Datenschutz im Crowd-Energy-Umfeld

Datensicherheit | Die fortschreitende Dezentralisierung der Energieproduktion fördert neuartige Konstrukte wie Eigenverbrauchsgemeinschaften, welche sich quasi autonom versorgen. Wie sind solche Gemeinschaften rechtlich zu behandeln, und welche Leitlinien müssen ihnen auferlegt werden? Ein Ansatz.

TEXT MICHÈLE BALTHASAR

Die zunehmende Dezentralisierung der Stromproduktion, die grösseren Speichermöglichkeiten sowie die damit einhergehende Entwicklung von intelligenten Netzen und intelligenten Messsystemen ermöglichen neue Kooperationskonzepte, wie etwa das vom Internationalen Institut für Management und Technologie der Universität Fribourg entwickelte Crowd-Energy-Konzept **(vgl. Kasten)**.

Anwendungsfall eines solchen Konzeptes, beziehungsweise dessen Grundelement, die iGSL-Zelle, sind Eigenverbrauchsgemeinschaften (EVG). Zur technischen Umsetzung von EVGs werden eine oder mehrere Stromerzeugungsanlagen, eventuell ein Batteriespeicher, intelligente Messsysteme und gegebenenfalls Wärmepumpen und weitere Elemente der Gebäudetechnik eingesetzt. Intelligente Überwachungs-, Visualisierungs- und Regelungsanwendungen (Software oder Apps) verbinden die Komponenten und unterstützen die Bewirtschaftung.

Mit dem ersten Massnahmenpaket der Energiestrategie 2050, welches am 1. Januar 2018 in Kraft tritt, werden EVGs in der Schweiz gefördert und umfassend gesetzlich geregelt. Gemäss Art. 15 des Entwurfs der Energieverordnung vom 1. November 2017 (E-EnV) ist der Zusammenschluss zum Eigenverbrauch zulässig, sofern die Produktionsleistung der Anlage bei mindestens 10 % der maximalen Netzanschlusskapazität liegt.[1)] EVGs können am geöffneten Markt teilnehmen, sofern der jährliche Stromverbrauch der EVG die Schwelle von 100 MWh übersteigt.

Datenschutz und -sicherheit spielen eine zentrale Rolle

EVGs verlangen nach einer Vielzahl von Daten (zum Beispiel Abrechnungsdaten oder Prognosedaten).

Bild: Elastic Compute Farm/pixabay

Diese werden mittels Informations- und Kommunikationstechnologie (IKT) aufgezeichnet, ausgetauscht und verknüpft.

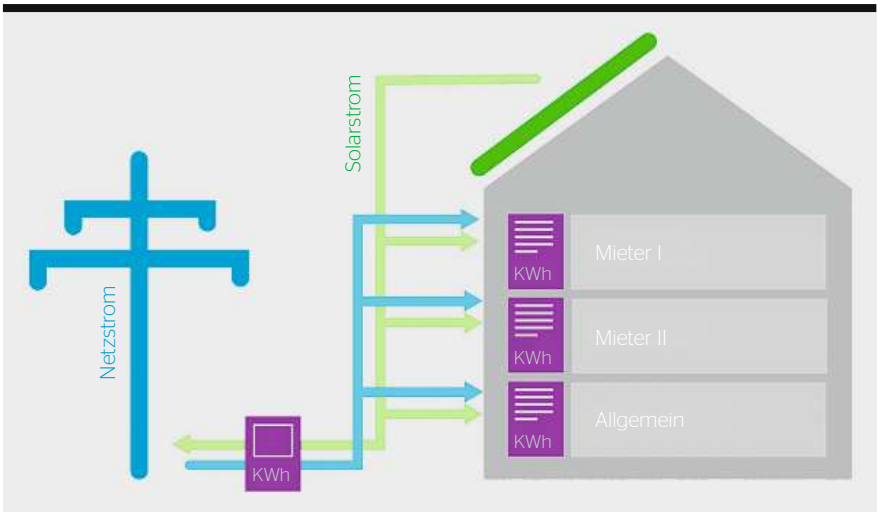
Durch die vermehrten Schnittstellen im Netz steigen allerdings die Verletzlichkeit und Verwundbarkeit sowie die Gefahr, durch gezielte Angriffe geschädigt zu werden. Aufgrund beispielsweise einer Distributed-Denial-of-Service-Attacke oder einer Infektion mit Malware könnte die Kontrolle über die EVG verloren gehen und zu einem lokalen Blackout führen. Aus den gesammelten Prosumer-Daten können aber auch Informationen über das Nutzerverhalten der Mitglieder einer EVG abgeleitet werden, was die EVG zu einer Quelle für zahlreiche Risiken wie etwa Betrug oder Einbrüche macht. Der Schutz und die Sicherheit von Daten spielt deshalb eine zentrale Rolle für EVGs.

Sinn und Zweck einer Leitlinie

Für Privatpersonen und Gewerbebetriebe sind EVGs eine Herausforderung. Sie verfügen kaum über Kompetenzen, um sich vor den genannten Risiken zu schützen. EVGs sollten deshalb, analog zu einer Datenschutz- und Datensicherheitsrichtlinie für Unternehmen, operationelle Regeln zum Schutz und zur Sicherheit von Daten einführen, an die sich alle halten müssen und die sie gegebenenfalls wieder abändern können. Ziel einer Leitlinie ist, die Privatsphäre von Personen zu schützen und Persönlichkeitsverletzungen zu verhindern beziehungsweise abzuwehren sowie die sich aus den Gesetzen ergebenden Rechte der Betroffenen zu wahren.

Rechtsgrundlagen

Hinsichtlich der anwendbaren Rechtsgrundlagen ist zwischen Daten, die einen Personenbezug haben (zum Beispiel Abrechnungs- oder Messdaten), und solchen, die in der Regel keinen Personenbezug aufweisen (zum Beispiel Prognosedaten oder Ein-/Ausspeisedaten), zu unterscheiden. Für Personendaten gelten die Datenschutzgesetzgebungen. Für Daten, die keinen Personenbezug aufweisen, ist die Datenschutzgesetzgebung nicht anwendbar, sondern es kommen allgemeine nationale und internationale Empfehlungen sowie Branchenstandards zur Anwendung. [1, 2, 3]



Ein Beispiel, wie eine EVG aufgebaut ist.

Regelungen zum Schutz personenbezogener Daten und zur Datensicherheit in der Schweiz finden sich im Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG) [4] sowie in der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG) [5]. Das DSG bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen und juristischen Personen, deren Daten bearbeitet werden.

Auf europäischer Ebene gilt ab 25. Mai 2018 die EU-Datenschutz-Grundverordnung vom 27. April 2016 (DSGVO) [6] unmittelbar in allen EU-Mitgliedstaaten. Mit der DSGVO soll einerseits der Schutz von personenbezogenen Daten innerhalb der Europäischen Union sichergestellt und anderseits der freie Datenverkehr innerhalb des europäischen Binnenmarktes gewährleistet werden. Neu können bei Verstössen gegen die DSGVO Geldbussen von bis zu 20 Mio. € oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden. Aufgrund des «Marktortprinzips» ist die DSGVO unter Umständen auch für EVGs in der Schweiz anwendbar.[2)]

Am 15. September 2017 hat der Bundesrat die Botschaft zu einer Totalrevision des Datenschutzgesetzes verabschiedet.[3)] Diese beabsichtigt, sich den Anforderungen der DSGVO anzunähern. Auch in der Schweiz werden deshalb die strafrechtlichen Sanktionen ausgebaut mit möglichen Bussen bis zu 250 000 CHF bei Verletzung der Aus-

Crowd Energy

Voraussetzung und Funktion

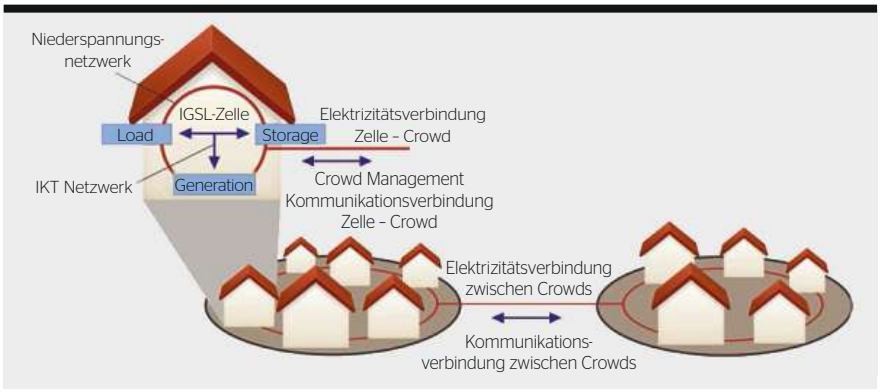
In einer Crowd Energy bündeln die Individuen und Organisationen ihre Energieressourcen mittels Informations- und Kommunikationstechnologie. Grundelement einer Crowd Energy bildet eine iGSL-Zelle. Dabei stehen «i» für «intelligent», «G» für «Generation» (Erzeugung), «S» für «Storage» (Speicherung) und «L» für «Load» (Last beziehungsweise Bedarf). In einer iGSL-Zelle wird Strom erzeugt, gespeichert und verbraucht. Sie ist die kleinste Einheit in einer Crowd und kann zum Beispiel ein Gebäude sein.

Crowd Energy entsteht, wenn mindestens zwei iGSL-Zellen mittels Informations- und Kommunikationstechnologie miteinander kooperieren, indem sie Informationen und Strom austauschen. Überschüssiger Strom wird anderen iGSL-Zellen, dem lokalen Energieversorger oder einem anderen Energielieferanten zur Verfügung gestellt. Stromdefizite werden von anderen iGSL-Zellen, anderen Energielieferanten oder dem lokalen EVU ausgeglichen.

Das Ziel einer Crowd ist die Etablierung eines komplett dezentralen Energiesystems, in dem Prosumer auf Basis vordefinierter Verträge und ohne Intermediäre automatisiert Energielieferungen untereinander ausführen. [9]

Bild: CKW

Auch Eigenverbrauchsgemeinschaften müssen dem Datenschutz und der Datensicherheit Rechnung tragen.



Schema einer Crowd Energy.

kunfts-, Melde- und Mitwirkungspflichten. Das revidierte Datenschutzgesetz (E-DSG) wird voraussichtlich im Laufe des Jahres 2019 in Kraft treten.

Neben diesen allgemeinen datenschutzrechtlichen Gesetzgebungen treten mit der Umsetzung der Energiestrategie 2050 auch spezialgesetzliche Regelungen zum Datenschutz und zur Datensicherheit in Kraft. So sieht etwa Art. 17 Abs. 4 des Entwurfs des Stromversorgungsgesetzes vom 1. September 2016 (E-StromVG) vor, dass beim Erlass von Vorschriften zum Betrieb intelligenter Messsysteme beim Endverbraucher in besonderem Masse auf deren Vereinbarkeit mit den Bestimmungen über den Datenschutz zu achten ist. Nach Art. 8d Abs. 5 des Entwurfs der Stromversorgungsverordnung vom 1. November 2017 (E-StromVV) gewährleistet der Netzbetreiber die Datensicherheit von Mess-, Steuer- und Regelsystemen und beachtet dabei insbesondere die Art. 8–10 VDSG sowie allfällige internationale Normen und Empfehlungen anerkannter Fachorganisationen.

Weitere Vorschriften im Zusammenhang mit der Verwendung der aus intelligenten Messsystemen gewonnenen Daten sind in Art. 8c und d E-StromVV enthalten. Diese lassen die Erhebung und die Bearbeitung der im Minimum notwendigen Daten in der entsprechenden Auflösung und Periodizität durch die Netzbetreiber grundsätzlich zu. Eine automatische Weitergabe dieser detaillierten Informationen ist jedoch ausgeschlossen. [7]

In Anbetracht der voraussichtlichen Entwicklungen der Gesetzgebung ist es sinnvoll, beim Erlass einer Leitlinie zum Datenschutz und zur Datensicherheit die zukünftigen gesetzlichen Entwicklungen bereits miteinzubeziehen. Für EVGs relevant ist vor allem die Datenschutzgesetzgebung. Die nachfolgenden Grundsätze einer Leitlinie richten sich deshalb nach dem E-DSG.

Wesentlicher Regelungsgehalt einer Leitlinie nach E-DSG

Gegenstand der Leitlinie ist der Schutz von Personendaten bei deren Bearbeitung innerhalb der EVG. Unter den Begriff «Personendaten» fallen alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Als Bearbeiten gilt jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.

Der **Geltungsbereich** der Leitlinie erstreckt sich über alle Akteure einer EVG, die Personendaten bearbeiten («Auftragsbearbeiter») und über die Personendaten bearbeitet werden («betroffene Personen»). Die einzelnen Vorgaben der Leitlinie müssen entsprechend der Rolle des betreffenden Akteurs ausgelegt und umgesetzt werden. Bearbeiter von Personendaten

Bilder: ulleo/pixabay | iimt

sind in erster Linie Provider von IT Services und Netzbetreiber. An diese richtet sich daher die Leitlinie vorrangig. Prosumer und Verbraucher dürften sich wenig mit der Bearbeitung von Personendaten befassen. Vielmehr werden deren eigene Daten bearbeitet. Ihnen dient die Leitlinie vor allem als effektives Instrumentarium, um Persönlichkeitsverletzungen zu verhindern, beziehungsweise abzuwehren sowie die sich aus dem Gesetz ergebenden Rechte geltend zu machen.

Die **Datenarten/-kategorien** der Leitlinie sind insbesondere folgende: Personenstammdaten, Kommunikationsdaten (zum Beispiel Telefon, E-Mail), Mess- und Abrechnungsdaten, Auskunftsangaben von Dritten (zum Beispiel aus öffentlichen Verzeichnissen).

Die Leitlinie regelt auch die **Organisation** der Mitglieder einer EVG (insbesondere Prosumer und Verbraucher). Diese dürften in der Regel eine «einfache Gesellschaft» im Sinne von Art. 530 ff. des Schweizerischen Obligationenrechts bilden. [8] Im Aussenverhältnis ist deshalb die einfache Gesellschaft als «Verantwortliche» zu qualifizieren. Sie vertritt die EVG gegen aussen und entscheidet über den Zweck, die Mittel und den Umfang der Bearbeitung von Personendaten. Im Innenverhältnis ist jedes Mitglied für seine Personendaten in IT-Systemen, Applikationen und Komponenten etc., für die rechtmässige Bearbeitung der Daten und die Einhaltung der Datenschutz- und Datensicherheitsvorgaben verantwortlich.

Es ist vor allem bei grossen EVGs zu empfehlen, einen Datenschutzbeauftragten zu benennen, der die Einhaltung der datenschutzrechtlichen Vorgaben überwacht und als Ansprechstelle für alle Fragestellungen im Zusammenhang mit dem Datenschutz gilt. Ein weiterer Vorteil der Benennung eines Datenschutzbeauftragten liegt darin, dass auf eine vorgängige Stellungnahme des eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten verzichtet werden kann, sofern eine Datenschutz-Folgenabschätzung zu erstellen ist.

Verzeichnis der Bearbeitungstätigkeiten: Die Verantwortliche der EVG, die einfache Gesellschaft, und die Auftragsbearbeiter (insbesondere Netzbetreiber und Service-Provider) führen ein Verzeichnis ihrer Bearbeitungstätigkeiten.[4)]

Bei der Bearbeitung der Personendaten sind folgende **Bearbeitungsgrundsätze** einzuhalten: Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, Zweckbindung, Transparenz, Richtigkeit und Datensicherheit.

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen: Die Datenbearbeitung ist bei der Planung der EVG technisch und organisatorisch so auszugestalten, dass die gesetzlichen und regulatorischen Datenschutzvorschriften eingehalten werden. Zudem müssen die technischen und organisatorischen Massnahmen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Persönlichkeit und die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein. Die EVG als Verantwortliche ist verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.

Bearbeitung durch Auftragsbearbeiter: Die Bearbeitung von Personendaten kann vertraglich oder durch Gesetzgebung – beispielsweise im Rahmen eines Outsourcings – einem Auftragsbearbeiter (zum Beispiel einem Cloud-Anbieter) übertragen werden, wenn die Daten so bearbeitet werden, wie die Verantwortliche es selbst tun dürfte, und keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. Dabei muss sich die EVG als Verantwortliche vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

Bekanntgabe von Personendaten ins Ausland: Personendaten dürfen ins Ausland bekannt gegeben werden,

RÉSUMÉ

Protection et sécurité des données dans l'environnement de Crowd Energy

Une ligne directrice pour les communautés d'autoconsommateurs

La décentralisation croissante de la production d'électricité, les plus grandes possibilités de stockage, ainsi que le développement des réseaux et systèmes de mesure intelligents qui vont avec permettent de nouveaux concepts de coopération, tels que celui de Crowd Energy.

Les communautés d'autoconsommateurs (CA) sont un exemple d'application de ce concept. Pour la mise en œuvre technique des CA, on a recours à une ou plusieurs installations de production de courant électrique, éventuellement à une batterie, à des systèmes de mesure intelligents et, le cas échéant, à des pompes à chaleur et à d'autres éléments de la technique du bâtiment. Des applications intelligentes de surveillance, de visualisation et de régulation (logiciels ou applications) connectent les composants et soutiennent la gestion.

Les CA nécessitent une multitude de données (par exemple des données de décompte ou de prévisions). Celles-ci sont enregistrées, échangées et reliées au moyen des technologies de l'information et de la communication. Toutefois, étant donné le nombre accru d'interfaces dans le réseau, la vulnérabilité augmente, de même que le risque d'être lésé par des attaques ciblées. Cependant les données collectées auprès des prosommateurs peuvent également fournir, par déduction, des informations sur le comportement d'utilisateur des membres de la CA, ce qui fait de cette dernière la source de nombreux risques, tels que la fraude ou des effractions. La protection et la sécurité des données joue par conséquent un rôle central pour les CA. Grâce à une directive contraignante qui comprend des règles opérationnelles pour la protection et la sécurité des données, il est possible de protéger la sphère privée des personnes impliquées. MR

wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet. Dies ist bei einer Datenbearbeitung in EU-Mitgliedstaaten regelmässig der Fall, nicht so jedoch bei Drittstaaten. Hier ist die Angemessenheit im Einzelfall zu prüfen. Werden Personendaten an EU-Mitgliedstaaten übermittelt, ist zudem die Anwendbarkeit der DSGVO zu prüfen und gegebenenfalls DSGVO-konform zu handeln.

Die Verantwortliche und die Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene **Datensicherheit**. Diese Massnahmen sollen sicherstellen, dass Verletzungen der Datensicherheit vermieden werden. In Frage kommen hierbei insbesondere Zugriffs- und Zugangskontrollen. Beispielsweise müssen der Zugang zu den peripheren Geräten oder Einrichtungen, wie etwa den intelligenten Messgeräten, und der Zugriff auf die gespeicherten Daten angemessen geschützt werden. Auch Transportkontrollen können nötig sein. Bei der Übermittlung sowie beim Transport von Datenträgern, die Personendaten enthalten, sind entsprechende Schutzmassnahmen (beispielsweise Verschlüsselung) anzuwenden. Insbesondere soll verhindert werden, dass die Personendaten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Auch Bekanntgabekontrollen (Datenempfänger, denen Personendaten auf elektronischem Weg [zum Beispiel via E-Mail] bekannt gegeben werden, sind vorgängig zu identifizieren), Speicherkontrollen (die Einsichtnahme, Veränderung, Eingabe oder Löschung von Personendaten durch Unbefugte ist zu verhindern) und Benutzerkontrollen (die vorgegebenen Massnahmen und Kontrollen zum Schutz vor unberechtigter Benutzung von IT-Systemen sind zu befolgen) müssen hier berücksichtigt werden.

Die Massnahmen sind auch angemessen auf das Schutzziel der Verfügbarkeit auszurichten. Dies, weil es bei der EVG um die gesicherte Versorgung mit elektrischer Energie während 24 Stunden pro Tag, 7 Tagen pro Woche und 365 Tagen im Jahr geht. Systemausfälle sollen keinen oder maximal einen beschränkten Lieferunterbruch zur Folge haben.

Datenschutz-Folgenabschätzung: Werden die Personendaten über einen längeren Zeitraum erhoben, wie dies etwa bei den Messdaten der Fall sein dürfte, kann damit auch Profiling betrieben werden. Profiling ist die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten, insbesondere, um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen. Die typischerweise zu erstellenden Verbraucherprofile dürften als Profiling qualifiziert werden. Sie bringen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich. Es ist deshalb in solchen Fällen eine Datenschutz-Folgenabschätzung zu erstellen. Diese umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit der betroffenen Person zu verringern.

Auskunftsgesuche, Recht auf Berichtigung und Löschung: Jede betroffene Person kann schriftlich Auskunft darüber verlangen, ob und, wenn ja, welche Personendaten über sie bearbeitet werden. Der betroffenen Person steht unter Beachtung des Verhältnismässigkeitsgrundsatzes zudem das Recht auf Berichtigung, Sperrung und Löschung ihrer Personendaten zu.

Eine Datenschutzweisung muss «gelebt» werden

Abschliessend ist anzufügen, dass mit der Einführung einer Datenschutzweisung die Grundlagen zum Schutz der Privatsphäre und der Verhinderung von Persönlichkeitsverletzungen zwar gelegt sind. Ein effektiver Schutz ist allerdings nur gegeben, wenn eine solche Datenschutzweisung auch «gelebt» wird, das heisst, die darin enthaltenen Grundsätze in der jeweiligen EVG auch konkret umgesetzt werden. Nur so kann sich diese effektiv vor den Risiken schützen, die aufgrund vermehrter Schnittstellen im Netz auf sie zukommen. Gleiches gilt im Übrigen auch für die ebenfalls noch zu erlassende Leitlinie zum Schutz von Daten, die keinen Personenbezug aufweisen und die sich auf Empfehlungen und Branchenstandards stützt.

Referenzen

[1] Smart Grid Roadmap (abrufbar unter bfe.admin.ch/smartgrids), BFE, 2015.
[2] Smart Grid Architecture Model (abrufbar unter gridscientific.com/images/Smart_Grid_Reference_Architechture.pdf), Smart Grid Coordination Group, 2012.
[3] CEN/CLC/ETSI/TR 50572, Smart Grid Coordination Group, 2011.
[4] SR 235.1.
[5] SR 235.11.
[6] 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).
[7] vgl. auch «Erläuternder Bericht zur E-StromVV», S. 7 ff, Februar 2017.
[8] SR 220.
[9] Stephanie Teufel, Yves Hertig, Mario Gstrein und Bernd Teufel, «Crowd Energy», Bulletin SEV/VSE, 12/2016, S. 31–34.

Autorin

Dr. **Michèle Balthasar** ist Head Legal & Privacy Consulting bei der Swiss Infosec AG.
→ Swiss Infosec AG, 6210 Sursee
→ michele.balthasar@infosec.ch

Der vorliegende Artikel entstand im Rahmen einer Masterarbeit zum Thema «Datenschutz und Datensicherheit im Crowd-Energy-Umfeld», welche die Autorin 2017 am Internationalen Institut für Management und Technologie der Universität Fribourg verfasste.

[1] Ein Netzbetreiber kann allerdings den Anschluss an das Netz verweigern, wenn aufgrund des Anschlusses unverhältnismässige Massnahmen für den sicheren Netzbetrieb ergriffen werden müssten oder wenn der Endverbraucher keine Gewähr für einen funktionierenden internen Betrieb geben kann (Art. 3a E-StromVV).
[2] Aufgrund des Marktortprinzips findet die DSGVO auch Anwendung auf die Verarbeitung von personenbezogenen Daten von betroffenen Personen, die sich in der EU befinden, durch einen nicht in der EU niedergelassenen Verantwortlichen und Auftragsverarbeiter, wenn die Datenverarbeitung damit im Zusammenhang steht, betroffenen Personen Waren und Dienstleistungen anzubieten (Art. 3 DSGV).
[3] Die Totalrevision erlaubt, das revidierte Datenschutzübereinkommen SEV 108 des Europarats zu ratifizieren sowie die Richtlinie [EU] 680/2016 zu übernehmen. Denn mit der Ratifikation der «Bilateralen II», welche Bestandteil des Schengen-Acquis bilden, hat sich die Schweiz verpflichtet, auch die Richtlinie [EU] 2016/680 nicht aber die Verordnung [EU] 2016/679 zu übernehmen.
[4] Der Bundesrat kann Ausnahmen für Unternehmen vorsehen, die weniger als 50 Mitarbeiter beschäftigen und deren Datenbearbeitung nur ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt (Art. 11 Abs. 2 E-DSG). Sollte der Bundesrat von dieser Möglichkeit Gebrauch machen, so dürften wohl ein Grossteil der EVGs darunter fallen, sofern deren Datenbearbeitung nur ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt.