung des § 52 DSG 2000.

Eine Rechtsschutzmöglichkeit, die den Betroffenen offensteht, wäre daher die Anrufung der ordentlichen Gerichte. Ansprüche wegen der Verletzung der Rechte auf Geheimhaltung durch Auftraggeber im privaten Bereich sind vom Betroffenen nach § 32 1 DSG 2000 auf dem Zivilrechtsweg geltend zu machen. Er kann gegen die DSG-widrige Verwendung von Daten zu seiner Person den Anspruch auf Unterlassung geltend machen. Dieser Anspruch besteht unabhängig vom Verschulden des Auftraggebers. Eine Unterlassungsklage setzt allerdings eine konkrete und akute Gefährdung durch den Beklagten oder – nach bereits erfolgter Rechtsverletzung – eine Wiederholungsgefahr voraus.

Für derartige Klagen sowie für Anträge auf Erlassung einer einstweiligen Verfügung ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Kläger – also der mutmaßliche Betroffene – seinen gewöhnlichen Aufenthalt oder Sitz hat. Alternativ dazu können Klagen und Anträge bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte – also die vom Kläger als Auftraggeber belangte Person – seinen gewöhnlichen Aufenthalt oder Sitz oder eine Niederlassung hat. Örtliche Zuständigkeitsvereinbarungen nach § 104 JN sind zulässig. Im Verfahren vor den Landesgerichten besteht absolute Anwaltpflicht. Eine **derartige Klage wäre daher mit einem nicht unerheblichen Kostenrisiko verbunden.**

Alternativ dazu käme das sog „Ombudsmann-Verfahren“ gemäß § 30 DSG 2000 in Betracht. Nach dieser Bestimmung kann sich jedermann wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten eines Auftraggebers oder Dienstleisters nach dem DSG 2000 mit einer Eingabe an die Datenschutzbehörde wenden. Geltend gemacht werden kann somit die Verletzung datenschutzrechtlicher Rechte oder Pflichten in Bezug auf eigene Daten durch den Betroffenen. Wird behauptet, dass ein Auftraggeber Daten über eine andere Person rechtswidrig verwendet, so ist dies als Aufforderung zur amtswegigen Prüfung durch die DSB zu verstehen. In diesem Fall besteht aber kein Anspruch auf Mitteilung, wie mit der Eingabe verfahren wurde.

Eine solche Eingabe an die DSB kann sich auch gegen eine Datenanwendung im privaten Bereich richten. In diesem Fall erlangt der Betroffene im Wege dieses Kontrollverfahrens jedoch keine rechtsverbindliche Entscheidung, sondern bewirkt allenfalls die Einleitung einer amtswegigen Überprüfung nach § 30 Abs. 4 DSG 2000 sowie eine Empfehlung der DSB. Er hat lediglich Anspruch darauf, darüber informiert zu werden, wie mit seiner Eingabe verfahren wurde. In Bezug auf Datenanwendungen im privaten Bereich hat die Eingabe nach § 30 DSG 2000 aus Sicht des Betroffenen gegenüber einer Klage aber den wesentlichen Vorteil, dass im Verfahren vor der DSB weder ein Anwaltszwang noch eine Kostenersatzpflicht im Fall des prozessualen Unterliegens bestehen. Der Rechtsbehelf kann daher ohne Kostenrisiko in Anspruch genommen werden.

Als Alternative zur Anrufung der Datenschutzbehörde steht darüber hinaus der Gang zur Streitschlichtungsstelle der E-Control offen. Auch dieses Verfahren hat für den Konsumenten/die Konsumentin den Vorteil, dass es für den Beschwerdeführer/die Beschwerdeführerin kostenlos ist. Die Schlichtungsstelle kann allerdings keine Entscheidung treffen, die zwingend vom belangten Unternehmen umzusetzen ist. Sie kann lediglich Lösungsvorschläge erarbeiten. Den Parteien steht es aber immer frei, ob sie diesem Lösungsvorschlag zuzustimmen wollen oder nicht.

H. Abschließende Anmerkungen zum Inkrafttreten der DSGVO im Jahr 2018

Das vorliegende Gutachten kommt zum Ergebnis, dass die Bereitstellung von intelligenten Messgeräten gegen den Willen der Betroffenen als Verletzung des Grundrechts auf Geheimhaltung personenbezogener Daten gemäß § 1 Abs. 1 DSG 2000 zu qualifizieren wäre.

Der einfachgesetzliche Teil des österreichischen Datenschutzgesetzes (Art. 2 DSG 2000) wird allerdings mit dem Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018 teilweise außer Kraft treten. Der Nationalrat hat daher jüngst (nämlich am 29. Juni 2017) das Datenschutz-Anpassungsgesetz 2018 beschlossen. Dieses wird (vorbehaltlich der Zustimmung des Bundesrates und der Kundmachung im BGBl) am 25. Mai 2018 in Kraft treten und an die Stelle des bisherigen Art. 2 des DSG 2000 (§§ 4 bis 64 DSG 2000) treten.

Von dieser Änderung bleibt der in Verfassungsrang stehende Teil des DSG 2000 (Art. 1 DSG 2000) allerdings unberührt. Das Grundrecht auf Datenschutz (§ 1 DSG 2000) wird daher keinerlei Veränderung erfahren, sondern in der bisher geltenden Fassung – auf die sich die vorliegende Studie stützt – vollinhaltlich weiter gelten. Insoweit wird die in der Studie getroffene Aussage, wonach sich aus § 1 DSG 2000 ergibt, dass jede/r KonsumentIn die Möglichkeit haben muss, den Einsatz eines intelligenten Stromzählers in seinem/ihrem Haushalt abzulehnen, auch nach dem 25. Mai 2018 weiterhin volle Gültigkeit haben.

Darüber hinaus ist festzuhalten, dass die Auslegung, wonach eine Bereitstellung von intelligenten Messgeräten gegen den Willen der Betroffenen normiert werden kann, nicht nur § 1 Abs. 1 DSG 2000, sondern auch Art. 8 EGRC verletzen würde. Der Eingriffsvorbehalt dieser beiden Grundrechtsnormen ist nämlich weitgehend deckungsgleich.⁴⁸ Der österreichische Gesetzgeber ist bei der Umsetzung der EU-Elektrizitätsbinnenmarkt-RL im Sinne einer doppelten Bindung⁴⁹ nämlich sowohl an das österreichische Verfassungsrecht (einschließlich des § 1 DSG 2000) als auch an die EGRC gebunden.

III. Zusammenfassung der wesentlichen Ergebnisse

- Die Informationen über den Energieverbrauch in einem bestimmten Haushalt sind personenbezogene Daten im Sinne des § 4 Z 1 DSG 2000.
- **Bereits das Aufzeichnen und Speichern des Stromverbrauchs eines Haushaltes stellt einen rechtfertigungsbedürftigen Eingriff in das Grundrecht auf Geheimhaltung personenbezogener Daten gemäß § 1 DSG 2000 dar, selbst wenn die Daten nicht laufend an den Netzbetreiber übermittelt, sondern lediglich (als Monatsverbrauchswert) „vor Ort“ im Messgerät gespeichert werden.**
- Da sich der Grundrechtseingriff durch den Gesetzgeber nicht auf lebenswichtige Interessen oder die Zustimmung des Betroffenen stützen kann, ist er nur gerechtfertigt, wenn er in Wahrung überwiegender Interessen anderer erfolgt.

⁴⁸ Vgl. *Ennöckl*, Der Schutz der Privatsphäre, 267 ff.

⁴⁹ Vgl. *Öhlinger/Eberhard*, Verfassungsrecht¹¹ (2016) Rz 200.

- Die Bereitstellung von intelligenten Messgeräten gegen den Willen der Betroffenen wäre als Verletzung des Grundrechts auf Geheimhaltung personenbezogener Daten gemäß § 1 Abs. 1 DSG 2000 zu qualifizieren. Daher muss jede/r KonsumentIn die Möglichkeit haben, den Einsatz eines intelligenten Stromzählers in seinem/ihrem Haushalt abzulehnen.
- Eine verfassungskonforme Auslegung des EIWOG und der IME-VO gebieten es, intelligente Messgeräte, die derart deaktiviert werden, dass sie aus datenschutzrechtlicher Sicht als (grundrechtskonformer) DSZ anzusehen sind, in die 95 %ige Quote des § 1 Abs. 1 Z 3 IME-VO einzurechnen.
- Andernfalls müssten die Regelungen des § 83 Abs. 1 sowie des § 7 Abs. 1 Z 31 EIWOG novelliert werden.
- Macht ein/e KonsumentIn von ihrem Recht, den Einsatz eines intelligenten Messgerätes abzulehnen Gebrauch und werden vom Netzbetreiber dennoch Daten über den im Vertrag vereinbarten Abrechnungsintervall hinaus abgelesen und übermittelt, so ist das als eine rechtswidrige Datenverwendung anzusehen. Eine monatliche Datenübertragung mittels digitalen Standardzählers ist im Fall einer vertraglich vereinbarten einjährigen Verrechnungsperiode nicht mit dem DSG 2000 vereinbar. In diesem Punkt müssen die „Sonstigen Marktregeln Strom“ der E-Control meines Erachtens geändert werden, um den Vorgaben des DSG 2000 zu entsprechen.
- Dagegen kann mit zivilrechtlicher Unterlassungsklage oder mit einer Eingabe gemäß § 323230 DSG 2000 an die Datenschutzbehörde vorgegangen werden. Darüber hinaus steht der Gang zur Streitschlichtungsstelle der E-Control offen.
- Die in dieser Studie getroffenen Aussagen werden auch nach dem Inkrafttreten der DSGVO am 25.05.2018 weiterhin volle Gültigkeit haben.

Wien, Juli 2017

Gesellschaftskritische Wissenschaft: die Studien der AK Wien

Alle Studien zum Downloaden:

wien.arbeiterkammer.at/service/studien

