

Themenpapier 40 Datenschutz und Datensicherheit bei Smart Metering

06.Juli 2017

Position der Branche

Der VSE unterstützt die Entwicklung von Smart Metering und ist der Meinung, dass der vermehrte Einsatz von intelligenten Zählern (Smart Metern) eine interessante Option darstellt.

Mit intelligenten Zählern können Lastgänge aufgezeichnet werden, die etwas über das Verhalten von Personen aussagen, und deshalb als Personendaten gelten. Deshalb muss sichergestellt werden, dass der Datenschutz gewährleistet ist. Zudem muss die Vertraulichkeit, Verfügbarkeit und Integrität der Messdaten geschützt werden.

Der Datenschutz ist sowohl auf kantonaler, wie auf Bundesebene geregelt. Kantonale, kommunale oder privatrechtlich organisierte Netzbetreiber, die im Rahmen eines öffentlichen Auftrags Daten bearbeiten, unterstehen dem jeweiligen kantonalen Datenschutzgesetz. Netzbetreiber, die zusätzlich rein privatrechtliche Tätigkeiten nachgehen, sind für diese Tätigkeiten der Bundesdatenschutzgesetzgebung (DSG/VDSG) unterstellt. Es ist unabdingbar, hier eine einheitliche, bundesweite Regelung für alle Marktakteure zu erarbeiten, entweder durch Harmonisierung der kantonalen Datenschutzgesetze oder durch eine Erweiterung der spezialgesetzlichen Regelung im StromVG/StromVV.

Der VSE ist bereit, mit Lieferanten und Endverbrauchern einen subsidiären Anforderungskatalog zu Datenschutz und Datensicherheit bei Smart Metern zu erarbeiten, und an einer Lösung für die Überprüfung der Anforderungen mitzuarbeiten. Die Lösung soll praxistauglich und wirtschaftlich sein, und dem aktuellen Stand der Technik entsprechen. Für bereits installierte Smart Metering Lösungen, die diese Regeln noch nicht einhalten, soll ein Investitionsschutz gelten.

Der Datenschutz schliesst den innerbetrieblichen Umgang und die Weiterverwendung der Daten mit ein.

Botschaft

Datenschutz:

- Gleich lange Spiesse für alle Marktakteure: Harmonisierung der aktuellen kantonalen und eidgenössischen Gesetzgebung

Datensicherheit:

- Die Branche ist bereit, mit Lieferanten und Endverbrauchern einen subsidiären Anforderungskatalog zur Datensicherheit bei Smart Metern zu erarbeiten, und an einer Lösung für die Überprüfung der Anforderungen mitzuarbeiten
- Die Lösung soll Anpassungen an sich ändernde Bedrohungsszenarien im Software-Bereich (Updates) erlauben

- Die angestrebte Lösung soll wirtschaftlich vertretbar sein. Die Kosten sollen als anrechenbare Kosten gelten
- Für bereits installierten Smart Meter soll ein Investitionsschutz gelten

Auslesefrequenz:

- Die Auslesehäufigkeit eines Smart Meters soll sich nach den betrieblichen Bedürfnissen richten

Chancen und Risiken

Chancen

- Mit einer Einigung auf eine landesweit gültige Lösung für den Datenschutz wird sichergestellt, dass für alle Marktakteure die gleichen Bedingungen gelten: eine Voraussetzung für einen funktionierenden Markt. Mit der Einigung entfällt der Auslöser für einzelnen Datenschutzbeauftragte, sich mit eigenen Forderungen zu profilieren. Dies kann die Akzeptanz des Smart Meters erhöhen
- Transparente und einheitliche Anforderungen, wie Datenschutz und Datensicherheit bei Smart Metern einzuhalten und die Kundendaten zu schützen sind, können die Akzeptanz des Smart Meters erhöhen
- Um die Anforderungen für Datenschutz und Datensicherheit bei Smart Metern einzuhalten, sind beim Netzbetreiber erhebliche Investitionen erforderlich. Diese beschränken sich nicht auf Sachwerte, sondern umfassen auch Wissen und Ausbildung der Mitarbeiter. Dies dürfte den Druck erhöhen, durch Zusammenarbeit oder Auslagerung, die Messkosten durch Skalierungseffekte zu senken und gleichzeitig eine einheitliche Qualität sicherzustellen

Risiken

- Das intelligente Messgerät kann einen Beitrag zu mehr Innovation bei Energiedienstleistungen bieten. Zu hohe Forderungen in Bezug auf Datenschutz und Datensicherheit birgt aber die Gefahr, dieses Potential zu schmälern, und gleichzeitig den administrativen Aufwand für den Netzbetreiber stark zu erhöhen

Herleitung/Begründung

1. Datenschutz

Da viele Netzbetreiber ihre Tätigkeit auf Basis von kantonalen Gesetzen bzw. Vorgaben ausüben, sind sie als Datenbearbeiter dem jeweiligen kantonalen Datenschutzgesetz unterstellt und nicht dem Bundesdatenschutzgesetz (DSG). Es ist unabdingbar, eine einheitliche Regelung zu erarbeiten, damit für alle Akteure: Netzbetreiber, Dienstleister und Endverbraucher die gleichen Bedingungen gelten, unabhängig von ihrer Organisationsform. Der VSE unterstützt eine schlanke einheitliche spezialgesetzliche Regelung im StromVG/StromVV¹ resp. ENG/ENV, damit die Einführung von Smart Meter nicht behindert wird.

1.1 Energiedaten

Mit Smart Meter können unterschiedliche Energiedaten aufgezeichnet werden, wie zum Beispiel:

- Monats- und Tageswerte für die Abrechnung

¹ vgl. Art 17c StromVG, Art. 8d StromVV zur ES2050

- 15'-Lastgänge für Prognose und Abrechnung
- Echtzeitdaten z.B. für Verbrauchsanalysen

Monats- und Tageswerte

Daten in dieser Granularität können ebenso als personenbezogene Daten gelten. Aus Sicht des Datenschutzes können zur Erfüllung der Pflichten aus Energielieferverträgen die erforderlichen Daten erfasst und genutzt werden. Dafür braucht es keine ausdrückliche Zustimmung des Kunden. Die tägliche Datenerfassung ist deshalb eine kostengünstige Alternative für Endverbraucher ohne Netzzugang, die mit der generellen 15'-Erfassung nicht einverstanden sind.

15'-Messdaten

15-Minuten-Messdaten gelten als Personendaten, wenn sie einer bestimmten oder bestimmbarer Person zugeordnet werden können. Ebenso liegen Personendaten vor, wenn eine Information mehreren Personen gleichzeitig (z.B. den Mitgliedern eines Haushalts) zugeordnet werden kann (vgl. z.B. David Rosenthal, Handkommentar DSG, Zürich 2008, Art. 3 N 33). Als Persönlichkeitsprofile sind sie dann gemäss Gesetz sogar besonders zu schützen. Die Zuordnung erfolgt erst nach der Erfassung, beim Verarbeiten der Daten. Der Datenschutz schliesst deshalb insbesondere auch den innerbetrieblichen Umgang und die Weiterverwendung der Daten mit ein.

Vor der Zuordnung der Daten zu einer Person, sind die Daten unter einem Pseudonym abgelegt und als unbedenklich einzustufen (z.B. für die Weiterverarbeitung in Bilanzsummenaggregate).

Echtzeitdaten

Die Auslesung von Echtzeitdaten kann, wegen der derzeit zur Verfügung stehenden Bandbreite, nur punktuell erfolgen. Diese Daten werden in der Regel für Verbrauchsanalysen erhoben; das darf nur mit dem Einverständnis des Kunden geschehen.

Technische Daten

Technische Messdaten, z.B. Frequenz- oder Spannungsmessdaten, die der Netzbetreiber für die Netzplanung und Netzsicherheit benötigt, sind keine Personendaten und deshalb datenschutzrechtlich unkritisch.

1.2 Auslesefrequenz

Mit der Fernauslesung der Daten der intelligente Zähler, kann der Netzbetreiber seine betrieblichen Prozesse optimieren (Mieterwechsel, Bilanzgruppenmanagement etc.). Voraussetzung dafür ist, dass diese Daten rechtzeitig erfasst werden können. Mit den derzeit verbreiteten Kommunikationstechnologien bedeutet dies üblicherweise eine tägliche Datenerfassung.

1.3 Archivierung

Der Zeitraum für die Archivierung der Daten richtet sich nach den technischen Vorgaben im StromVV Art. 8 Abs. 4 (derzeit 5 Jahren).

2. Vergabe von Messdienstleistungen

Überträgt ein Netzbetreiber Dienstleistungen des Messwesens und des Informationsaustauschs in Bezug auf Smart Metering an Dritte, sind die Rechten und Pflichten des Dienstleisters vertraglich zu regeln. Dies

gilt insbesondere auch für die Anforderungen und Massnahmen im Bereich Datenschutz und Datensicherheit.

3. Datensicherheit

Der Datenschutz bedingt, dass die Messdaten mit entsprechenden Massnahmen gesichert werden. Die Massnahmen beschränken sich nicht auf das intelligente Messgerät, sondern umfassen das gesamte intelligente Messsystem, sowie eine allfällige Visualisierungsplattform und schliessen den innerbetrieblichen Umgang mit den Daten sowie die Datenverarbeitung und -weitergabe mit ein.

Die Branche ist bereit, anhand der vom BFE vorgelegten Schutzbedarfsanalyse, mit Herstellern und Endverbrauchern einen subsidiären Anforderungskatalog zur Datensicherheit des intelligenten Messsystems zu erarbeiten, und an einer Lösung für deren Überprüfung mitzuarbeiten.

Mit einer solchen Konformitätsprüfung wird sichergestellt, dass ein intelligentes Messgerät sicher im Feld eingesetzt werden kann. Dies ist jedoch eine Momentaufnahme: Die Bedrohungslage kann sich mit der Zeit ändern. Die Messgeräte-Software soll mit einem Software-Update an die geänderte Bedrohungslage angepasst werden können, ohne eichrechtliche Konsequenzen auszulösen.

Gesetzliche Ausgangslage

Studien/Berichte:

- «Ansätze zur Gewährleistung der IKT-Sicherheit von intelligenten Messsystemen bei Endverbrauchern» (31.10.2015, Abschlussbericht im Auftrag des Bundesamtes für Energie BFE)
- Studie «Schutzbedarfsanalyse Smart Metering in der Schweiz» (17. Juni 2015, Abschlussbericht im Auftrag des Bundesamtes für Energie BFE)

Auskünfte

Hendrik la Roi

Telefon: 062 825 25 34

E-Mail: hendrik.laroi@strom.ch

Verband Schweizerischer Elektrizitätsunternehmen

Hintere Bahnhofstrasse 10, 5001 Aarau, www.strom.ch