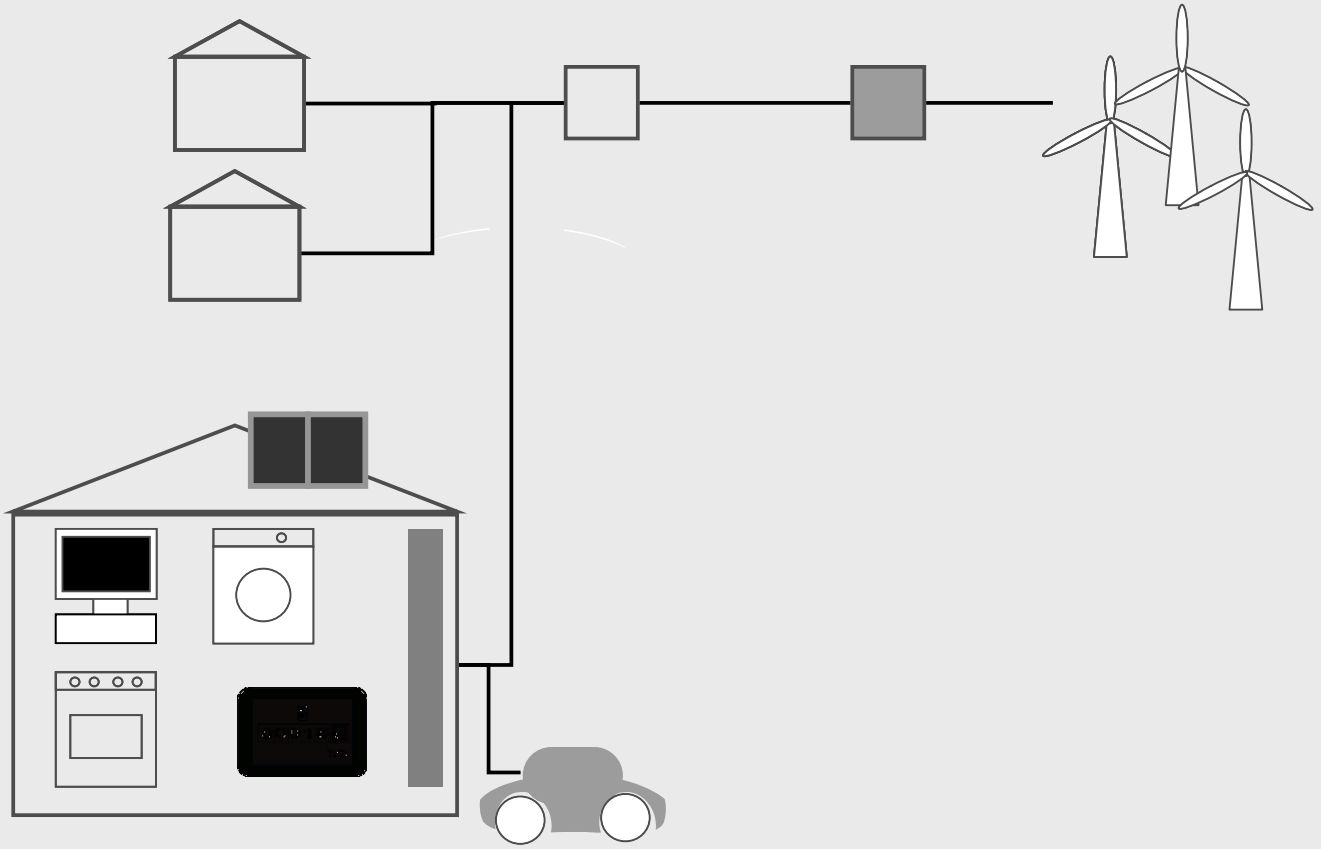

Orientierungshilfe datenschutzgerechtes Smart Metering

Juni 2012

Konferenz der Datenschutzbeauftragten des Bundes und der Länder
und Düsseldorfer Kreis

Impressum

Konferenz der Datenschutzbeauftragten des Bundes und der Länder
und Düsseldorfer Kreis

Kontakt
ref4@bfdi.bund.de

Stand
Juni 2012

USE CASE VERZEICHNIS

1 Einleitung

Die Sicherstellung einer nachhaltigen Energieversorgung stellt ein wichtiges energiepolitisches Ziel Deutschlands dar. Intelligente Energienetze und -zähler (sog. Smart Meter) sind eine Grundvoraussetzung für eine ressourcenschonende, umweltfreundliche und effiziente Produktion, Verteilung und Nutzung von Energie, da sie neue Tarife, wie etwa lastvariable Tarife und Zeitzonentarife, erst möglich machen. Mit der Novellierung des Energiewirtschaftsgesetzes (EnWG) im Jahr 2011 wurde in Deutschland hierfür der Startschuss gegeben. Das Gesetz enthält auch die erforderlichen grundsätzlichen Datenschutzregelungen. Zur Konkretisierung und detaillierten Ausgestaltung dieser Grundsätze muss noch eine Rechtsverordnung erlassen werden. Dieses Papier gibt Empfehlungen sowohl zur Ausgestaltung der Verordnung als auch zur datenschutzgerechten Konzeption der technischen Systeme für das Smart Metering. Zudem bietet es Hilfestellungen für die Arbeit der Datenschutzaufsichtsbehörden in den Ländern.

Der Einsatz von Smart Metering als Mittel für eine umweltschonende Energienutzung stellt aber keinen deutschen Sonderweg dar. Es handelt sich vielmehr um eine gesamteuropäische Initiative. Alle Mitgliedstaaten der Europäischen Union sind verpflichtet, intelligente Energienetze und -zähler einzuführen. Daher wird europaweit über die zu beachtenden Datenschutzstandards diskutiert. Am 9. März 2012 hat die Europäische Kommission Empfehlungen zur Vorbereitung für die Einführung intelligenter Messsysteme herausgegeben[1]. Darin fordert die Kommission, den Schutz der Privatsphäre in vollem Umfang für die Verarbeitung personenbezogener Daten durch intelligente Messsysteme zu gewährleisten.

Die Orientierungshilfe ist diesen europäischen Vorgaben verpflichtet und will zeigen, wie die zentralen Forderungen des Datenschutzes wie Zweckbindung, Datensparsamkeit und Erforderlichkeit berücksichtigt werden können. Dabei wird die gesamte Prozesskette der Verarbeitung personenbezogener Daten betrachtet. Diese beginnt mit dem Messen von Strommengen mittels Zählern und reicht über die Verarbeitung im Smart Meter bis zur weiteren Nutzung durch die an der Energielieferung, -verteilung und -abrechnung beteiligten Stellen. Dabei werden verschiedene Anwendungsfälle, so genannte Use Cases, dargestellt, analysiert und datenschutzrechtlich bewertet. Die Use Cases beziehen sich auf diejenigen Datenverarbeitungsprozesse, für die es eine gesetzliche Ermächtigungsgrundlage gibt. Betrachtet werden die Use Cases aus der Perspektive des Datenschutzes und derjenigen Personen, die von der Kommunikation mit Verbrauchs- bzw. Steuerungsdaten, die von Smart Meter erhoben werden, betroffen sind. Sie haben insofern keinen Anspruch auf Vollständigkeit und bilden nicht die komplette energiewirtschaftliche Perspektive ab. Das Intelligente Energienetz wird nur soweit betrachtet, wie Smart Meter Steuerungsdaten für das Netz bereitstellen. Jedoch werden in diesem Papier noch keine datenschutzrechtlichen Anforderungen an das Intelligente Energienetz formuliert. Die Use Cases dienen der Definition von Voraussetzungen, unter denen die Datenverarbeitung beim

[1] Vgl. Com(2012) 1342 final

Smart Metering datenschutzrechtlich zulässig ist und die auch bei der Konzeption von Geräten, Verfahren und Infrastrukturen zu beachten sind. Es gilt insbesondere zu vermeiden, dass Profile der Lebensführung von Menschen gebildet werden können. Dies käme einem Eingriff in die Privatsphäre entsprechend einem „messtechnischen Lauschangriff“[2] gleich.

2 Rahmenbedingungen

Die Rahmenbedingungen werden anhand der Beschreibung von Begriffen, Rollen und Funktionen sowie der Darstellung der einschlägigen Datenarten vorgestellt.

2.1 Begriffe

Der **Zähler** bezeichnet die Messeinrichtung zur Erzeugung von Messdaten.

Das **Gateway** stellt die Kommunikationseinheit eines intelligenten Messsystems zur sicheren Kommunikation zwischen Haushalt und externen berechtigten Marktteilnehmern dar. Die Kommunikation kann dabei mit mehr als einem Marktteilnehmer erfolgen. In Mehrfamilienhäusern kann das Gateway an mehrere Zähler angeschlossen sein, jeder Haushalt hat dafür seinen eigenen, sicher abgetrennten Bereich. Das Gateway wird durch das Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und die Technische Richtlinie TR-03109 spezifiziert.

Smart Meter bezeichnet das gesamte intelligente Messsystem, das aus einer Messeinrichtung und einer Kommunikationseinheit mit Zusatzfunktionen besteht. Die Anforderungen an Smart Meter werden in § 21d EnWG durch einen Verweis auf Schutzprofile und Technische Richtlinie spezifiziert.

Smart Metering betrifft sämtliche Aktionen, die durch ein Smart Meter durchgeführt werden.

Unterbrechbare Verbrauchseinrichtungen verfügen über einen separaten Zählpunkt und werden vom Letztverbraucher dem Netzbetreiber zur Netzentlastung zur Verfügung gestellt. Unterbrechbare Verbrauchseinrichtungen können beispielsweise Speicher, Anlagen zur Energieerzeugung oder steuerbare Geräte („Weiße Ware“) sein. Betrachtet werden nur unterbrechbare Verbrauchseinrichtungen, die über das Gateway mit externen Marktteilnehmern verbunden sind.

[2] Vgl. Klaus Müller, Gewinnung von Verhaltensprofilen am intelligenten Stromzähler, DuD 2010/06, S. 359ff.

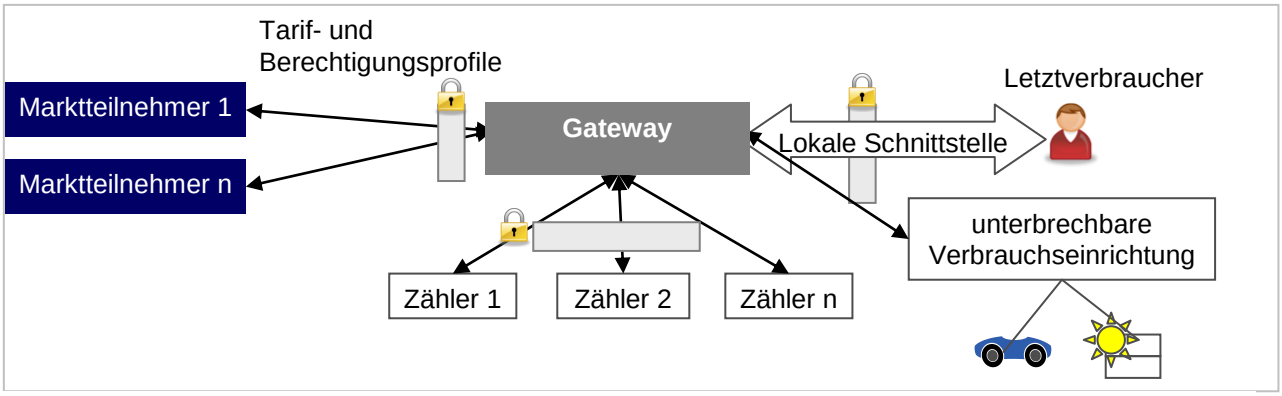

Abbildung 1: Smart Meter und Umgebung

2.2 Akteure und Rollen

Die Akteure und deren Rollen sind § 21g EnWG entnommen.

Bezeichnung	Beschreibung
Berechtigter Marktteilnehmer	externer Akteur, der nach festgelegten Kriterien als Kommunikationspartner für das Gateway zugelassen ist
Energielieferant	liefert für den Letztverbraucher Energie und rechnet diese ab
Gateway-Administrator	administriert das Gateway beim Letztverbraucher, z.B. durch Einbau, Betrieb, Wartung sowie Konfiguration
Letztverbraucher	bezieht und verbraucht Energie und kann als natürliche Person ein eigenes Recht auf informationelle Selbstbestimmung geltend machen
Messstellenbetreiber	administriert ggf. das Messsystem
Netzbetreiber	Verteil- oder Übertragungsnetzbetreiber
Prosumer	bezieht nicht nur als Letztverbraucher Energie, sondern speist selbst erzeugte Energie ins Netz ein oder/und stellt Speicherkapazitäten zur Zwischenspeicherung von Energie zur Verfügung
Übertragungsnetzbetreiber	verbindet die Verteilnetze und transportiert Energie
Verteilnetzbetreiber	sorgt für die Stromverteilung vor Ort bis zum Letztverbraucher

2.3 Datenarten

Nicht alle Datenarten finden sich in den Use Cases wieder. Alle Daten, die mit einem Smart Meter erhoben werden, sind personenbezogen, unabhängig davon, ob es sich um technische Daten handelt.

Bezeichnung	Beschreibung
Abrechnungsdaten (Einspeisung)	Einspeisedaten aggregiert pro Tarifzone, in welcher eine bestimmte Vergütung für Energie gültig ist, kumuliert nach gewähltem Abrechnungszeitraum
Abrechnungsdaten (Verbrauch)	Verbrauchsdaten aggregiert pro Tarifzone, in welcher ein bestimmter Preis für Energie gültig ist, kumuliert nach gewähltem Abrechnungszeitraum
Ausspeisemenge	Verbrauch einer unterbrechbaren Verbrauchseinrichtung
Credentials	Berechtigungsnachweis des Letztverbrauchers oder des Gateway-Administrators zur Authentisierung und Autorisierung
Einspeisemenge	abgegebener Strom pro Zeitintervall
Gateway-Administrationsdaten	Gateway-ID, IP-Adresse, Gateway-Schlüssel, Gateway-Zertifikat, Updates, Patches, Gateway-Statusdaten, Berechtigungsprofildaten, Zeit, Liste aller zugeordneten Zähler und deren Zertifikate, ggf. Liste der Messstellenbetreiber für jeden Zähler …
Kundendaten	Name, Vorname, Geburtsdatum, Anschrift, Kundennummer, privater/gewerblicher Kunde, Kontoverbindung, Zählpunkt
Messdaten	Daten, die mit dem Zähler ermittelt werden
Netzzustandsdaten	Phasenwinkel, Spannung, Frequenz, Stromfluss, etc.
Rechnungsbetrag	durch den Letztverbraucher zu zahlender Betrag pro gewähltem Zeitintervall
Rechnungsdaten	Abrechnungs- und Kundendaten
Smart Meter Daten	Messdaten, die durch Smart Meter erhoben werden: Smart Meter Daten sind personenbezogene Daten
Speichermenge	gespeicherte Energie pro Zeiteinheit
Statusdaten Energiespeicher	Bereitschaft zur Aufnahme von Energie
Statusdaten unterbrechbare Verbrauchseinrichtung	Ein- und Ausspeisemenge der unterbrechbaren Verbrauchseinrichtung, Statusdaten Energieangebot, Statusdaten Energiespeicher

3 Rechtliche Einordnung

Mit der Novellierung des Energiewirtschaftsgesetzes wurde ein Rechtsrahmen für die Einführung von Smart Metern geschaffen. Das Gesetz regelt die Rahmenbedingungen für die Datenverarbeitung beim Smart Metering und enthält die notwendigen Ermächtigungsgrundlagen, um diese Vorgaben in Verordnungen der Bundesregierung, Schutzprofilen und Technischen Richtlinien des BSI, Festlegungen der Bundesnetzagentur (BNetzA) sowie eichrechtlichen Anforderungen durch die Physikalisch Technische Bundesanstalt (PTB) zu konkretisieren.

Derzeit liegen ein Schutzprofil sowie eine Technische Richtlinie für Smart Meter vor, die vom BSI erarbeitet und veröffentlicht[3] worden sind. Darin werden verbindliche und einheitliche Mindeststandards sowie Vorgaben zur Funktionalität und Interoperabilität festgelegt, die für die technische Umsetzung der spezifischen Datenschutz- und Datensicherheitsanforderungen notwendig sind. In der Verordnung nach § 21i Abs. 1 Nr. 4 EnWG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten mit der notwendigen Bestimmtheit abschließend zu regeln, um die erforderliche Rechtsklarheit zu schaffen. Dies dient einerseits der Sicherung der Betroffenenrechte und ihrer Durchsetzbarkeit und andererseits der Rechtssicherheit der Betreiber von Smart Meter.

3.1 Bereichsspezifische Rechtsgrundlage

Smart Meter Daten stellen grundsätzlich personenbezogene Daten dar. Dies gilt auch, soweit es sich um technische Daten handelt. Allerdings kann die Sensitivität der verschiedenen Daten unterschiedlich hoch sein, so dass der Datenschutzbedarf entsprechend variiert. Dies ändert jedoch nichts am Personenbezug. Nach dem Bundesdatenschutzgesetz (BDSG) handelt es sich auch bei personenbeziehbaren Daten um personenbezogene Daten. Werden Daten von einem Smart Meter erhoben, verarbeitet, dargestellt oder übermittelt, ist das Recht auf informationelle Selbstbestimmung betroffen. Der Datenschutzbedarf der personenbezogenen Daten ist abhängig davon, inwieweit aus den Daten Rückschlüsse auf das Verhalten und die Lebensgewohnheiten der Letztverbraucher möglich sind.[4] Daher ist die Intensität des Eingriffs in dieses Grundrecht abhängig von verschiedenen Faktoren wie dem Auslesetakt, der Sensitivität der Daten, der Übertragung an externe Stellen oder dem Schwierigkeitsgrad, die Daten einer bestimmten Person zuzuordnen.

Das Datenschutzrecht geht von einem Verbot mit Erlaubnisvorbehalt aus. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat.

[3] www.bsi.bund.de

[4] Diese Definition geht weiter als die in der Gesetzesbegründung, die davon ausgeht, dass ein Eingriff erst dann vorliegt, wenn Rückschlüsse auf das Verhalten und die Gewohnheiten der Verbraucher ermöglicht werden (vgl. BT Drs. 17/6072, S. 77), und damit verkennt, dass auch i. ü. personenbezogene Daten verarbeitet werden.

§ 21g EnWG stellt eine Rechtsvorschrift in diesem Sinne dar. Danach darf die Verarbeitung nur erfolgen, soweit dies erforderlich ist für die in § 21g Abs. 1 Nr. 1 bis Nr. 8 EnWG abschließend aufgeführten Zwecke. Die Norm zählt Stellen auf, die zum Datenumgang berechtigt sind, und verweist für die Einwilligung zur Erweiterung des Nutzerkreises auf § 4a BDSG, der die Voraussetzungen einer wirksamen Einwilligung vorgibt. Die jeweils ermächtigte Stelle ist verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes. Zudem sieht das Energiewirtschaftsgesetz die Möglichkeit der Auftragsdatenverarbeitung vor. Dem Letztverbraucher wird die Anonymisierung und Pseudonymisierung seiner Daten zugesichert.

Näheres ist in einer Rechtsverordnung zu regeln (§ 21g Abs. 6 i. V. m. § 21i Abs. 1 Nr. 4 EnWG). Das Energiewirtschaftsgesetz führt bereits die Grundsätze der Verhältnismäßigkeit und der Zweckbindung auf. Festgeschrieben werden dort zudem das Koppelungsverbot, die Information des Letztverbrauchers, das Einwilligungserfordernis sowie Kontroll- und Einwirkungsmöglichkeiten für das Fernmessen und Fernwirken. Die Rechtsverordnung soll Höchstfristen für die Speicherung festlegen und die berechtigten Interessen der Unternehmen und Betroffenen angemessen berücksichtigen. Weiterhin sind die Eigenschaften und Funktionalitäten von Smart Meter datenschutzgerecht zu regeln.

§ 21e EnWG sieht vor, dass nur Messsysteme verwendet werden dürfen, die den Datenschutz-, Datensicherheits- und Interoperabilitätsanforderungen für Smart Meter zum jeweils aktuellen Stand der Technik entsprechen. Hervorgehoben wird die Verpflichtung zur Anwendung von Verschlüsselungsverfahren bei der Nutzung allgemein zugänglicher Kommunikationsnetze. Zur Sicherstellung der Anforderungen von Schutzprofilen und Technischen Richtlinien installiert die Norm ein Zertifizierungsverfahren, das ebenfalls in einer Rechtsverordnung zu konkretisieren ist. Nach § 14a EnWG können Letztverbraucher im Bereich der Niederspannung den Betreibern von Elektrizitätsverteilernetzen gegen Berechnung eines reduzierten Netzentgeltes die Steuerung von unterbrechbaren Verbrauchseinrichtungen zur Netzentlastung gestatten. Die Einzelheiten dieses Einwilligungserfordernisses sind wiederum in einer Rechtsverordnung zu regeln.

3.2 Einwilligung des Letztverbrauchers

§ 21g Abs. 1 EnWG erlaubt eine Verarbeitung personenbezogener Daten nur, soweit dies erforderlich ist für bestimmte, im Gesetz abschließend aufgeführte Fälle, die im Rahmen der Datenschutzverordnung nach § 21i Abs. 1 Nr. 4 EnWG näher auszugestalten sind.[5] So dürfen etwa bei einem herkömmlichen Tarif, bei dem nur die verbrauchte Gesamtstrommenge eines bestimmten Zeitraumes relevant ist, auch keine weiteren Daten aufgezeichnet werden.[6]

[5] Zu den entsprechenden Forderungen und Empfehlungen siehe unter 4.
[6] Vgl. BT Drs. 17/6072, S. 79.

Jegliche darüber hinausgehende Datenverarbeitung ist nur mit Einwilligung des Letztverbrauchers zulässig. Dies gilt auch für die Beauftragung weiterer Stellen (vgl. § 21g Abs. 2 und § 21b Abs. 2 EnWG). Als Grundprinzip der Einwilligung sollte die Verordnung daher vorsehen, dass Aktionen seitens des Verbrauchers nur für die Offenlegung von Daten, die über die gesetzlich aufgeführten Funktionen hinausgehen, erfolgen müssen, nicht aber für den Schutz der personenbezogenen Daten. Wenn dem Verbraucher mehrere Optionen angeboten werden, sollte die Standardeinstellung die datenschutzfreundlichste Einstellung sein („privacy by default“).

Soweit es den Umgang mit personenbezogenen Daten betrifft, gelten neben dem Energiewirtschaftsgesetz die Vorgaben des Bundesdatenschutzgesetzes. Dies gilt insbesondere für § 4a BDSG. Danach ist eine Einwilligung nur wirksam, wenn sie auf der freien, bestimmten und informierten Entscheidung des Letztverbrauchers beruht. Für die Verordnung empfiehlt sich ein Verweis auf diese Vorgaben.[7]

Es ist sicherzustellen, dass detaillierte Informationen über den Energieverbrauch nur dem betroffenen Letztverbraucher zugänglich sind. Wenn dieser sich für eine detaillierte Erfassung seiner Verbrauchsdaten entscheidet, muss vor jeder einzelnen Nutzung oder Weitergabe dieser Informationen für andere Zwecke sein informiertes positives Einverständnis eingeholt werden. Zur Gewährleistung der Datenhoheit muss er selbst bestimmen können, wem er welche Daten für welche Zwecke überlässt. Dafür muss er die Möglichkeit erhalten, Tarif- und Berechtigungsprofile, die sich aus seinen vertraglichen Vereinbarungen ergeben, zu kontrollieren und effektiv gegen Abweichungen vorzugehen. Dies kann durch die Schaffung effizienter Prozesse zur Wahrung der Betroffenenrechte sichergestellt werden.

Die Einwilligungserklärungen müssen ohne Nachteile für den Letztverbraucher, die über die unmittelbaren Folgekosten hinausgehen, und ohne Fristen frei widerruflich sein. Für jeden freiwillig gewählten Dienst muss jederzeit eine unabhängige Kündigungsmöglichkeit bestehen.

Darüber hinaus ist insbesondere das Koppelungsverbot in der Verordnung näher zu regeln. Die Inanspruchnahme von z. B. umweltschonenden oder kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene in die Offenlegung ihrer personenbezogenen Nutzungsprofile einwilligen müssen. So darf auch die Datenverarbeitung zur Veranschaulichung des Energieverbrauchs nicht an den Abschluss eines Energielieferungsvertrags mit variablem Tarif gekoppelt werden.

4 Forderungen und Empfehlungen

4.1 Allgemein

Wesentliches Ziel ist es, die schutzwürdigen Interessen der Betroffenen in Bezug auf ihr Recht auf informationelle Selbstbestimmung zu wahren. Es gilt zu verhindern,

[7] Dies folgt auch aus § 21g Abs. 2 EnWG.

dass Informationen über das Nutzungsverhalten der Letztverbraucher unberechtigterweise erlangt werden können. Hierzu bedarf es verbindlicher Regelungen, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen und den Einsatz von Maßnahmen nach dem jeweils aktuellen Stand der Technik sicherstellen. Neben gesetzlichen Regelungen für die Erhebung, Verarbeitung und Nutzung der durch die Smart Meter erhobenen Daten bedarf es verbindlicher Standards für den technischen Datenschutz und die IT-Sicherheit. Die Forderungen sind entsprechend den in den Use Cases dargestellten Anforderungen zu präzisieren.

I. Zweckbindungsgrundsatz

Die strikte Zweckbindung der anfallenden personenbezogenen Daten ist zu beachten. Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die in § 21g Abs. 1 EnWG aufgezählten Zwecke erforderlich ist.[8] So dürfen Abrechnungsdaten nur für die Erstellung der Abrechnung verarbeitet werden.

II. Datenvermeidung, Datensparsamkeit und Verhältnismäßigkeit

Die Auswahl und Gestaltung von Datenverarbeitungsprozessen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Daher sind Regelungen zu treffen, mit denen eine strikte Beschränkung der Datenverarbeitung auf das jeweils erforderliche Maß in Bezug auf Art und Menge der Daten erreicht wird. Festzulegen sind diejenigen auf Smart Metering basierenden Daten, die für die jeweils näher bestimmten Zwecke erforderlich sind, insbesondere soweit sie den privaten Bereich mittels Smart Meter verlassen.

Bei der Bestimmung der Daten, die im Rahmen der jeweiligen Erlaubnistatbestände verarbeitet werden dürfen, sind zudem die in § 21g Abs. 3 EnWG aufgeführten Datenkategorien der Verkehrs- und Bestandsdaten in der Verordnung zu definieren.[9]

Die Festlegung von größtmöglichen Intervallen zwischen den einzelnen Ablesezyklen ist von zentraler Bedeutung. Es muss verhindert werden, dass aus dem Verbrauch Rückschlüsse auf das Verhalten der Letztverbraucher gezogen werden können. Die Ablesevorgänge sind auf das erforderliche Maß (z. B. der monatlichen/jährlichen Übermittlung/Ablesung) zu begrenzen.

Smart Meter Daten sind möglichst nicht mit Personenbezug zu übermitteln. Soweit dies nach dem Verwendungszweck möglich ist, sind personenbezogene Daten zu anonymisieren, pseudonymisieren oder aggregieren.

Smart Meter Daten sollen nur dann den Haushalt verlassen, wenn dies erforderlich ist. Dies muss technisch durch entsprechende Tarif- und Berechtigungsprofile, welche die Übermittlung von Daten an externe Marktteilnehmer regeln, abgebildet werden. Zur Umsetzung variabler Tarife sollen Smart Meter die notwendigen Berechnungen zur Verbrauchsermittlung in Tarifzonen selbst durchführen können.

[8] Vgl. hierzu im Einzelnen die Anwendungsfälle unter 4.3.
[9] Der Begriff der Verkehrs- und Bestandsdaten wird in § 21g Abs. 3 EnWG verwendet. Es handelt sich dabei nicht um einen Begriff des BDSG.

Auch muss es die Möglichkeit geben, hoch aufgelöste Daten etwa zur Verbrauchsvisualisierung lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.

Bei der Ausgestaltung der Verfahren sind die Stellen zu minimieren, an die Daten übermittelt werden. Zudem sind entsprechend angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.

III. Transparenz der Datenverarbeitung: Gewährleistung von Informations- und Betroffenenrechten

Das Recht auf informationelle Selbstbestimmung fordert zum einen, dass der Letztverbraucher zu jeder Zeit über die Verwendung von Smart Meter Daten und die jeweiligen Zwecke informiert ist. Kommunikationsvorgänge und Verarbeitungsschritte von Smart Meter müssen daher zu jeder Zeit sichtbar und die Einhaltung der Bestimmungen in rechenschaftspflichtigen Praktiken nachweisbar sein. Zum anderen bedarf es durchsetzbarer Ansprüche auf Löschung, Berichtigung und Widerspruch für die Betroffenen.[10]

Die Verantwortlichkeiten für die jeweiligen Datenverarbeitungsprozesse müssen eindeutig geregelt und für den Letztverbraucher transparent sein. Nur eine eindeutige Zuweisung ermöglicht dem Letztverbraucher die Durchsetzung seiner Rechte sowie die Wahrnehmung seiner Möglichkeiten bei der Vertragsgestaltung. Eine klare Zuständigkeitsverteilung erleichtert zudem die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften durch die Datenschutzaufsichtsbehörden, deren Zuständigkeit sich parallel zu den Verantwortlichkeiten der Akteure bestimmt.[11]

IV. Datensouveränität der Betroffenen

Zur Gewährleistung der informationellen Selbstbestimmung darf die Verarbeitung von personenbezogenen Daten nur unter Kontrolle des Betroffenen erfolgen. Die rechtliche und tatsächliche Herrschaft des Letztverbrauchers über das Smart Meter und die von diesem erhobenen und verarbeiteten Smart Meter Daten muss stets gewährleistet sein. Der Letztverbraucher muss in die Lage versetzt werden, den Zugriff auf und die Steuerung des Smart Meter im Haushalt zu erkennen und auch unter klar definierten Voraussetzungen zu unterbinden (Interventionsmöglichkeit), z. B. durch Ausschalten der Kommunikation mit Sicherstellung, dass Messen nach vertraglicher Vereinbarung weiter geschieht und eine korrekte Abrechnung möglich ist.

Dafür sind Mechanismen vorzusehen, die dem Letztverbraucher die Kontrolle über alle verfügbaren Informationen ermöglichen. Insbesondere muss der Letztverbraucher die Möglichkeit haben, zu erkennen, welche Informationen zur Erfüllung des

[10] Diese sollten zumindest dem Umfang des § 35 BDSG entsprechen.
[11] Die datenverarbeitenden Stellen unterliegen der Datenschutzaufsicht der Aufsichtsbehörden in den Bundesländern. Maßgeblich für die örtliche Zuständigkeit ist der Sitz der jeweiligen datenverarbeitenden Stelle.

Vertragszwecks nicht erforderlich sind.[12] Der Verbraucher muss über seine Möglichkeiten, die Funktionen des Smart Meter und die damit einhergehenden Datenverarbeitungsprozesse informiert werden und Erklärungen zur Nutzung erhalten.

Von Bedeutung ist die Wahlfreiheit des Letztverbrauchers. So darf z. B. keine Verpflichtung bestehen, einen bestimmten Tarif zu wählen oder an der Zählerstandsgangmessung teilzunehmen.

V. Datensicherheit und technischer Datenschutz

Vorzusehen sind organisatorische und technische Regelungen sowie Maßnahmen, mit denen ein unzulässiger Umgang mit den anfallenden Daten verhindert wird. Die Vertraulichkeit, Integrität, Intervenierbarkeit, Transparenz, Nichtverkettbarkeit sowie Verfügbarkeit[13] der Daten muss dabei sichergestellt werden. Smart Meter sollen nicht von außen frei zugänglich sein und enge Profile für den berechtigten Zugang zu den Daten müssen definiert werden. Anhaltspunkte hierzu bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des BSI, wie beispielsweise die Regelung des Zugriffs über Berechtigungsprofile oder das Push-Verfahren, bei dem eine Kommunikationsverbindung immer durch das Gateway initiiert wird.

Hohe technische Standards sind vorzusehen, welche die personenbezogenen Daten sowohl bei der Speicherung als auch bei der Übermittlung schützen. Die Manipulationssicherheit der Smart Meter muss gewährleistet werden. Der Schutz kann insbesondere dadurch erreicht werden, dass nur ein minimierter Zugriff auf die Daten erlaubt ist, alle beteiligten Akteure die Schutzstandards erfüllen und eine sichere Vernichtung der Daten am Ende der Nutzungsdauer erfolgt.

VI. Privacy by Design[14]

Die Gewährleistung des Datenschutzes muss bereits bei der Konzeption und Gestaltung der technischen Systeme erfolgen. Von Anfang an müssen die Datenverarbeitungssysteme ein integriertes Datenschutzmanagementsystem enthalten und technische Maßnahmen der Datensicherheit vorsehen. Der Letztverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen. Für die Sicherstellung dieser Anforderungen bedarf es rechtlich verbindlicher Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz. Anhaltspunkte für die festzuschreibenden Kriterien liefern das Schutzprofil des BSI sowie die Technische Richtlinie.

[12] Die Verarbeitung solcher Informationen kann durch eine Einwilligung des Letztverbrauchers gerechtfertigt sein, vgl. unter 2.
[13] Hierbei handelt es sich um die Schutzziele, die im Rahmen des § 9 BDSG zu beachten sind.
[14] Zu den Grundsätzen des Privacy by Design vgl. z. B.: Ann Cavoukian, Privacy by Design, Strong privacy protection – Now, and well into the future, http://www.ipc.on.ca/images/Resources/PbDReport.pdf.

4.2 Bewertungsmethodik Datenschutzbedarf der Use Cases

Use Cases werden typischerweise in unsicheren Planungs- und Entscheidungssituationen genutzt, in denen viele Details offen bleiben müssen. Sie sind im Detail unvollständig und weisen einen hohen Anteil an Annahmen aus.

Im Folgenden werden Use Cases für Smart Metering anhand definierter Schutzziele der Datensicherheit und des Datenschutzes beschrieben und bewertet. Aus der Bewertung lässt sich ein Datenschutzbedarf der betroffenen Daten ableiten. Zunächst wird die Bewertungssystematik vorgestellt.

Der **Datenschutzbedarf**, der sich aus der Bewertung der Use Cases für die betroffenen Daten ergibt, wird mit der dreiteiligen Bewertungsskala **normal**, **hoch** und **sehr hoch** dargestellt.[15] Fragen des Schutzbedarfes stellen sich regelmäßig im Bereich der Datensicherheit. Im Unterschied zu Betrachtungen der Datensicherheit stehen jedoch nicht die technisch-organisatorischen Risiken einer Stelle, sondern die Risiken der Personen, welche von einem personenbezogenen Verfahren betroffen sind, im Vordergrund. Entsprechend muss die Definition der **Datenschutzbedarfskategorien** gegenüber dem methodischen Vorbild angepasst werden:

- Die Datenschutzbedarfskategorie **normal** bedeutet, dass die Schadensauswirkungen begrenzt und überschaubar sind. Eingetretene Schäden für den Betroffenen sind relativ leicht zu heilen.
- Die Datenschutzbedarfskategorie **hoch** ist dann angemessen gewählt, wenn die Schadensauswirkungen von einer Person als beträchtlich eingeschätzt werden.
- Die Datenschutzbedarfskategorie **sehr hoch** bleibt den Fällen vorbehalten, in denen Schadensauswirkungen ein existentiell bedrohliches, katastrophales Ausmaß erreichen können. Die Auswirkungen auf eine Person oder einen Haushalt mit mehreren Personen lassen sich typischen Szenarien zuordnen, etwa: Verstoß gegen Normen (Gesetz/Vertrag), Beeinträchtigung der auf den Lebensalltag bezogenen Funktionalität, Beeinträchtigung des Vertrauensverhältnisses zur Organisation, finanzielle Auswirkungen sowie unmittelbare Auswirkungen auf eine Person im Hinblick auf Folgen für ihre Selbstbestimmtheit im Sinne von Bürger- und Kundenrechten sowie für die körperliche Unversehrtheit.

Diese Datenschutzbedarfsfeststellungen sind anzuwenden auf sechs elementare **Schutzziele** des Datenschutzes, nämlich **Verfügbarkeit, Integrität, Vertraulichkeit** sowie **Transparenz**, **Intervenierbarkeit** und **Nichtverkettbarkeit**. Die ersten drei genannten Schutzziele stellen die bewährten Schutzziele der Datensicherheit dar, wie sie für die Formulierung des Schutzprofils herangezogen wurden. Die weiteren Schutzziele ergänzen diese aus Datenschutzsicht um die Kontroll- und Prüffähigkeit

[15] Vgl. BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise, S.49ff, https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30748/standard_1002_pdf.pdf .

von Verfahren, die technisch-organisatorische Umsetzung der Betroffenenrechte und den Nachweis eines kontrollierten Änderungsmanagements auf Seiten der Stelle, die personenbezogene Daten verarbeitet. Sie muss nachweisen, dass sie die sechs Schutzziele berücksichtigt, indem sie ihr Datenschutzmanagement entsprechend ausrichtet. Dies gilt insbesondere für die Umsetzung der Auskunfts- und Widerspruchsrechte der Betroffenen und für die Prüftätigkeiten von Aufsichtsbehörden.

Ein ganz wesentliches Element ist zudem die enge, kausale Verknüpfung von Schutzzielen und den daraus folgenden Maßnahmen. Die sechs Schutzziele sind mit sechs typischen Maßnahmenbündeln gekoppelt:

- **Verfügbarkeit** wird typischerweise durch Redundanz, etwa durch Vorhalten von Parallelsystemen, Datenbeständen, durch Reparaturstrategien sowie Vertretungsregeln sichergestellt. Generell gilt, dass der Datenschutzbedarf für das Beliefern mit Energie als „sehr hoch“ einzuschätzen ist. Soweit die Nichtverfügbarkeit von Daten zu einer Nichtversorgung von Strom führt, ist der Schutzbedarf als sehr hoch zu bewerten. Ein Leben ohne stabile Stromversorgung eines Haushalts ist praktisch nicht möglich. Dieser Datenschutzbedarf gilt als gesetzt und wird nachfolgend nicht weiter betrachtet.
- **Integrität**sverstöße werden beim Verarbeiten von Daten durch den Vergleich von Prüfsummen (Hashwerten) aufgedeckt. Bei Prozessen werden diese durch Abweichung der Ist-Werte von den abgestimmten und festgelegten Soll-Werten aufgezeigt. Das Gateway bietet Mechanismen für Hashwert-Vergleiche. Inwieweit Abweichungen von Soll-Werten automatisch zur Alarmierung führen, ist offen.
- Um die **Vertraulichkeit** von Daten und Prozessen zu sichern, verschlüsselt oder separiert man diese. Der Datenschutzbedarf „normal“ kann die Verschlüsselung von Daten erforderlich machen. Höhere Stufen der Vertraulichkeiten bedeuten dann vor allem eine stärkere Sicherung der Generierung und des Austausches von Schlüsseln, auch zur Integritätssicherung. Beim Smart Meter spielt die Sicherung der Vertraulichkeit insbesondere zum Schutz vor unbefugtem Zugriff auf Daten eine Rolle, etwa durch den Messstellenbetreiber oder den Verteilnetzbetreiber.
- **Transparenz** beinhaltet, dass die Umsetzung der Schutzziele nachvollziehbar geprüft werden kann. Dies kann durch das technische System selbst oder durch Nachweise der verantwortlichen Stelle erfolgen. Transparenz muss sowohl gegenüber dem Letztverbraucher als auch den Aufsichtsbehörden gewahrt sein. Der Datenschutzbedarf „normal“ bedeutet dabei, dass sämtliche Komponenten, Schnittstellen und Datenstrukturen der beteiligten IT-Systeme spezifiziert werden. Die Maßnahmen zur Informationssicherheit müssen spezifiziert und mit ihren Konfigurationen im Produktionsbetrieb dokumentiert sein. Sich verändernde System- und Prozesszustände sind ebenfalls zu protokollieren. Wird der Datenschutzbedarf der Transparenz höher eingestuft, bedeutet das in der Regel, dass die Protokollierung sicherheitstechnisch besser abge-

sichert werden muss. Dies kann zur Folge haben, dass ein dedizierter Protokollierungsserver betrieben werden muss, damit eine Systemadministration revisionsfest kontrolliert werden kann.

- **Intervenierbarkeit** wird mit einem gesicherten Zugriff auf den Datenbestand durch den Letztverbraucher oder durch ein gesichertes Veränderungsmanagement operationalisiert. Der Datenschutzbedarf „normal“ bedeutet typischerweise, dass der Betroffene einen gesicherten Ansprechpartner auf Seiten der verantwortlichen Stelle haben muss. Ein höherer Datenschutzbedarf führt dazu, dass eine Stelle nachweislich Datenbestände, Datenstrukturen, IT-Systeme und Prozesse jederzeit in einem gesicherten Change-Management ändern kann. Auch kann bei erhöhtem Datenschutzbedarf die Intervenierbarkeit auf Seiten des Betroffenen auf die Implementierung eines „Eingriffsankers“ zur Unterbindung der Kommunikation in berechtigten Fällen hinauslaufen, der sich unter Kundenkontrolle befindet.[16] Eine solche Maßnahme bildet auf technisch-organisatorischer Ebene das Analogon zu einer Einwilligungsregelung.
- **Nichtverkettbarkeit** wird umgesetzt in Fällen, bei denen der Empfänger von Daten nicht zwingend die persönlichen Daten des Absenders kennen muss. Auch kann mit technischen Verfahren, die eine enge Zweckbindung umsetzen, erreicht werden, dass keine weiteren Interessen der datenverarbeitenden Stelle entstehen können. Bei der Feststellung eines normalen Datenschutzbedarfs ist die Datenstruktur so umzusetzen, dass diese eng am Zweck ausgerichtet ist. Auch ist eine organisatorische Teilung der Rollen nach Aufgabengebiet vorzunehmen. Bei hohem Datenschutzbedarf sind für Daten eine Pseudonymisierung und Mandantentrennung notwendig. Bei sehr hohem Datenschutzbedarf sind eine Anonymisierung von Daten sowie eine physikalische Trennung von Systemen erforderlich. In Bezug auf Smart Metering bedeutet die Feststellung eines hohen Datenschutzbedarfs, dass nicht mehrere Aufgaben von einer Organisationseinheit übernommen werden dürfen.

Entsprechend der BSI-Grundschutzmethodik gelten neben diesem Grundkonstrukt aus der Datenschutzbedarfsfeststellung, dem Ausweisen von Schutzzielen und den entsprechend abgeleiteten Maßnahmen zum Erreichen der Schutzziele auch andere methodische Grundsätze, die zu beachten sind:

- Das **Maximumprinzip** besagt, dass in einem System der höchste festgestellte Datenschutzbedarf einer Komponente für das gesamte System gilt.
- Der **Kumulationseffekt** betrifft die Eigenschaft von Systemen, dass z.B. ein normaler Datenschutzbedarf für viele Komponenten in der Gesamtheit zu einem höheren Datenschutzbedarf führen kann. Gegenseitige Abhängigkeiten sind zu beachten.

[16] Vgl. z.B. § 31a Abs. 2 Berliner Datenschutzgesetz (Prinzip „rote Lampe“/„roter Knopf“).

- Wichtig ist zudem das **Vererbungsprinzip**, wonach der Datenschutzbedarf von Daten an IT-Systeme, Räume und Prozesse, die diese Daten verwenden, vererbt wird.

Daran sei nur knapp erinnert, es kann an dieser Stelle aber nicht weiter darauf eingegangen werden.[17]

4.3 Bewertung der Use Cases

Die Bewertung erfolgt nach vorgestellter Methodik. Folgende wichtige Anmerkungen vorab:

- Alle Daten, die mit einem Smart Meter erhoben werden, sind personenbezogen, unabhängig davon, ob es sich um technische Daten handelt. Die Sensitivität der Daten ist zwar verschieden, so dass daraus ein unterschiedlicher Datenschutzbedarf resultieren kann. Dies ändert aber nichts am Personenbezug. Nach dem Bundesdatenschutzgesetz handelt es sich auch bei personenbeziehbaren Daten um personenbezogene Daten.
- Die Bewertung des Datenschutzbedarfes erfolgt auch für die bewährten Schutzziele der Datensicherheit aus der Perspektive der betroffenen Personen, deren Datenschutz auch über die Schutzziele der Datensicherheit sichergestellt werden soll.
- Der Letztverbraucher hat die Datensouveränität über das Smart Meter inne, so dass dieser immer als Akteur aufgeführt wird, wenn Daten vom Smart Meter erhoben, übermittelt oder verarbeitet werden.
- Der Datenfluss wird aus energiewirtschaftlicher Perspektive nicht vollständig abgebildet und betrachtet nur die Datenflüsse, bei welchen Smart Meter Daten übermittelt werden. Beispielsweise werden die Datenflüsse zwischen den unterschiedlichen Akteuren, die originär nicht mit Smart Meter erhoben werden wie beispielsweise Vertragsdaten, nicht betrachtet, da dies den Rahmen der Orientierungshilfe überschreiten würde.
- Das Intelligente Energienetz wird nicht betrachtet. Wenn Smart Meter die Steuerungsdaten für das Intelligente Netz bereitstellen, werden diese als Use Cases aufgeführt, allerdings ohne die Konsequenzen aus der Datenbereitstellung zu betrachten.
- Der Datenschutzbedarf insgesamt resultiert nach dem Maximumprinzip aus den Schutzzielen.
- Eine Begründung des Datenschutzbedarfes eines Schutzzieles erfolgt nur für „Hoch“ und „Sehr hoch“. In diesen Fällen werden dem Schutzniveau entsprechende Maßnahmen benannt.

[17] Vgl. BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise, S. 54ff.

4.3.1. Gestaltung Vertragsverhältnis

Use Case 4.3.1-1: Beendigung des Energielieferungsvertrages

Use Case	**Beendigung des Energielieferungsvertrages**	
Ziel	Übermittlung der Abrechnungsdaten für die Endabrechnung, Löschen aller Daten des Energielieferanten als Kommunikationspartner des Gateways	
Akteure	Letztverbraucher, Energielieferant, Gateway-Administrator	
Prozessbeschreibung	Die Abrechnungsdaten für die Endabrechnung werden ein letztes Mal versendet, der Gateway-Administrator unterbricht zum Kündigungsdatum die Kommunikation mit dem Energielieferanten, löscht die Tarif- und Berechtigungsprofile und alle weiteren Daten des Energielieferanten (Zertifikate).	
Daten	Abrechnungsdaten (Verbrauch), Zertifikate, Schlüssel, Berechtigungsprofildaten	
Datenfluss	Letztverbraucher → Energielieferant Gateway-Administrator →Letztverbraucher	
Anmerkungen	Es wird davon ausgegangen, dass die im Schutzprofil vorgesehene sternförmige Kommunikation, die über Tarif- und Berechtigungsprofile ermöglicht wird, in Anspruch genommen wird und dadurch ein direkter Datenfluss von Letztverbraucher (Smart Meter) zu Energielieferant stattfindet. Datenflüsse zwischen Gateway-Administrator und Energielieferanten, die zur Umsetzung der Beendigung des Energielieferungsvertrages notwendig sind, werden bewusst nicht betrachtet, da diese Daten nicht mit Smart Meter, sondern konventionell erhoben wurden (beispielsweise über Verträge).	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	
Integrität	Hoch	Änderungen im Bereich des Zertifikatsmanagements, Berechtigungsprofile etc.
Vertraulichkeit	Hoch	Zugriff des Gateway-Administrators, dieser nimmt eine zentrale Rolle mit umfangreichen Rechten ein, so dass die Vertraulichkeit sichergestellt werden muss
Transparenz	Hoch	Nachvollziehbarkeit der Kündigung und deren Umsetzung (insb. Löschung des Berechtigungsprofils)
Intervenierbarkeit	Normal	
Nichtverkettbarkeit	Normal	
Maßnahmen	Der Letztverbraucher muss über die vollzogene Kündigung informiert werden. Ein Nachweis über ein gesichertes Änderungsmanagement nach Stand der Organisationslehre (ITIL, ISO 27001, ISO 29100/1001, BSI-Grundschutz) zur Sicherung der Transparenz und Integrität muss beim Energielieferanten und Gateway-Administrator vorhanden sein. Der Letztverbraucher braucht eine zentrale Anlaufstelle, um im Zweifelsfall schnell intervenieren zu können und seine Rechte einzufordern.	

	Verschlüsselte Kommunikationskanäle und Ende-zu-Ende-Verschlüsselung mit Zertifizierung nach Stand der Technik. Zertifizierungsverfahren für den Gateway-Administrator ist erforderlich.

Use Case 4.3.1-2: Vertragsabschluss mit berechtigtem Marktteilnehmer

Use Case	**Vertragsabschluss mit berechtigtem Marktteilnehmer**	
Ziel	Einrichten aller Daten des Energielieferanten als Kommunikationspartner des Gateways	
Akteure	Letztverbraucher, Energielieferant oder berechtigter Marktteilnehmer, Gateway-Administrator	
Prozessbeschreibung	Der Letztverbraucher schließt einen Vertrag mit einem Energielieferanten oder einem weiteren berechtigten Marktteilnehmer ab. Der Gateway-Administrator prüft das Zertifikat des Energielieferanten oder berechtigten Marktteilnehmers, installiert dieses im Gateway und legt ein neues Berechtigungsprofil an. Die Aktivitäten werden im Kunden-Log des Gateways protokolliert.	
Daten	Berechtigungsprofildaten, Zertifikate, Schlüssel	
Datenfluss	Letztverbraucher → Energielieferant Gateway-Administrator → Letztverbraucher	
Anmerkungen	Es wird davon ausgegangen, dass die im Schutzprofil vorgesehene sternförmige Kommunikation, die über Tarif- und Berechtigungsprofile ermöglicht wird, in Anspruch genommen wird und dadurch ein direkter Datenfluss von Letztverbraucher (Smart Meter) zum berechtigten Marktteilnehmer stattfindet. Die Datenflüsse zwischen Gateway-Administrator und berechtigtem Marktteilnehmer, die zur Umsetzung des Vertragsabschlusses notwendig sind, werden bewusst nicht betrachtet, da diese Daten nicht mit Smart Meter, sondern konventionell erhoben wurden (beispielsweise über Verträge).	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Sehr hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	
Integrität	Sehr hoch	Aufspielen des neuen Zertifikates, Berechtigungsprofile, Schlüssel durch Gateway-Administrator
Vertraulichkeit	Hoch	Zugriff des Gateway-Administrators, dieser nimmt eine zentrale Rolle mit umfangreichen Rechten ein, so dass die Vertraulichkeit sichergestellt werden muss
Transparenz	Hoch	Nachvollziehbarkeit des Wechsels durch Letztverbraucher, Überprüfbarkeit des Berechtigungsprofils
Intervenierbarkeit	Hoch	Einschreiten gegen falsche Berechtigungsprofile muss möglich sein
Nichtverkettbarkeit	Normal	
Maßnahmen	Ein Nachweis über ein gesichertes Änderungsmanagement nach Stand der Organisationslehre (ITIL, ISO 27001, ISO 29100/1001, BSI-Grundschutz) zur Sicherung der Transparenz und Integrität muss beim Energielieferanten und Gateway-Administrator	

	vorhanden sein. Der Letztverbraucher braucht eine zentrale Anlaufstelle, um im Zweifelsfall schnell intervenieren zu können und seine Rechte einzufordern. Der Letztverbraucher muss über die Umsetzung des Vertrages informiert werden. Die Aktivitäten werden im Kunden-Log des Gateways protokolliert. Verschlüsselte Kommunikationskanäle und Ende-zu-Ende-Verschlüsselung und Integritätssicherung durch Signaturverfahren mit Zertifizierung nach Stand der Technik. Zertifizierungsverfahren für den Gateway-Administrator ist erforderlich.

Use Case 4.3.1-3: Wechsel des Energielieferanten

Use Case	**Wechsel des Energielieferanten**	
Ziel	Übermittlung der Abrechnungsdaten für die Endabrechnung, Löschen aller Daten des alten Energielieferanten als Kommunikationspartner des Gateways, Einrichten der Daten für den neuen Energielieferanten	
Akteure	Letztverbraucher, alter Energielieferant, neuer Energielieferant, Gateway-Administrator	
Prozessbeschreibung	Der Letztverbraucher wechselt den Energielieferanten auf eigene Veranlassung. Die Abrechnungsdaten für die Endabrechnung werden ein letztes Mal versendet, der Gateway-Administrator unterbricht zum Wechseldatum die Kommunikation mit dem alten Energielieferanten, löscht das Berechtigungsprofil und alle weiteren Daten des alten Energielieferanten (Zertifikate). Der Gateway-Administrator prüft das Zertifikat des neuen Energielieferanten, installiert dieses im Gateway und legt ein neues Berechtigungsprofil an. Die Aktivitäten werden im Kunden-Log des Gateways protokolliert.	
Daten	Abrechnungsdaten (Verbrauch), Zertifikate, Schlüssel, Berechtigungsprofildaten	
Datenfluss	Letztverbraucher → neuer Energielieferant Letztverbraucher → alter Energielieferant Gateway-Administrator → Letztverbraucher	
Anmerkungen	Es wird davon ausgegangen, dass die im Schutzprofil vorgesehene sternförmige Kommunikation, die über Tarif- und Berechtigungsprofile ermöglicht wird, in Anspruch genommen wird und dadurch ein direkter Datenfluss von Letztverbraucher (Smart Meter) zum Energielieferanten stattfindet. Die Datenflüsse zwischen Gateway-Administrator und Energielieferanten, die zur Umsetzung des Wechsels notwendig sind, werden bewusst nicht betrachtet, da diese Daten nicht mit Smart Meter, sondern konventionell erhoben wurden (beispielsweise über Verträge).	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Sehr hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	
Integrität	Sehr hoch	Aufspielen des neuen Zertifikates, Berechtigungsprofile, Schlüssel durch Gateway-Administrator
Vertraulichkeit	Hoch	Zugriff des Gateway-Administrators, dieser nimmt eine zentrale Rolle mit umfangreichen Rechten ein, so dass die Vertraulichkeit sichergestellt werden muss
Transparenz	Hoch	Nachvollziehbarkeit des Wechsels durch Letztverbraucher, Überprüfbarkeit des Berechtigungsprofils
Intervenier-	Hoch	Einschreiten gegen falsche Berechtigungsprofile muss möglich sein

barkeit		
Nichtverkett-barkeit	Normal	
Maßnahmen	Ein Nachweis über ein gesichertes Änderungsmanagement nach Stand der Organisationslehre (ITIL, ISO 27001, ISO 29100/1001, BSI-Grundschutz) zur Sicherung der Transparenz und Integrität muss beim Energielieferanten und Gateway-Administrator vorhanden sein. Der Letztverbraucher braucht eine zentrale Anlaufstelle, um im Zweifelsfall schnell intervenieren zu können und seine Rechte einzufordern. Der Letztverbraucher muss über den vollzogenen Wechsel informiert werden. Die Aktivitäten werden im Kunden-Log des Gateways protokolliert. Verschlüsselte Kommunikationskanäle und Ende-zu-Ende-Verschlüsselung und Integritätssicherung durch Signaturverfahren mit Zertifizierung nach Stand der Technik. Zertifizierungsverfahren für den Gateway-Administrator ist erforderlich.	

Use Case 4.3.1-4: Tarifwechsel

Use Case	**Tarifwechsel**	
Ziel	Technische Umsetzung des Tarifwechsels im Gateway	
Akteure	Letztverbraucher, Energielieferant, Gateway-Administrator	
Prozessbeschreibung	Der Letztverbraucher vereinbart mit seinem Energielieferanten einen neuen Tarif oder eine neue Abrechnungsart. Der Gateway-Administrator ändert die Parameter des Tarifprofils zum festgelegten Datum.	
Daten	Tarifprofildaten	
Datenfluss	Letztverbraucher → Energielieferant Gateway-Administrator → Letztverbraucher	
Anmerkungen	Es wird davon ausgegangen, dass die im Schutzprofil vorgesehene sternförmige Kommunikation, die über Tarif- und Berechtigungsprofile ermöglicht wird, in Anspruch genommen wird und dadurch ein direkter Datenfluss von Letztverbraucher (Smart Meter) zu Energielieferant stattfindet. Die Datenflüsse zwischen Gateway-Administrator und dem Energielieferanten, die für den Tarifwechsel notwendig sind, werden bewusst nicht betrachtet, da diese Daten nicht mit Smart Meter, sondern konventionell erhoben wurden (beispielsweise über Verträge).	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	
Integrität	Normal	
Vertraulichkeit	Hoch	Zugriff des Gateway-Administrators
Transparenz	Hoch	Änderungen an Tarifprofilen müssen für den Letztverbraucher nachvollziehbar sein; Letztverbraucher muss nachvollziehen können, dass ein Zugriff und welche Änderungen stattgefunden haben
Intervenier-	Normal	

barkeit		
Nichtverkett-barkeit	Normal	
Maßnahmen	Ein Nachweis über ein gesichertes Änderungsmanagement nach Stand der Organisationslehre (ITIL, ISO 27001, ISO 29100/1001, BSI-Grundschutz) zur Sicherung der Transparenz und Integrität muss beim Energielieferanten und Gateway-Administrator vorhanden sein. Der Letztverbraucher braucht eine zentrale Anlaufstelle, um im Zweifelsfall schnell intervenieren zu können und seine Rechte einzufordern. Der Letztverbraucher muss über den vollzogenen Wechsel informiert werden. Die Aktivitäten werden im Kunden-Log des Gateways protokolliert. Verschlüsselte Kommunikationskanäle und Ende-zu-Ende-Verschlüsselung mit Zertifizierung nach Stand der Technik. Zertifizierungsverfahren für den Gateway-Administrator ist erforderlich.	

Use Case 4.3.1-5: Informationspflichten bei ungültigen Zertifikaten

Use Case	**Informationspflichten bei ungültigen Zertifikaten**	
Ziel	Sicherer Betrieb des Gateways bei Bekanntwerden eines Angriffes auf die oberste Zertifizierungsstelle	
Akteure	Letztverbraucher, Gateway-Administrator	
Prozessbeschreibung	Es wird ein erfolgreicher Angriff auf die oberste Zertifizierungsstelle bekannt. Alle oder eine bestimmte Anzahl der bisher ausgestellten Zertifikate sind nicht mehr vertrauenswürdig und werden ausgetauscht. Die Aktivitäten werden im Kunden-Log des Gateways protokolliert.	
Daten	Zertifikate, Schlüssel	
Datenfluss	Gateway Administrator → Letztverbraucher	
Anmerkungen		
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	
Integrität	Hoch	Austausch Zertifikate
Vertraulichkeit	Hoch	Zugriff Gateway-Administrator
Transparenz	Hoch	Fehler müssen nachvollziehbar sein. Korrektur auch. Letztverbraucher muss nachvollziehen können, sofern falsche Zertifikate im Einsatz waren und mit welchen Akteuren (Zertifikatsinhabern) kommuniziert worden ist.
Intervenierbarkeit	Normal	
Nichtverkett-	Normal	

barkeit		
Maßnahmen	Verschlüsselte Kommunikationskanäle und Ende-zu-Ende-Verschlüsselung und Integritätssicherung durch Signaturverfahren mit Zertifizierung nach Stand der Technik. Zertifizierungsverfahren für den Gateway-Administrator ist erforderlich. Ein Nachweis über ein gesichertes Änderungsmanagement nach Stand der Organisationslehre (ITIL, ISO 27001, ISO 29100/1001, BSI-Grundschutz) zur Sicherung der Transparenz und Integrität muss beim Energielieferanten und Gateway-Administrator vorhanden sein. Der Letztverbraucher muss über falsche Zertifikate informiert werden und Kommunikationsvorgänge mit Zertifikatsinhabern nachvollziehen können. Tätigkeiten zur Korrektur müssen vom Gateway-Administrator dargestellt werden. Die Tätigkeiten müssen auch im Kunden-Log abgerufen werden können. Letztverbraucher ist Herrscher des Verfahrens. Er hat Datenhoheit. Kommunikation kann durch ihn unterbrochen werden, relevante Daten werden im Gateway zwischengespeichert. Der korrekte Umgang mit Zertifikaten ist maßgeblich für ein datenschutzgerechtes Smart Metering. Organisation darf Versorgung bei Angriff nicht unterbrechen, kein automatisches Abschalten.	

Use Case 4.3.1-6: Einrichten Zugangskonto für Letztverbraucher im Gateway

Use Case	**Einrichten Zugangskonto für Letztverbraucher im Gateway**	
Ziel	Mandantentrennung im Gateway durch Einrichten eines abgetrennten Bereichs für jeden Letztverbraucher	
Akteure	Letztverbraucher, Gateway-Administrator	
Prozessbeschreibung	Der Gateway Administrator richtet auf dem Gateway ein Zugangskonto für den Letztverbraucher ein. Die Aktivitäten werden im System-Log protokolliert und sind für den Letztverbraucher im Kunden-Log nachvollziehbar. Nach erfolgreichem Einrichten des Zugangskontos erhält der Letztverbraucher eine Mitteilung.	
Daten	Letztverbrauchercredentials	
Datenfluss	Gateway-Administrator → Letztverbraucher	
Anmerkungen	Die Datenflüsse, die für das Einrichten eines Zugangskontos notwendig sind und die ohne direkte Beteiligung des Letztverbrauchers (Smart Meter) ablaufen, werden bewusst nicht betrachtet, da diese Daten nicht mit Smart Meter, sondern konventionell erhoben wurden (beispielsweise über Verträge).	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	
Integrität	Hoch	Aufspielen der Letztverbrauchercredentials
Vertraulichkeit	Hoch	Zugriff des Gateway-Administrators
Transparenz	Hoch	Nachvollziehbarkeit des erfolgreichen Einrichtens
Intervenier-	Hoch	Einschreiten gegen falsches Zugangskonto muss möglich sein

barkeit		
Nichtverkett-barkeit	Normal	
Maßnahmen	Der Letztverbraucher braucht eine zentrale Anlaufstelle, um gegen falsch eingerichtete Zugangskonten intervenieren zu können. Der Letztverbraucher muss über das Einrichten des Zugangskontos informiert werden. Die Aktivitäten werden im Kunden-Log des Gateways protokolliert. Ein Nachweis über ein gesichertes Änderungsmanagement nach Stand der Organisationslehre (ITIL, ISO 27001, ISO 29100/1001, BSI-Grundschutz) zur Sicherung der Transparenz und Integrität muss beim Energielieferanten und Gateway-Administrator vorhanden sein. Verschlüsselte Kommunikationskanäle und Ende-zu-Ende-Verschlüsselung und Integritätssicherung durch Signaturverfahren mit Zertifizierung nach Stand der Technik. Zertifizierungsverfahren für den Gateway-Administrator ist erforderlich.	

Use Case 4.3.1-7: Löschen des Zugangskontos des Letztverbrauchers

Use Case	**Löschen des Zugangskontos des Letztverbrauchers**	
Ziel		
Akteure	Letztverbraucher, Gateway-Administrator	
Prozessbeschreibung	Der Gateway Administrator löscht auf dem Gateway das Zugangskonto für den Letztverbraucher. Die Aktivitäten werden im System-Log protokolliert. Nach erfolgreichem Löschen des Zugangskontos erhält der Letztverbraucher eine Mitteilung.	
Daten	Letztverbrauchercredentials (bzw. Löschbefehl für die Letztverbrauchercredentials)	
Datenfluss	Gateway-Administrator → Letztverbraucher	
Anmerkungen	Die Datenflüsse, die für das Löschen eines Zugangskontos notwendig sind und die ohne direkte Beteiligung des Letztverbrauchers (Smart Meter) ablaufen, werden bewusst nicht betrachtet, da diese Daten nicht mit Smart Meter, sondern konventionell erhoben wurden (beispielsweise über Verträge).	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	
Integrität	Normal	
Vertraulichkeit	Hoch	Zugriff des Gateway-Administrators
Transparenz	Hoch	Nachvollziehbarkeit des erfolgreichen Löschens
Intervenierbarkeit	Normal	
Nichtverkett-	Normal	

barkeit		
Maßnahmen	Der Letztverbraucher muss über das erfolgreiche Löschen des Zugangskontos informiert werden. Ein Nachweis über ein gesichertes Änderungsmanagement nach Stand der Organisationslehre (ITIL, ISO 27001, ISO 29100/1001, BSI-Grundschutz) zur Sicherung der Transparenz und Integrität muss beim Energielieferanten und Gateway-Administrator vorhanden sein.	

4.3.2. Messen

Use Case 4.3.2-1: Abrechnung Netzentgelte gegenüber Netznutzer

Use Case	**Abrechnung Netzentgelte gegenüber Netznutzer**	
Ziel	Abrechnung der Netzentgelte für die Netznutzung zwischen Netznutzer (in der Regel der Energielieferant) und Netzbetreiber	
Akteure	Letztverbraucher, Netznutzer (Energielieferant), Netzbetreiber	
Prozessbeschreibung	Einmal pro Jahr (bzw. Monat) erfolgt die Abrechnung der Netzentgelte zwischen Netzbetreiber und Netznutzer. Der Netznutzer muss Netzentgelte für die Netznutzung durch den gelieferten Strom bezahlen, so dass Verbrauchsdaten pro Jahr (bzw. Monat) übermittelt werden.	
Daten	Verbrauch pro Jahr (bzw. Monat)	
Datenfluss	Letztverbraucher → Netzbetreiber → Energielieferant (Netznutzer)	
Anmerkungen	Die Abrechnung der Netzentgelte zwischen Netzbetreiber und Netznutzer erfolgt derzeit pro Entnahmestelle (Zähler). Inwieweit der Haushaltebezug erforderlich ist, ist fraglich, kumulierte Messwerte erscheinen ausreichend. Sofern Verbrauchsdaten nur einmal im Jahr als Jahreswert übermittelt werden, wird der Haushaltebezug nicht kritisch bewertet. Werden die Verbrauchsdaten feingranular erhoben und übermittelt, wird der Haushaltebezug kritisch gesehen.	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Normal	Für den Fall, dass nur einmal im Jahr der Jahreswert übermittelt wird
Verfügbarkeit	Normal	
Integrität	Normal	
Vertraulichkeit	Normal	
Transparenz	Normal	
Intervenierbarkeit	Normal	
Nichtverkettbarkeit	Normal	

Maßnahmen	Bei Übermittlung eines aggregierten Jahreswertes pro Haushalt ist der Use Case aus Sicht des Datenschutzes unkritisch. Sofern Erhebung/Übermittlung häufiger geplant ist, ist eine Zuordnung zum Energielieferanten über ein Pseudonym für die Zwecke ausreichend, ein Haushaltebezug ist nicht notwendig.

Use Case 4.3.2-2: Ausweisen Netzentgelte gegenüber Letztverbraucher

Use Case	**Ausweisen Netzentgelte gegenüber Letztverbraucher**	
Ziel	Datenbereitstellung zum Ausweisen des Anteils der Netzentgelte auf der Rechnung des Letztverbrauchers	
Akteure	Letztverbraucher, Energielieferant	
Prozessbeschreibung	Der Energielieferant erstellt für den Letztverbraucher die Rechnung und weist hier die Kosten verursacht durch Netzentgelte aus.	
Daten	Daten bereits durch Use Case 4.3.2-1 vorhanden	
Datenfluss	-	
Anmerkungen	Der Datenfluss von Verteilnetzbetreiber zu Bilanzkreisverantwortlichem wird bewusst nicht betrachtet, da davon ausgegangen wird, dass die Verbrauchsdaten derart aggregiert werden, dass es sich nicht mehr um personenbezogene Daten handelt. Sofern Netzentgelte zukünftig feingranularer ausgewiesen werden, folgende Anmerkung: Die Netzentgelte lassen sich aus den bereits vorhandenen Rechnungsdaten berechnen, wenn sich Verbrauch und Netzentgelt linear verhalten und alle Letztverbraucher das gleiche Netzentgelt bezahlen. Sofern der Letztverbraucher reduzierte Netzentgelte nach § 14a EnWG zahlt, ist zu prüfen, ob auch für diesen Fall eine Berechnung linear erfolgen kann.	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt		kein Datenfluss, daher auch keine Datenschutzbedarfsfeststellung notwendig
Verfügbarkeit		
Integrität		
Vertraulichkeit		
Transparenz		
Intervenierbarkeit		
Nichtverkettbarkeit		
Maßnahmen		

Use Case 4.3.2-3: Bilanzierung nach Zählerstandsgangmessung

Use Case	**Bilanzierung nach Zählerstandsgangmessung**	
Ziel	Abrechnung bezogener sowie eingespeister Energie im Bilanzierungssystem	
Akteure	Letztverbraucher, Verteilnetzbetreiber, Übertragungsnetzbetreiber, Bilanzkreisverantwortlicher, Energielieferant	
Prozessbeschreibung	1) Der Verteilnetzbetreiber aggregiert für alle in seinem Netzgebiet befindlichen Zählpunkte die jeweiligen Messwerte zu Bilanzkreissummenzeitreihen. 2) Außerdem übersendet er an den jeweiligen Energielieferanten zu Kontrollzwecken die Einzelzeitreihen.	
Daten	Verbrauchsdaten pro Zeitintervall	
Datenfluss	1) Letztverbraucher -> Verteilnetzbetreiber -> Übertragungsnetzbetreiber -> Bilanzkreisverantwortlicher (aggregierte Bilanzkreissummenzeitreihen) 2) Letztverbraucher → (Verteilnetzbetreiber) → Energielieferant (Einzelzeitreihen)	
Anmerkungen	Dieser Use Case ist aus Sicht des Datenschutzes höchst problematisch, solange der Haushaltebezug gegeben ist. Ein Haushaltebezug ist für die Bilanzierung nicht erforderlich. Um eine bessere Abbildung des tatsächlichen Verbrauchs und der tatsächlichen Einspeisung im Bilanzierungssystem zu erreichen und die statistischen Verfahren zu verbessern, genügen nicht-haushaltbeziehbare Messungen an Ortsnetzstationen. Es ist darauf hinzuweisen, dass Daten, die per Zählerstandsgangmessung für die Bilanzierung erhoben wurden, nur für den Zweck verwendet werden dürfen, für welche sie ursprünglich erhoben wurden (Zweckbindung). Verbrauchsdaten, die typischerweise im 15-Minuten Takt erhoben werden, sind hoch sensibel und ermöglichen eine Profilbildung. Dies gilt unabhängig davon, ob es sich um Vergangenheitswerte oder Echtzeitwerte handelt. Das Schutzprofil für das Gateway beinhaltet nach Stand September 2011 eine lokale Verbrauchsvisualisierung und Tarifierung im Gateway, so dass eine externe Versendung von Verbrauchsdaten im 15-Minuten Takt technisch nicht erforderlich ist. Werden diese sensiblen Verbrauchsdaten im Rahmen der Zählerstandsgangmessung extern mit Haushaltebezug versendet, wird das bisher datenschutzfreundliche Konzept umgangen.	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Sehr hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen Prognosen mit hoch aufgelösten Verbrauchsdaten aus der Vergangenheit stellen einen essentiellen Eingriff in die informationelle Selbstbestimmung dar und sind regelungstechnisch fragwürdig.
Verfügbarkeit	Normal	
Integrität	Normal	
Vertraulichkeit	Sehr hoch	Sensible Verbrauchsdaten
Transparenz	Hoch	Letztverbraucher muss Datenübermittlung nachvollziehen können
Intervenierbarkeit	Sehr hoch	Letztverbraucher muss Einwirkungsmöglichkeiten haben, da die Daten sehr sensibel sind.
Nichtverkettbarkeit	Sehr hoch	Verbrauchsdaten sind feingranular und können zu umfangreichen Profilen verkettet werden.

Maßnahmen	Maßnahmen werden nicht benannt, da noch viele Punkte offen sind. Ist aus Datenschutzsicht höchst problematisch.

Use Case 4.3.2-4: Daten für Zu- und Abschalten von Lasten

Use Case	**Datenbereitstellung für Zu- und Abschalten von Lasten**	
Ziel	Zu- und Abschalten von unterbrechbaren Verbrauchseinrichtungen	
Akteure	Letztverbraucher, Netzbetreiber	
Prozessbeschreibung	Im 15-Minuten-Takt wird die Differenz zwischen Einspeisung und Verbrauch von Energie ermittelt. Sofern es hier Abweichungen gibt, wird mit Regelenergie ein Ausgleich geschaffen. Durch Zu- und Abschalten von unterbrechbaren Verbrauchseinrichtungen nach § 14a EnWG soll Regelenergie bereitgestellt werden.	
Daten	Einspeise- und Ausspeisemenge pro 15 Minuten	
Datenfluss	Letztverbraucher → Netzbetreiber	
Anmerkungen	Aus welchem Grund muss die Erhebung der Ein- und Ausspeisemenge im 15-Minuten-Takt erfolgen?	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	Betrachtung des Einzelhaushaltes aus Datenschutzsicht unkritisch
Integrität	Normal	Betrachtung des Einzelhaushaltes aus Datenschutzsicht unkritisch
Vertraulichkeit	Hoch	Rückschlüsse auf einzelne Geräte möglich (z.B. Bewegungsprofile bei Elektroauto)
Transparenz	Normal	
Intervenierbarkeit	Normal	
Nichtverkettbarkeit	Hoch	Profilbildung durch Verbrauchsdaten von unterbrechbaren Verbrauchseinrichtungen darf nicht ermöglicht werden
Maßnahmen	Verschlüsselte Kommunikationskanäle und Ende-zu-Ende-Verschlüsselung mit Zertifizierung nach Stand der Technik. Die Daten sind unmittelbar nach Auswertung zu löschen und dürfen nicht mit anderen Verbrauchsdaten verbunden und genutzt werden.	

4.3.3. Beliefern und Abrechnen

Use Case 4.3.3-1: Zentrale Tarifierung bei externem Marktteilnehmer

Use Case	**Zentrale Tarifierung bei externem Marktteilnehmer**	
Ziel	Zentrale Erstellung der Abrechnungsdaten bei externem Marktteilnehmer zur Tarifierung	
Akteure	Letztverbraucher, Energielieferant (bzw. Auftragsdatenverarbeiter)	
Prozessbeschreibung	Nach hinterlegtem Tarifprofil werden die Verbrauchsdaten pro Zeitintervall an den Energielieferanten gesendet. Dieser ordnet die Verbrauchsdaten Tarifzonen zu und erstellt damit die Abrechnungsdaten. Rechnungsdaten basieren auf Tarifdaten, die mit den Abrechnungsdaten verrechnet werden. Die eigentliche Rechnungserstellung erfolgt konventionell.	
Daten	Verbrauchsdaten pro Zeitintervall	
Datenfluss	Letztverbraucher → Energielieferant	
Anmerkungen	Es wird davon ausgegangen, dass die im Schutzprofil vorgesehene sternförmige Kommunikation, die über Tarif- und Berechtigungsprofile ermöglicht wird, in Anspruch genommen wird und dadurch ein direkter Datenfluss von Letztverbraucher (Smart Meter) zu Energielieferant stattfindet.	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Sehr hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen. Die Datenschutzbedarfsfeststellungen gelten nur für die Ermittlung und die Übertragung der Daten des Energieverbrauchs.
Verfügbarkeit	Normal	
Integrität	Normal	
Vertraulichkeit	Hoch	Sensible Daten
Transparenz	Hoch	Letztverbraucher muss nachvollziehen können, welche Daten aus welchem Grund an einen externen Empfänger versendet wurden.
Intervenierbarkeit	Normal	
Nichtverkettbarkeit	Sehr hoch	Verbrauchsdaten sind sensibel, Zweckbindung muss beachtet werden
Maßnahmen	Der Letztverbraucher muss darüber informiert werden, wer welche Daten zu welchem Zweck erhält, um dies überprüfen zu können. Gleiches gilt für die Modalitäten der Ablesung und Datenübermittlung sowohl im Vorfeld als auch jederzeit während des Betriebes. Die Aktivitäten werden im Kunden-Log des Gateways protokolliert. Verschlüsselte Kommunikationskanäle und Ende-zu-Ende-Verschlüsselung mit Zertifizierung nach Stand der Technik. Die Daten sind unmittelbar nach Erstellung der Abrechnungsdaten unter Beachtung der eich- und zivilrechtlichen Vorgaben beim Energieversorgungsunternehmen zu löschen und dürfen nicht mit anderen Verbrauchsdaten verbunden und genutzt werden. Im Übrigen gilt für die Verarbeitung der personenbezogenen Daten im normalen Geschäftsprozess das Bundesdaten-	

	schutzgesetz (BDSG).

Use Case 4.3.3-2: Dezentrale Tarifierung im Gateway

Use Case	**Dezentrale Tarifierung im Gateway**	
Ziel	Dezentrale Erstellung der Abrechnungsdaten im Gateway zur Tarifierung	
Akteure	Letztverbraucher, Energielieferant	
Prozessbeschreibung	Nach hinterlegtem Tarifprofil werden die Verbrauchsdaten im Gateway Tarifzonen zugeordnet und nach hinterlegtem Intervall aggregiert für jede Tarifzone an den Energielieferanten gesendet. Rechnungsdaten basieren auf Tarifdaten, die mit den Abrechnungsdaten verrechnet werden. Die eigentliche Rechnungserstellung erfolgt konventionell.	
Daten	Abrechnungsdaten (Verbrauch)	
Datenfluss	Letztverbraucher → Energielieferant	
Anmerkungen	Es wird davon ausgegangen, dass die im Schutzprofil vorgesehene sternförmige Kommunikation, die über Tarif- und Berechtigungsprofile ermöglicht wird, in Anspruch genommen wird und dadurch ein direkter Datenfluss von Letztverbraucher (Smart Meter) zu Energielieferant stattfindet.	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen. Die Datenschutzbedarfsfeststellungen gelten nur für die Ermittlung und die Übertragung der Abrechnungsdaten.
Verfügbarkeit	Normal	
Integrität	Normal	
Vertraulichkeit	Normal	Bis hoch, sofern zur Datenübermittlung ein kurzes Zeitintervall gewählt wird, da je nach Tarifgestaltung bei kürzeren Zeitintervallen sensible Verbrauchsdaten bekannt werden.
Transparenz	Hoch	Sensibilität der Verbrauchsdaten ist abhängig von Abrechnungsmodalitäten
Intervenierbarkeit	Normal	
Nichtverkettbarkeit	Normal	
Maßnahmen	Abrechnungsmodalitäten müssen klar nachvollziehbar sein, der Letztverbraucher muss darüber detaillierte Informationen erhalten. Das Gateway muss in der Lage sein, die dezentrale Tarifierung durchzuführen. **Die dezentrale Tarifierung im Gateway ist datenschutzfreundlich** und ermöglicht die Nutzung neuer Tarife, ohne detaillierte Verbrauchsprofile preisgeben zu müssen. Eine Lastenverschiebung wird nur dann möglich, wenn Letztverbraucher die neuen Tarife auch wirklich nutzen. Die dezentrale Tarifierung stellt dabei ein wesentliches Akzeptanzkriterium in der Bevölkerung dar, sofern die Letztverbraucher gezwungen werden, Verbrauchsprofile freizugeben, werden diese die neuen Tarife nicht nutzen.	

Use Case 4.3.3-3: Dezentrale Erstellung des Rechnungsbetrages im Gateway

Use Case	**Dezentrale Erstellung des Rechnungsbetrages im Gateway**	
Ziel	Bereitstellung der Rechnungsdaten durch das Gateway	
Akteure	Letztverbraucher, Energielieferant	
Prozessbeschreibung	Nach hinterlegtem Tarifprofil werden die Verbrauchsdaten im Gateway Tarifzonen zugeordnet, mit einem Preissignal für diese Tarifzone multipliziert und nach hinterlegtem Intervall wird der Rechnungsbetrag an den Energielieferanten gesendet. Die eigentliche Rechnungserstellung erfolgt konventionell.	
Daten	Rechnungsbetrag	
Datenfluss	Letztverbraucher → Energielieferant	
Anmerkungen	Es wird davon ausgegangen, dass die im Schutzprofil vorgesehene sternförmige Kommunikation, die über Tarif- und Berechtigungsprofile ermöglicht wird, in Anspruch genommen wird und dadurch ein direkter Datenfluss von Letztverbraucher (Smart Meter) zu Energielieferant stattfindet. Die Möglichkeit der Erstellung des Rechnungsbetrages im Gateway ist derzeit nach Schutzprofil nicht vorgesehen, dennoch ist es möglich, dass Hersteller derartige Funktionen zusätzlich implementieren.	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Normal	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	
Integrität	Normal	
Vertraulichkeit	Normal	
Transparenz	Normal	
Intervenierbarkeit	Normal	
Nichtverkettbarkeit	Normal	
Maßnahmen	Datenschutzfreundlichste Art der Erstellung des Rechnungsbetrages	

4.3.4. Einspeisen und Abrechnen

Use Case 4.3.4-1: Einspeisen und dezentrale Abrechnung

Use Case	**Einspeisen und dezentrale Abrechnung**
Ziel	Bereitstellung der Einspeisemenge für die Abrechnung der eingespeisten Energie durch den Abnehmer des Stroms, dem Energielieferanten

Akteure	Prosumer, Energielieferant, Verteilnetzbetreiber	
Prozessbeschreibung	Der Prosumer speist die erzeugte bzw. vorgehaltene Energie in das Stromnetz. Der Verteilnetzbetreiber verteilt den Strom entsprechend weiter. Nach hinterlegtem Tarifprofil werden die Einspeisedaten im Gateway Tarifzonen zugeordnet und nach hinterlegtem Intervall aggregiert für jede Tarifzone an den Energielieferanten gesendet. Da die Abrechnung der Einspeisung dezentral im Gateway erfolgt, muss der Use Case „Selbstverbrauch der erzeugten Energie und Einspeisen der Restmenge„ nicht separat betrachtet werden. Der abnehmende Energielieferant erhebt die Einspeisemenge, um den Netzzustand (siehe 3.4.7-1) zu ermitteln und bei Bedarf die Energieerzeugungs- bzw. Energiespeichereinheit(en) (z.B. Elektroauto) fernzuschalten. Die eingespeiste Energiemenge wird entsprechend dem Tarif (z.T. im EEG geregelt) abgerechnet.	
Daten	Abrechnungsdaten (Einspeisung)	
Datenfluss	Prosumer → Energielieferant	
Anmerkungen	Eine feingranulare Übertragung der Einspeisemenge durch den Einzelhaushalt ist nicht erforderlich, da die Abrechnung der Einspeisemenge dezentral erfolgen kann. Es wird davon ausgegangen, dass die im Schutzprofil vorgesehene sternförmige Kommunikation, die über Tarif- und Berechtigungsprofile ermöglicht wird, in Anspruch genommen wird und dadurch ein direkter Datenfluss vom Prosumer (Smart Meter) zu Energielieferant stattfindet.	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Normal	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	wichtig für Netzzustandsmessung (Fernschaltung), jedoch ist ein einzelner Ausfall eines Stromerzeugers nicht kritisch
Integrität	Normal	
Vertraulichkeit	Normal	
Transparenz	Normal	
Intervenierbarkeit	Normal	
Nichtverkettbarkeit	Normal	
Maßnahmen		

4.3.5. Steuerung von unterbrechbaren Verbrauchseinrichtungen

Use Case 4.3.5-1: Statusdaten von unterbrechbaren Verbrauchseinrichtungen

Use Case	**Statusdaten von unterbrechbaren Verbrauchseinrichtungen**	
Ziel	Steuerung von unterbrechbaren Verbrauchseinrichtungen, je nach Netzauslastung und Tarifgestaltung, durch den Netzbetreiber	
Akteure	Letztverbraucher, Netzbetreiber	
Prozessbeschreibung	Der Netzbetreiber kann, je nach Netzauslastung und gewähltem Kundentarif, die Energieaufnahme von unterbrechbaren Verbrauchseinrichtungen (aktuell z.B. Elektro-Speicherheizungen oder Elektro-Wärmepumpen; zukünftig z.B. Waschmaschine, Wäschetrockner oder Geschirrspüler) steuern und sie somit an- und ausschalten, bzw. ihre Leistung über die Menge der Energieaufnahme beeinflussen. Letztverbraucher gibt Statusdaten seiner unterbrechbaren Verbrauchsgeräte ab, damit der Netzbetreiber weiß, wie er entsprechend seiner Energiebilanz im Netz unterbrechbare Verbrauchsgeräte ansteuern kann. Der Letztverbraucher signalisiert, ob und wann die unterbrechbaren Verbrauchseinrichtungen gesteuert werden können.	
Daten	Statusdaten unterbrechbarer Verbrauchseinrichtungen	
Datenfluss	Letztverbraucher → Netzbetreiber	
Anmerkungen		
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	
Integrität	Normal	
Vertraulichkeit	Hoch	Rückschluss über Lebensgewohnheiten möglich
Transparenz	Hoch	Weitreichende Konsequenzen der Datenbereitstellung
Intervenierbarkeit	Normal	
Nichtverkettbarkeit	Hoch	Rückschluss auf Lebensgewohnheiten möglich
Maßnahmen	Je nach gewähltem Tarif kann der Energielieferant im Rahmen eines vorher geschlossenen Vertrages, die unterbrechbaren Verbrauchseinrichtungen steuern. Der Letztverbraucher muss dafür Statusdaten zur Verfügung stellen, die jedoch keine Rückschlüsse auf seine Lebensgewohnheiten ermöglichen dürfen. Die Statusdaten der einzelnen Geräte dürfen nicht miteinander verknüpft werden, sie sind unmittelbar zu löschen. Um das informationelle Selbstbestimmungsrecht wahrnehmen zu können, muss der Letztverbraucher einen Einblick darin haben, wann welche Daten zu den unterbrechbaren Verbrauchseinrichtungen übermittelt werden und was dies für Auswirkungen auf die Steuerung seiner unterbrechbaren Verbrauchsgeräte hat.	

	Außerdem muss hierfür dem Letztverbraucher ein Gestaltungsspielraum eingeräumt werden, z. B. für das zeitliche Intervall der Übermittlung der Daten, kein Übermitteln während bestimmter Tageszeiten, Ausschalten während des Urlaubs u. ä. Verschlüsselte Kommunikationskanäle und Ende-zu-Ende-Verschlüsselung mit Zertifizierung nach Stand der Technik.

4.3.6. Umsetzung zeitvariabler Tarife und Verbrauchsvisualisierung

Use Case 4.3.6-1: Tarifierung

Use Case	**Tarifierung**	
Ziel	Datenbereitstellung zur Umsetzung variabler Tarife	
Akteure	Letztverbraucher, Energielieferant	
Prozessbeschreibung	Damit die Abrechnung der neuen Tarife möglich ist, werden Daten pro Tarifzone auf unterschiedliche Art und Weise bereitgestellt. Bei der zentralen Tarifierung werden Verbrauchsdaten nach hinterlegtem Zeitintervall an den Energielieferanten gesendet und dieser ordnet den Verbrauchswerten Tarifzonen zu. Bei der dezentralen Tarifierung werden die Verbrauchsdaten lokal im Gateway Tarifzonen zugeordnet, eine Übermittlung der aggregierten Daten erfolgt nach hinterlegtem Zeitintervall. Bei der dezentralen Erstellung des Rechnungsbetrages werden Verbrauchsdaten lokal im Gateway Tarifzonen zugeordnet, mit dem Preissignal der Tarifzonen multipliziert und zu einem Rechnungsbetrag addiert. Der Rechnungsbetrag wird nach festgelegtem Zeitintervall an den Energielieferanten übermittelt. Da diese unterschiedlichen Arten zu tarifieren sich bei der Abrechnung auswirken, wurden diese Fälle im Detail in Use Case in 4.3.3-1, 4.3.3-2 und 4.3.3-3 betrachtet.	
Daten		
Datenfluss		
Anmerkungen		
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt		
Verfügbarkeit		
Integrität		
Vertraulichkeit		
Transparenz		
Intervenierbarkeit		
Nichtverkettbarkeit		

Maßnahmen	

Use Case 4.3.6-2: Lokale und externe Verbrauchsvisualisierung

Use Case	Lokale und externe Verbrauchsvisualisierung	
Ziel	Nachvollziehbarkeit des Verbrauchs für den Letztverbraucher zur Verbrauchsanalyse	
Akteure	Letztverbraucher, Energielieferant, evtl. berechtigter Marktteilnehmer	
Prozessbeschreibung	Die feingranularen Verbrauchsdaten können Grundlage für eine Verbrauchsvisualisierung für den Letztverbraucher sein: **Fall 1**: Die Visualisierung geschieht als Anwendung auf einem lokalen Endgerät des Letztverbrauchers. Die Daten werden dafür über die lokale Schnittstelle des Gateways abgerufen. Die Aufbereitung und Visualisierung der Daten verbleiben somit lokal ausschließlich in der Hoheit des Letztverbrauchers. **Fall 2**: Die Aufbereitung und Visualisierung der Verbrauchsdaten erfolgt extern und sie verlassen den Haushalt des Letztverbrauchers. Die aufbereiteten, visualisierten Daten sind nach Kontaktaufnahme durch den Letztverbraucher abrufbar.	
Daten	Fall 1: Mess- oder Verbrauchsdaten in beliebig feiner Auflösung Fall 2: Mess- oder Verbrauchsdaten	
Datenfluss	Fall 1: Letztverbraucher → lokale Nutzerschnittstelle Fall 2: Letztverbraucher → Energielieferant, berechtigter Marktteilnehmer	
Anmerkungen		
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Sehr hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	
Integrität	Normal	
Vertraulichkeit	Sehr hoch	Der Zweck der Datenauswertung besteht gerade darin, das Nutzungsverhalten des Letztverbrauchers nachvollziehbar zu machen. Es handelt sich dabei um sehr sensible Daten.
Transparenz	Hoch	Der Letztverbraucher muss verstehen, welche Instanz außer ihm sein Nutzungsverhalten kontrollieren kann.
Intervenierbarkeit	Fall 1: normal Fall 2: sehr hoch	Wenn der Nutzer ausschließlich die Hoheit über die Auswertung der Daten hat, bedarf es keiner weiteren Vorgaben. Wenn die Daten die Hoheit des Nutzers verlassen, sollte der Nutzer jederzeit seine Einwilligung auch unmittelbar operativ entziehen können.
Nichtverkettbarkeit	Sehr hoch	Wie bei Vertraulichkeit.
Maßnahmen	Die Daten zur Visualisierung sind hoch aufgelöst, durch die Übermittlung hoch auflösender Messdaten an Marktteilnehmer entsteht ein hohes datenschutzrechtliches Risiko. Mit einer lokalen Schnittstelle von Smart Meter zum Verbraucher soll sich jeder Verbraucher ein Bild über seinen Energieverbrauch machen können, ohne dass sensible Verbrauchsdaten im Sekundentakt an Dritte weitergeleitet werden müssen. Nur so hat der Verbraucher die Möglichkeit, sich energieeffizient zu verhal-	

	ten, ohne datenschutzrechtliche Kollateralschäden in Kauf nehmen zu müssen. Es ist kein zusätzlicher Nutzen ersichtlich, wenn diese Daten durch einen externen Drittanbieter oder den Energielieferanten aufbereitet werden. Eine solche Aufbereitung kann durch ein Programm jederzeit und in bestmöglicher Auflösung oder Aggregation auf lokalen Endgeräten des Letztverbrauchers mit gleicher Leistungsfähigkeit geschehen. Wenn eine solche Auswertung auf der Grundlage einer Einwilligung trotzdem durch eine externe Instanz geschehen soll, dann setzt dies den Einsatz wirksamer Verschlüsselungstechniken Ende-zu-Ende, eine entsprechend vertraglich vereinbarte Zweckbindung sowie die Möglichkeit zu einer jederzeitigen Kündigung und Löschung der Daten voraus. Ausführliche Information des Letztverbrauchers ist erforderlich.

4.3.7. Ermittlung Netzzustand

Use Case 4.3.7-1: Ermittlung Netzzustand zur Betriebsführung

Use Case	**Ermittlung Netzzustand zur Betriebsführung**	
Ziel	Sicherstellung der Energieversorgung durch Erhebung von Netzzustandsdaten	
Akteure	Letztverbraucher, Verteilnetzbetreiber	
Prozessbeschreibung	Verteilnetzbetreiber erhebt Netzzustandsdaten, um die Stabilität des Netzes zu überprüfen. Je nach Ergebnis folgen unterschiedliche Maßnahmen (Einspeisung, Fernabschaltungen oder Ähnliches).	
Daten	Spannung, Frequenz, Strom, Phasenwinkel (ggf. weitere)	
Datenfluss	Letztverbraucher → Verteilnetzbetreiber	
Anmerkungen	Folgende Punkte sind nicht abschließend diskutiert: • **Erforderlichkeit von Smart Meter Daten für das Intelligente Energienetz**: Eine Messung der Werte in der Ortsnetzstation erscheint ausreichend. Die nach EnWG begründeten und dokumentierten Fälle zur Ermittlung des Netzzustandes sind nicht bekannt. Die Erforderlichkeit der Erhebung von Netzzustandsdaten über Smart Meter im Vergleich zu Messungen in der Ortsnetzstation sollte in neutralem Gutachten untersucht werden. • **Rückschlüsse von Netzzustandsdaten auf sensible Verbrauchsdaten**: Je nach Wert der Netzzustandsdaten werden Maßnahmen ergriffen, um Verbrauch und Einspeisung in Einklang zu bringen, so dass Netzzustandsdaten Rückschlüsse auf den Verbrauch zulassen können. Es wird empfohlen von einer neutralen Stelle ein Gutachten erstellen zu lassen, inwieweit Netzzustandsdaten Rückschlüsse auf den Verbrauch ermöglichen, hierbei ist darauf hinzuweisen, dass die Rückverfolgbarkeit gerade in Kombination von mehreren Netzzustandsdaten erfolgen kann. • Wie wird der Netzzustand bisher berechnet? Welche Änderungen sind im Energieumfeld zu erwarten, so dass die bisherige Berechnung nicht mehr ausreicht?	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Sehr hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	Die Verfügbarkeit ist aus Datensicherheitsperspektive wichtig für Netz-

		zustandsmessung, jedoch ist ein einzelner Ausfall eines Datenbereitstellers, insbesondere aus Sicht des Letztverbrauchers und des Datenschutzes, unkritisch.
Integrität	Normal	
Vertraulichkeit	Hoch	Abhängig davon, welche Rückschlüsse auf sensible Verbrauchsdaten möglich sind
Transparenz	Hoch	Sensible Verbrauchsdaten
Intervenierbarkeit	Normal	
Nichtverkettbarkeit	Sehr hoch	Abhängig davon, welche Rückschlüsse auf sensible Verbrauchsdaten möglich sind. Da die Daten ggf. feingranular erhoben werden, ist eine Profilbildung möglich.
Maßnahmen	Es wird davon ausgegangen, dass sich aus den Netzzustandsdaten Rückschlüsse auf den Verbrauch ziehen lassen. Die These wird dadurch bekräftigt, dass andernfalls die Erhebung der Netzzustandsdaten keinerlei Aussage hätte und bei der Netzsteuerung nicht berücksichtigt werden könnte (Zuschalten bzw. Abschalten von Lasten). Die Daten müssen nach Zweck verschlüsselt werden. Verschlüsselte Kommunikationskanäle und Ende-zu-Ende-Verschlüsselung mit Zertifizierung nach Stand der Technik. Der Letztverbraucher braucht eine zentrale Anlaufstelle und ausführliche Informationen darüber, wer welche Daten zu welchem Zweck erhält. Die Aktivitäten werden im Kunden-Log protokolliert. Eine Erhebung der Netzzustandsdaten über Smart Meter erfordert keinen Bezug zum Haushalt. Eine Zuordnung zu einer Ortsnetzstation ist ausreichend. Dies kann über ein Pseudonym für eine Ortsnetzstation erreicht werden. Weiter sind Messungen an Ortsnetzstationen denkbare Alternativen.	

Use Case 4.3.7-2: Ermittlung Netzzustand zur Netzplanung

Use Case	**Ermittlung Netzzustand zur Netzplanung**	
Ziel	Auf Basis von Vergangenheitswerten soll die Netzplanung erfolgen (Kapazitäten, Ausbau, etc.)	
Akteure	Letztverbraucher, Verteilnetzbetreiber	
Prozessbeschreibung	Der Verteilnetzbetreiber führt seine Netzplanung durch und nutzt Netzzustandsdaten der Vergangenheit dazu.	
Daten	Spannung, Frequenz, Strom, Phasenwinkel (ggf. nur eine Auswahl)	
Datenfluss	Letztverbraucher → Verteilnetzbetreiber	
Anmerkungen	Wie feingranular werden die Daten dafür verwendet? Hinweis: auch wenn es sich um Vergangenheitswerte handelt, sind Netzzustandsdaten nicht weniger sensibel, es sei denn, diese werden aggregiert, so dass diese nicht mehr personenbezogen sind. Siehe Use Case 4.3.7-1	
	Datenschutzbedarf	**Begründung**
Datenschutz-		Siehe Use Case 4.3.7-1

bedarf gesamt		
Verfügbarkeit		
Integrität		
Vertraulichkeit		
Transparenz		
Intervenier-barkeit		
Nichtverkett-barkeit		
Maßnahmen		

4.4 Ergebnis: Zusammenfassung der Maßnahmen

Anforderungen an die datenverarbeitenden Stellen

Das novellierte Energiewirtschaftsgesetz regelt in § 21e Abs. 4 EnWG, dass zur Datenerhebung, -verarbeitung, -speicherung, -prüfung, und -übermittlung ausschließlich technische Systeme und Bestandteile eingesetzt werden dürfen, die den Anforderungen von Schutzprofilen entsprechen.

Dieser technischen Maßnahme müssen sich aber auch organisatorische Maßnahmen anschließen. Entsprechend müssen ebenfalls der Zugriff und die Administration der Smart Meter Gateways in die datenschutzrechtlichen Überlegungen einbezogen werden.

Folgende Anforderungen sind an den Gateway-Administrator für eine sichere Installation und einen sicheren Betrieb zu stellen:

- Voraussetzung für die Zertifizierung ist die notwendige Einrichtung eines Datenschutz-Managementsystems (Gesteuertes Change-Management, Kundenbetreuung, Prüfbarkeit in Bezug auf Compliance, zweckgebundene Datenverarbeitung, etc.). Weiter soll zur Sicherung der Transparenz und Integrität bei Kommunikationspartnern des Gateways und beim Gateway-Administrator ein Nachweis über ein gesichertes Änderungsmanagement nach Stand der Organisationslehre (beispielsweise ITIL, ISO 27001, ISO 29100/1001, BSI-Grundschutz) sowie Datenschutzmanagement vorhanden sein.
- Zertifizierung des „Gateway-Administrators“ durch eine Zertifizierungsstelle
- regelmäßige Re-Zertifizierung inkl. Prüfung der stattgefundenen Tätigkeiten
- die Möglichkeit von zufälligen Stichproben, so dass die Zertifizierungsstelle dem Gateway-Administrator im berechtigten Fall die Zertifizierung entziehen kann

Sicherstellung Integrität durch Zertifizierung nach Stand der Technik

Diese Maßnahme erfordert verschlüsselte Kommunikationskanäle und Ende-zu-Ende-Verschlüsselung und Integritätssicherung durch Signaturverfahren mit Zertifizierung nach Stand der Technik.

Zentrale Anlaufstelle für den Letztverbraucher

Der Letztverbraucher braucht eine zentrale Anlaufstelle, um im Zweifelsfall schnell intervenieren zu können und seine Rechte einzufordern.

Vermeidung des gläsernen Letztverbrauchers

Die Granularität der Daten muss für jeden Use Case kritisch geprüft und hinterfragt werden. Einsatz von Pseudonymen, die nicht einem Haushalt zugeordnet werden können, müssen für die Use Cases, die keinen Haushaltbezug erfordern, umgesetzt werden (Hinweis: die Zähler-ID kann einem Haushalt zugeordnet werden!). Eine zweckgebundene Pseudonymisierung, das heißt ein Pseudonym für jeden Zweck der Datenerhebung, verhindert die Verkettbarkeit von Daten und wirkt der Profilbildung von Letztverbrauchern entgegen.

Transparenz für den Letztverbraucher

Der Letztverbraucher muss prüfen können, wer welche Daten zu welchem Zweck erhalten hat und über die Modalitäten der Ablesung und Datenübermittlung im Vorfeld informiert werden. Er muss nachvollziehen können, wer, wann, welche Daten erhalten hat und aus welchem Grund. Er muss über sämtliche Änderungen, beispielsweise der Tarif- und Berechtigungsprofile, und Störungen informiert werden. Eine anschauliche Aufbereitung der Daten für den Letztverbraucher ist wünschenswert. Besondere Vorfälle sollen hervorgehoben werden (beispielsweise Benachrichtigungen per E-Mail bei bestimmten Vorfällen).

Intervenierbarkeit bei Störungen/Fehlern

Der Letztverbraucher muss in klar definierten Fällen von Störungen (falsche Tarif- und Berechtigungsprofile, falsche Zertifikate etc.) die Kommunikation unterbinden können. Daten, die eigentlich übertragen werden sollten, können in diesen Fällen im Gateway zwischengespeichert werden.