Datenschutz

Schnittstelle als Risiko

[22.07.2020] Die Datenschutz-Grundverordnung gilt auch für das Smart Metering. Deshalb ist die Öffnung der CLS-Schnittstelle für die Erhebung von Verbrauchswerten im Submetering aus datenschutzrechtlicher Sicht bedenklich.

Die bei der Aufzeichnung durch Smart Meter erhobenen Stromverbrauchsdaten sind von hoher datenschutzrechtlicher Bedeutung, denn sie ermöglichen einen tiefen Einblick in die durch Artikel 13 GG gewährleistete Unverletzlichkeit der Wohnung. Aus ihnen lassen sich Rückschlüsse auf den individuellen Lebensablauf der Bewohner ziehen. Deshalb ist relevant, wie granular Verbrauchsdaten gespeichert werden, wo sie gespeichert werden und wer Zugang zu welchen Daten erhält. Der Datenschutz ist ein europäisches und deutsches Grundrecht.
Das EU-Recht (Art. 16 AEUV, Artikel 8 EU-GRCh) garantiert jeder Person ein Grundrecht auf Schutz der sie betreffenden Daten. Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO) direkt anwendbares Recht in allen EU-Mitgliedsstaaten. Das neue EU-Datenschutzrecht soll die Grundrechte und Grundfreiheiten natürlicher Personen schützen (Art. 1 Abs. 2 DSGVO). Es begrenzt die Verarbeitung personenbezogener Daten und soll den betroffenen Personen eine effektive Kontrolle über ihre Daten ermöglichen. Insofern knüpft die DSGVO an das im deutschen Verfassungsrecht verankerte Grundrecht auf informationelle Selbstbestimmung an. Eine allein auf die Verhinderung des missbräuchlichen Zugriffs Unberechtigter beschränkte Sichtweise würde zu kurz greifen.

Konkretisierte Vorgaben

Die Vorgaben der DSGVO werden durch das Messstellenbetriebsgesetz (MsbG) konkretisiert. Beim Aufbau und Betrieb intelligenter Messsysteme müssen sowohl die DSGVO-Vorgaben als auch die Regelungen des Messstellenbetriebsgesetzes (MsbG) beachtet werden.
Die Bestimmungen technologischen Datenschutzes (Art. 25 DSGVO) basieren auf dem Grundgedanken, dass sich der Datenschutz am besten gewährleisten lässt, wenn er bereits bei der Erarbeitung eines Datenverarbeitungskonzepts und bei der Gestaltung von Produkten und Diensten technisch integriert wurde (Data Protection by Design, Data Protection by Default). Schon in der Entwicklung sind technische und organisatorische Maßnahmen zum Datenschutz zu ergreifen, die sicherstellen, dass durch Voreinstellung nur die personenbezogenen Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind.
Gemäß Art. 5 Abs. 1 lit. c) DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung) – der Eingriff in das Grundrecht auf Datenschutz muss so gering wie möglich gehalten werden. Zudem sind die Grundsätze der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DSGVO) zu beachten und bilden die Kernelemente des Systemdatenschutzes. Technische und organisatorische Maßnahmen haben nach dem Stand der Technik ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste zu gewährleisten (Art. 32 DSGVO).

Beschränkung der Verarbeitung

Gemäß Art. 5 Abs. 1 DSGVO dürfen personenbezogene Daten nach Granularität und Anlass nur in dem erforderlichen Umfang erhoben und weiterverarbeitet werden, um die Vorgabe der Datenminimierung einzuhalten. Zudem muss eine Beschränkung der Verarbeitung nach dem Need-to-know-Prinzip entsprechend den Zwecken und den Aufgaben der Verantwortlichen erfolgen.
Das MsbG integriert und konkretisiert die vorstehenden datenschutzrechtlichen Grundsätze, in dem es in Kapitel 3 Regelungen zur Datenerhebung, -verarbeitung und -nutzung trifft. So sehen die §§ 55-59 MsbG besondere Regelungen zur Messwerterhebung vor und begrenzen den zulässigen Umfang der Datenerhebung. Es werden abgestufte Vorgaben zur Detailgenauigkeit und Auflösung der Messwerte gemacht. Neben Aspekten der Verschlüsselung geht es also regelmäßig darum, wie granular Verbrauchsdaten gespeichert werden, wo sie gespeichert werden und wer Zugang zu den Daten erhält. Die Informationen, die der Kunde freiwillig mitteilt und/oder die Folge seiner privatautonomen Vertragsgestaltung sind, um eine Wertrealisierung für sich zu nutzen, können im Smart Meter Gateway (SMGW) voreingestellt und gezielt erhoben werden. Damit trägt sie zugleich dem Gebot der Datenminimierung (Art. 5 DSGVO) Rechnung und stärkt die Kontrolle der Kunden über ihre Daten (Datensouveränität).

Sensible Daten

Die vorstehenden Grundsätze müssen auch im Hinblick auf Erfassung und Verarbeitung der Verbrauchswerte weiterer Sparten durch technische Voreinstellungen sichergestellt werden. Auch bei Messwerten übriger Sparten handelt es sich um sensible Daten, die zu einer Erstellung von Verhaltensprofilen des Nutzers verwendet werden können.
Die Weiterentwicklung von Smart Meter Gateways sowie die sektorübergreifende Bedeutung sind in der Roadmap des Bundesministeriums für Wirtschaft und Energie (BMWi) und des Bundesamts für Sicherheit in der Informationstechnik (BSI) beschrieben. Die „Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende“ ist der maßgebliche und stetig fortzuschreibende Arbeitsplan für die Fortentwicklung des Smart Meter Gateways für weitere Einsatzbereiche nach dem Gesetz zur Digitalisierung der Energiewende (GDEW) hin zur umfassenden Kommunikationsplattform für die Energiewende.
Eine hierauf gegründete Systemarchitektur muss sowohl die sichere Anbindung aller Messeinrichtungen (Strom-, Gas- und Wasserzähler, aber auch Heizwärme- und weitere Submetering-Messeinrichtungen) sicherstellen, daneben aber auch die Anforderungen zur Datensouveränität und an den Datenschutz berücksichtigen. Eine Unterscheidung zwischen Strom-, Gas- und Wasserzählern und solchen, die im Submetering beim Kunden unmittelbar Messwerte erheben, darf für die datenschutzrechtliche Behandlung keine Relevanz haben. Einen dem widersprechenden Einsatz des SMGW gilt es zu verhindern.

Direkte Kommunikation

Die direkte Kommunikation zwischen der CLS-Schnittstelle (Controllable Local Systems) von Smart Meter Gateways und externen Marktteilnehmern (EMT) jedoch sieht keine Einbindung des Gateway-Administrators während der Kommunikation vor. Lediglich der Erstkontakt für den Kommunikationsaufbau findet über den Administrator statt. Geprüft wird nur die Authentizität des EMT und dessen Zugriffsberechtigung. Anschließend erfolgt die Eröffnung des Verbindungskanals. Die den Datenschutz und die Datensicherheit gewährleistenden Mindestanforderungen des § 22 MsbG durch Schutzprofile und TR sehen diesen Kommunikationsweg aus gutem Grund nicht vor.
Für die Anwendungsfälle Zählerverwaltung und den Abruf und Empfang von Messwerten über die LMN-Schnittstelle (Lokales Metrologisches Netz) stellt die Technische Richtlinie BSI TR-03109 strikte Anforderungen an Sicherheit und Kommunikation des SMGW, die auch bei anderen Messgegenständen

(Wasser, Wärme, Gas) nicht abgeschwächt werden oder durch Öffnung der CLS-Schnittstelle für die direkte Verbrauchsmessung beim Kunden umgangen werden dürfen.
Die Weiterentwicklung der System-Architektur der SMGW-Kommunikationsplattform für den Einsatzbereich aller Messsysteme sollte ausschließlich über die datenschutzkonforme LMN-Schnittstelle erfolgen. Die Öffnung der CLS-Schnittstelle für die Erhebung und Übertragung von Verbrauchswerten im Submetering begegnet datenschutzrechtlichen Bedenken.
Peter Schaar war bis 2013 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit; Viola Rund ist Syndikusrechtsanwältin bei der Hausheld AG.

()

Dieser Beitrag ist im Juni Sonderheft 2020 von stadt+werk zur Digitalisierung der Energiewirtschaft erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Smart Metering, CLS-Schnittstelle, DSGVO