Datensicherheit und Datenschutz für Smart Grids: Offene Fragen und mögliche Lösungsansätze

Bericht vom 30. Juni 2014

Im Auftrag von:

Bundesamt für Energie BFE
CH-3003 Bern
www.bfe.admin.ch

Auftragnehmer:

AWK Group AG
Leutschenbachstrasse 45
CH-8050 Zürich
www.awk.ch

VISCHER AG
Rechtsanwälte

Schützengasse 1
Postfach 1230
CH-8021 Zürich
www.vischer.com

Forschungsstelle für
Informationsrecht (**FIR-HSG**)
Universität St.Gallen
Guisanstrasse 36
CH-9010 St.Gallen
www.fir.unisg.ch

Autoren:

AWK Group AG
Schmuel Holles
Jennifer De Capitani
Tobias Keel

VISCHER AG
Dr. Stefan Rechsteiner
lic.oec. et lic. iur. HSG Azra
Dizdarevic-Hasic

FIR-HSG
Prof. Dr. Peter Hettich, FIR-HSG
Lukas Stocker, M.A. HSG
Lukas Mathis, B.A. HSG
Louisa Galbraith, B.A. HSG
Jannick Koller, B.A. HSG

Begleitung seitens des Auftraggebers:

Dr. Matthias Galus, Abteilung Energiewirtschaft, Sektion Netze

Die vorliegende Studie wurde von einer **Begleitgruppe** unterstützt.

Abkürzungen und Begriffe

Abkürzung	Beschreibung
BFE	Bundesamt für Energie
BHKW	Blockheizkraftwerk
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
CIA / CIAN	Confidentiality, Integrity, Availability, Non-Repudiation
DM	Datenmanager
DOCSIS	Data Over Cable Service Interface Specification
DSM	Demand Side Management
DSR	Demand Side Response
EDM	Energiedatenmanagement
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
FTTx	Fiber To The x
GIS	Geoinformationssystem
GPRS	General Packet Radio Service
HSxPA	High Speed Packet Access
ICT	Information- & Communication Technology
IH	Instandhaltung
KW	Kraftwerk
LAN	Local Area Network
LTE	Long Term Evolution
MPLS	Multiprotocol Label Switching
PDH	Plesiochrone Digitale Hierarchie
SCADA	Supervisory Control and Data Acquisition
SDH	Synchrone Digitale Hierarchie
SDL	Systemdienstleistung
SDV	SDL-Verantwortlicher
SG-CG	Smart Grid Coordination Group
UCMR	Use Case Management Repository
ÜN	Übertragungsnetz
VN	Verteilnetz
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
xDSL	x Digital Subscriber Line
xWDM	x Wavelength Division Multiplexing

Tabelle 1: Abkürzungen und Begriffe

Referenzierte Dokumente

Titel	Autor / Herausgeber	Datum
[1] Mandat M/490 Auftrag an die Europäischen Normungsorganisationen zur Erstellung von Normen zur Unterstützung der Einführung intelligenter Stromnetze in Europa	Europäische Kommission	01.03.2011
[2] Mandat M/441 Normungsauftrag an CEN, CENELEC und ETSI auf dem Gebiet der Messgeräte mit dem Ziel der Entwicklung einer offenen Architektur für Verbrauchszähler unter Einbeziehung von Interoperabilität ermöglichenden Kommunikationsprotokollen	Europäische Kommission	12.03.2009
[3] Appropriate security measures for smart grids	ENISA	12/2012
[4] Smart Grid Information Security	CEN-CENELEC-ETSI Smart Grid Coord. Group	11/2012
[5] First Set of Standards	CEN-CENELEC-ETSI Smart Grid Coord. Group	11/2012
[6] Smart Grid Reference Architecture	CEN-CENELEC-ETSI Smart Grid Coord. Group	11/2012
[7] Sustainable Processes	CEN-CENELEC-ETSI Smart Grid Coord. Group	11/2012
[8] Zustandsanalyse und Entwicklungsbedarf von Technologien für ein Schweizer Smart Grid	CONSENTEC	07/2013
[9] Nationale Strategie zum Schutz kritischer Infrastrukturen SKI	Bundesamt für Bevölkerungsschutz BABS	27.06.2012
[10] Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS	19.06.2012

Tabelle 2: Referenzierte Dokumente

Inhaltsverzeichnis

1. Auftrag

Beim schrittweisen Ausstieg aus der Kernenergie soll im Rahmen der Energiestrategie 2050 mit einer Strategie Stromnetze eine bedarfs- und zeitgerechte Netzentwicklung ermöglicht werden. Zur Bewältigung der netzseitig anstehenden Herausforderungen müssen intelligente Lösungen bereitgestellt werden, namentlich die Smart Grids. Dies erfordert den Einbezug und die Koordination vieler heterogener Akteure. Die Smart Grid Roadmap, welche vom Bundesamt für Energie erarbeitet wird, leistet dies.

Darüber hinaus ist die Smart Grid Roadmap im Ergebnis ein Fahrplan für die Weiterentwicklung der elektrischen Netze. Sie umfasst eine Skizze zu Entwicklungen von technologischen Lösungen und notwendigen neuen Rahmenbedingungen, um den derzeitigen und kommenden Herausforderungen zu begegnen.

In dieser Studie werden die Grundlagen für die Erstellung und Definition von Standards und Richtlinien im Umfeld der Datensicherheit und des Datenschutzes geschaffen, welche aufgrund der Smart Grid Technologien und deren Einsatzgebiete erforderlich werden. Die Studie wurde in die folgenden Arbeitspakete unterteilt:

- Arbeitspaket 1: ICT Architektur Smart Grids – Definition der Anwendungsfälle, Rollen, Datenobjekte, Kommunikationsinfrastrukturen sowie Komponenten, welche gesamtheitlich die ICT Architektur eines zukünftigen Smart Grids darstellen könnten.
- Arbeitspaket 2: Richtlinien und Standards – Identifikation des Datensicherheitsbedarfs in dieser ICT Architektur sowie Ableitung des zukünftigen Standardisierungsbedarfs zur Festlegung der Anforderungen an die Datensicherheit in diesem Umfeld.
- Arbeitspaket 3: Datenschutz – Identifikation der Fragestellungen im Datenschutz sowie Aufzeigen möglicher diesbezüglicher Lösungsansätze.

Der exakte Inhalt der Arbeitspakete und deren Einbettung in den Studienauftrag werden bei der Beschreibung der Vorgehensmethodik in Kapitel 4.1 beschrieben.

Die Erarbeitung und Ergebnisse des Arbeitspakets 1 werden in den Kapiteln 4 und 5 beschrieben, welche anhand der definierten Anwendungsfälle die ICT Architektur und den Datensicherheitsbedarf analysiert.

Die Erarbeitung und Ergebnisse des Arbeitspakets 3 werden in Kapitel 6 beschrieben. wo die Datenschutzaspekte und mögliche Lösungsansätze analysiert werden. .

In den Kapiteln 7, 8 und 9 wird das Arbeitspaket 2 mit dem Standardisierungsbedarf und dem möglichen weiteren Vorgehen (Standardisierungs-Roadmap) zur Erstellung von Standards und Richtlinien ausgeführt. Die Durchführung der Arbeiten erfolgte gemeinsam durch die AWK (Fokus ICT-Architektur und Datensicherheit in den Arbeitspaketen 1 und 2) und VISCHER AG / FIR-HSG (Fokus Datenschutz in den Arbeitspaketen 1 und 3).

2. Management Summary

In zukünftigen intelligenteren Netzen werden verschiedene, teilweise neue Technologien, z. B. neuartige Messverfahren, Steuerungen in Verteilnetzen oder Speicher, derart miteinander vernetzt, dass sie neue Funktionalitäten der elektrischen Netze ermöglichen. Die Vernetzung der neuen Technologien erfolgt durch Informations- und Kommunikationstechnologien (IKT). Um die neuen Technologien effektiv zu betreiben und die neuen Funktionalitäten zu ermöglichen muss eine Vielzahl von Informationsobjekten bzw. Daten aufgenommen, verarbeitet und wieder versendet werden. Solche Informationsobjekte können z. B. den Zustand der elektrischen Netze beschreiben, Steuerbefehle oder Informationen an Produzenten und Konsumenten beinhalten.

Das Austauschen von Informationen ermöglicht zwar erst das Zusammenspiel der neuen Technologien in einem Smart Grid bedingt aber auch ein gewisses Risiko. Zum einen da insbesondere bei Endverbrauchern Daten aufgenommen werden, deren Persönlichkeitsrechte gewahrt werden müssen, zum anderen da Informationen zum Betrieb des Stromversorgungssystems ausgetauscht werden, die kritisch für die Systemstabilität sein können. Daher sind Datenschutz, i.S. v. Schutz personenbezogener Daten vor Missbrauch und Datensicherheit, i. S. v. Schutz von Daten vor Verlust, Verfälschung, Beschädigung oder Löschung durch organisatorische und technische Maßnahmen und durch Software, zu gewährleisten. Der Datenschutz bedingt also ebenfalls eine gewisse Datensicherheit. Um den Handlungsbedarf in den Bereichen Datensicherheit, Datenschutz und Standardisierung sowie den Zeithorizont dafür zu identifizieren, muss zunächst ermittelt werden, welche Rollen zu welchen Zwecken Daten austauschen. Dazu können auf Basis der gegeneinander abgegrenzten Funktionalitäten (siehe Kapitel 8) Anwendungsfälle modelliert werden. Innerhalb dieser interagieren verschiedene Rollen, die durch Akteure ausgefüllt werden[1]. Rollen können von verschiedenen Akteuren übernommen werden. Eine Übersicht der Rollen mit ihren jeweiligen Tätigkeitsbereichen ist in Tabelle M1 zusammengefasst. Eine Zuweisung von Rollen zu Akteuren ist eine Frage der Marktausgestaltung. Im Rahmen der vorliegenden Untersuchungen wird darauf bewusst verzichtet.

Rolle	Beschreibung
Prosumer / Verbraucher	Der Prosumer ist gleichzeitig der Einspeiser (Producer) und der Endverbraucher (Consumer) ins Stromnetz und befindet sich normalerweise in der Netzebenen 5 oder 7. Unter diesem Begriff werden im Bericht sowohl reine Endverbraucher, reine dezentrale Einspeiser als auch deren Kombination zusammengefasst. Die beim Prosumer anfallenden Datenobjekte, also innerhalb der Geräte ab Netzanschluss der Netzebenen 5-7 (z.B. in den Messsystemen), werden für diese Studie zwecks Analyse des Datenschutz- und Datensicherheitsbedarfs ihm zugeordnet.
Datenmanager (DM)	Der Datenmanager stellt die Schnittstelle für die Energie- und Netzdaten des Prosumers dar, welche von ihm gemessen, verwaltet, verarbeitet und an die relevanten Datenempfänger übermittelt werden. Er empfängt Daten und gibt Daten weiter, je nach Anwendungsfall aggregiert oder anonymisiert. Hier sei nochmals explizit vermerkt, dass diese Rolle nicht losgetrennt von anderen Rollen wahrgenommen werden muss, so wird sie heute beispielsweise vom Verteilnetzbetreiber wahrgenommen.
Verteilnetzbetreiber	Der Verteilnetzbetreiber ist für den Betrieb und Unterhalt des Verteilnetzes zuständig und verantwortet als Solcher die Versorgungssicherheit in seinem Netzgebiet.

[1] Die Rolle des Messtellenbetreibers hat gewisse Rechte und Pflichte und wird derzeit in der Schweiz vom Verteilnetzbetreiber ausgefüllt. Der Verteilnetzbetreiber als solcher ist gleichzeitig eine Rolle und ein Akteur.

Übertragungsnetzbetreiber	Der Übertragungsnetzbetreiber ist für den Betrieb und Unterhalt des Übertragungsnetzes zuständig und verantwortet die Versorgungssicherheit im Übertragungsnetz.
Erzeuger	Der zentrale Erzeuger erzeugt elektrische Energie und speist diese in die Netzebenen 1-3 ein.
Systemdienstleistungs-Verantwortlicher (SDV)	Der SDV ist verantwortlich für die kommerzielle und operative Planung und Ausführung der SDL und die entsprechende Verteilung der abgerufenen Regelenergie auf die beteiligten leistungsvorhaltenden Anlagen.
Energielieferant	Der Energielieferant ist zuständig für die Energielieferung an seine Endkunden (Prosumer).
Dienstleister Gebäude-automation	Der Dienstleister Gebäudeautomation ist eine mögliche zukünftige Rolle, welche mittels Anbindung an die Gebäudeautomation Hausautomations-Dienstleistungen anbieten kann.
Marktpartner	Weitere Marktpartner können zukünftig beliebige weitere Dienstleistungen anbieten und werden entsprechend unter dem Sammelbegriff „Marktpartner“ subsumiert. Da die Marktpartner auch auf diverse Smart Grid Datenobjekte zugreifen müssen, sind deren Datensicherheit und der Datenschutz zu berücksichtigen. Heutiges Beispiel solcher Marktpartner ist der Bilanzgruppenverantwortliche.

Tabelle M1: Zukünftig antizipierte Rollen, die in auf Basis von Smart Grids miteinander in Anwendungsfällen Interagieren und damit die Funktionalitäten von Smart Grids realisieren.

2.1. Ableitung des Handlungsbedarfs für Datensicherheit und Datenschutz

Auf Basis der Anwendungsfälle und der verschiedenen Rollen kann eine mögliche Smart Grid IKT Architektur entwickelt werden. Ein Vorgehen gemäss Best-Practice unter Benutzung des Smart Grid Architecture Model (SGAM) (Cen, 2012) ermöglicht zunächst die Ableitung einer IKT Referenzarchitektur. Diese verbindet die traditionelle, erweiterte Wertschöpfungskette von Produktion, Verteilung und Verbrauch mit Smart Grid Anwendungsfällen und den dazu notwendigen IKT Komponenten. Auf der obersten Ebene der Referenzarchitektur werden Funktionskategorien eingeordnet. Die darunter liegende Funktionsebene beinhaltet Anwendungsfälle, welche Informationsobjekte verwenden. Auf der Informationsebene werden Informationsobjekte zwischen den in den jeweiligen Anwendungsfällen aktiven Rollen ausgetauscht, z. B. notwendige Messdaten von Endverbrauchern. Der physische Austausch dieser Informationsobjekte findet auf der Kommunikationsebene statt[2]. Schliesslich werden die Informationsobjekte auf Komponentenebene verwendet. Hier werden Informationsobjekte entweder erzeugt, z. B. durch Messeinrichtungen, oder für die Steuerung. von bspw. Verbrauchern, verwendet. Abbildung veranschaulicht zusammenfassend die Smart Grid Referenzarchitektur.

[2]Unterschiedliche Kommunikationstechnologien werden je nach Zielsetzung und Umfeld eingesetzt. Dazu zählen die Unternehmenskommunikation (WAN, z.B. MPLS, SDH/PDH/IP), die Endkundenkommunikation (Access, z.B. WLAN, GSM/UMTS/LTE, DSL, FTTH, PLC) oder der Inhouse-Bereich (LAN, z.B. Ethernet/WLAN, Haus-LAN, serielle Kommunikation).

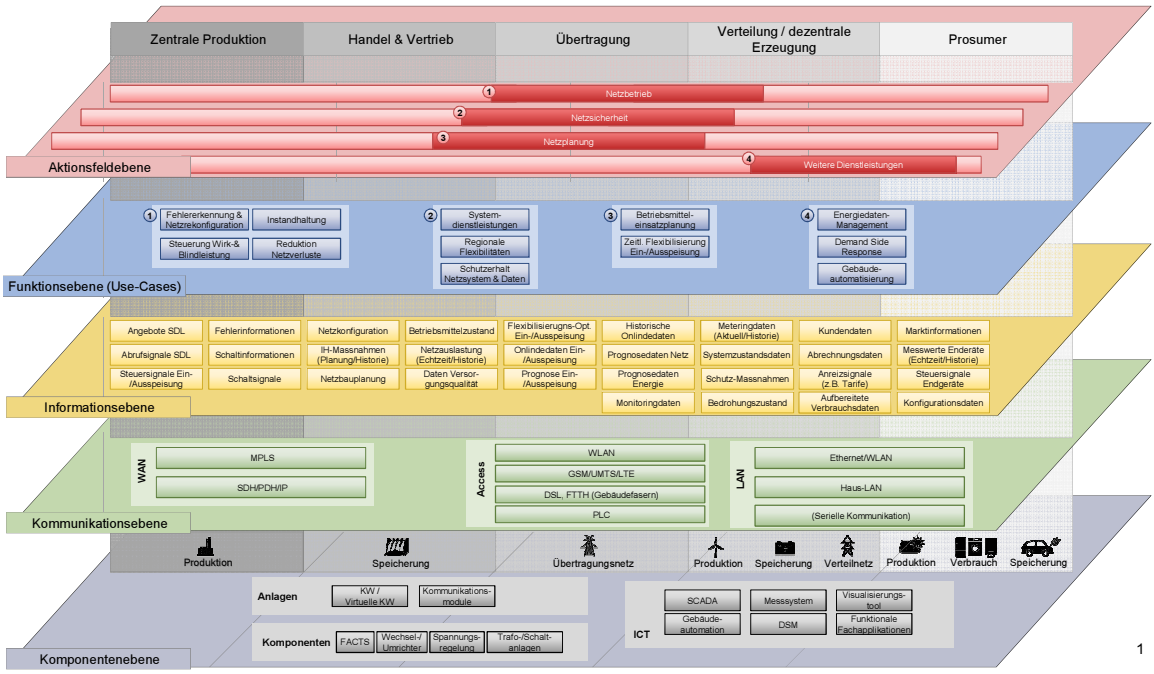


Abbildung M1: Anwendung des Smart Grid Architecture Models (SGAM) zur Identifizierung der notwendigen Datenobjekte welche Technologien und Rollen verbinden und damit Funktionalitäten realisieren.

Aus der Referenzarchitektur können über einen Zwischenschritt[3], der für alle Anwendungsfälle beschreibt welche Rollen über welche Kommunikationstechnologien welche Informationsobjekte austauschen, die übertragenen Informationsobjekte nach Rollen geordnet werden. Diese Informationsobjekte können dann einer Analyse hinsichtlich Vertraulichkeit (C), Integrität (I) und Verfügbarkeit (A) unterzogen werden[4]. Die Analyse ermöglicht eine qualitative Bewertung von Daten hinsichtlich Datenschutz und Datensicherheit. Daraus ergibt sich ein Bedarf zur Sicherung der Daten aus Sicht der Versorgungssicherheit oder aus Sicht des Schutzes personenrelevanter Daten (Datenschutz). So kann es für die Versorgungssicherheit notwendig sein, dass Informationsobjekte zum Beispiel kontinuierlich und korrekt an relevanten Stellen zur Verfügung stehen. Solche Informationsobjekte umfassen z. B. den Schaltzustand des Netzes bzw. Informationen über die aktuelle Topologie oder die Auslastung des Netzes. Eine Fehlinformation zu dem aktuellen Netzzustand kann die Versorungssicherheit gefährden, da u. U. Entscheidungen, z. B. hinsichtlich einer Schalthandlung getroffen werden, die die Netzstabilität gefährden können. Hinsichtlich des Datenschutzes können die Informationsobjekte schützenswerte Personen- oder Firmendaten betreffen, welche vor Zugriff durch Unberechtigte geschützt werden müssen. Solche Daten umfassen z. B. Gebote für Systemdienstleistungen auf Basis der Kraftwerksverfügbarkeit oder Persönlichkeitsprofile mit Informationen über die Vorlieben einzelner Personen.

Die Analyse zeigt, dass vor allem der Datenschutz im Bereich der Endverbraucherdaten wichtig ist. Der Bedarf an Datensicherheit in diesem Bereich wird vornehmlich durch Anforderungen an den Datenschutz getrieben und weniger durch die weiterhin zu gewährleistende Versorgungssicherheit. Im Netzbereich muss die Datensicherheit vor allem aus versorgungssicherheitstechnischen Gründen bei der Übertragung und Speicherung der

[3] Den Zwischenschritt bildet eine Smart Grid IKT Architektur. Sie findet sich in der vom BFE in Auftrag gegeben Studie „Datenschutz und Datensicherheit in Smart Grids“ AWK 2014.

[4] Dies ist ein Best-Practice Vorgehen zur Feststellung des Datensicherheitsbedarfs. Die Analyse wird auch CIA Analyse genannt wobei das Kürzel für C-Vertraulichkeit (Confidentiality), I-Integrität (Integrity) und A-Verfügbarkeit (Availability) steht.

Informationsobjekte gegeben sein. Der Handlungsbedarf ist jedoch abhängig von der konkreten Ausgestaltung der Anwendungsfälle. Da diese derzeit nur schwer antizipierbar ist, ist eine abschliessende Identifizierung nicht möglich. Für die Ableitung erster Tendenzen lassen sich Informationsobjekte gruppieren und schliesslich zusammenfassen zu Daten für Komponenten oder Applikationen und schliesslich zu grösseren Standardisierungskategorien. Tabelle M2 zeigt die Standardisierungskategorien und die von entsprechenden Standards betroffenen Rollen. Zur Einschätzung der Sensibilität und des Sicherheitsbedarfs der Informationsobjekte wird eine Analyse gemäss derzeitigen Best-Practice hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit (Confidentiality, Integrity, Availability – CIA) der Daten durchgeführt. Die Ergebnisse sind ebenfalls in Tabelle M2 dargestellt.

Standardisierungs-kategorie	Betroffene Rollen	Sicherheitskriterien von Informationsobjekt-gruppen pro Kategorie C I A	Anzahl von Informations-gruppen pro Standar-disierungskategorie in Abhängigkeit der Da-tenkritikalität.
Messsysteme (MS)	Prosumer		Informationsgruppe MS 1 Informationsgruppe MS 2
Anbindung Gebäude (AG)	Prosumer		Informationsgruppe AG 1 Informationsgruppe AG 2
Prosumer Daten (PD)	Datenmanager Energielieferant Dienstleister GA Weitere Marktpartner		Informationsgruppe PD 1 Informationsgruppe PD 2 Informationsgruppe PD 3
Netzmanagement Daten (ND)	Übertragungsnetz-betreiber Verteilnetzbetreiber Erzeuger SD-Verantwortlicher		Informationsgruppe ND 1 Informationsgruppe ND 2 Informationsgruppe ND 3 Informationsgruppe ND 4 Informationsgruppe ND 5 Informationsgruppe ND 6 Informationsgruppe ND 7

Tabelle M2: Standardisierungskategorien, von den Standards betroffene Rollen sowie Gruppierung der Einschätzung von Sicherheitskriterien Vertraulichkeit, Integrität und Verfügbarkeit (Confidentiality, Integrity, Availability – CIA) für relevante Informationsobjekte.

Pro Standardisierungskategorie fallen eine Vielzahl verschiedener Informationsobjekte an. Diese Informationsobjekte müssen einzeln auf ihrer Kritikalität hinsichtlich der Sicherheitskriterien überprüft werden und können unterschiedliche Kritikalitäten hinsichtlich der Kriterien erreichen. Tabelle M2 zeigt eine Übersicht über die Kritikalitäten der Daten pro

Kategorie an. Die Kritikalität hinsichtlich der Sicherheitskriterien wird nicht pro Informationsobjekt dargestellt sondern pro Gruppe von Informationsobjekten, die die gleiche Kritikalität aufweisen. Damit werden also pro Indikator (Ampel) mehrere Informationsobjekte gleichzeitig dargestellt.

Messsysteme umfassen physisch alle Systeme beim Endkunden, welche Daten messen und für deren Weiterverwendung bereitstellen. Viele Informationsobjekte innerhalb dieser Standardisierungskategorie sind als kritisch bezüglich der Vertraulichkeit und Integrität bewertet werden können (Informationsgruppe MS 2). Es handelt sich hierbei meist um personenbezogene Daten. Die Verfügbarkeit für alle Informationsobjekte kann weitgehend als unkritisch eingestuft werden, da sie aus Gründen der Versorgungssicherheit wenig relevant sind. Erste wichtige Standards sind vorhanden oder werden derzeit erarbeitet. Ein Handlungsbedarf wird hier, trotz der Verfügbarkeit von einigen Standards, vor allem im Bereich Datensicherheit geortet.

Intelligente Gebäudegeräte oder Gebäudeautomation werden vermehrt bei den Prosumern eingesetzt. Im Zentrum etwaiger Standardisierungsbemühungen stehen hier vor allem die Schnittstellen zwischen Stromnetz und Gebäudeautomation. Es können die prosumerbezogenen Datenobjekte bezüglich der Vertraulichkeit und Integrität als kritisch eigestuft werden, wohingegen die Verfügbarkeit als unkritisch beurteilt werden kann (Informationsgruppe AG 2). Erste Standards sind bereits vorhanden, müssen aber noch weiterentwickelt werden. Auch hier wird also ein Handlungsbedarf identifiziert.

Prosumerdaten werden von Netzbetreibern und Marktpartnern in verschiedenen Ausprägung benötigt, bearbeitet und gespeichert. Unabhängig von der Quelle dieser Datenobjekte (Messsystem, Gebäudeautomation etc.) müssen Regelungen für den Umgang mit diesen Informationsobjekten bestehen. Dazu können unter anderem Vorgaben zu Speicherung, Verwendung und Weitergabe der Informationsobjekte gehören. Je nach Anwendung bei den Akteuren und den dafür benötigten Daten ergibt sich somit eine Kritikalität im Bereich der Vertraulichkeit und der Integrität (Informationsgruppe PD 3). In wenigen Ausnahmen der Informationsobjekte wird keine oder nur eine geringe Kritikalität, so bei der Integrität festgestellt. Die Verfügbarkeit wird generell als unkritisch beurteilt. Innerhalb dieser Kategorie sind grösstenteils noch Standardisierungsaufgaben zu lösen und Regelungen zu treffen, die eine Vereinfachungen und Harmonisierung zwischen verschiedenen Akteuren im Umgang mit diesen Daten erreichen.

Der Kategorie Netzmanagement gehören Daten an, die z. B. für Automatisierungen und Optimierungen des Netzbetriebs, der Netzregelung, sowie des Asset Managements nötig sind und bei den Rollen Verteilnetzbetreiber, Übertragungsnetzbetreiber, Erzeuger sowie dem SDV anfallen. Innerhalb dieser Standardisierungskategorie bestehen bereits, etablierte und bewährte Standards. Es zeigt sich durch die Vielfalt der sich hier ergebenden „Ampeln“, dass Informationsobjekte innerhalb dieser Kategorie aufgrund der Vielfalt der Verwendungszwecke ganz unterschiedliche Beurteilung hinsichtlich der Sicherheitskriterien erfahren. Viele Informationsobjekte sind mindestens bezüglich der Vertraulichkeit und Integrität als kritisch zu beurteilen (Informationsgruppen ND 3, 5 - 7). Ein grosser Teil vorhandener Informationsobjekte ist ebenfalls hinsichtlich der Verfügbarkeit als kritisch einzustufen. Dies ist bei den SCADA Datenobjekten sowie den Schalt- und Steuersignalen vor allem aus Gründen Versorgungssicherheit der Fall. Es sind aber auch datenschutzrelevante und kritische Bereiche vorhanden, wo Prosumer Daten verwendet werden. Für diese Kategorie zeichnet sich ein Bedarf an Harmonisierung bzw. Erweiterung ab. Grundsätzlich sind die bestehenden Standards jedoch ausreichend für neue Anwendungsfälle.

2.2. Schlussfolgerungen für Standardisierung im Bereich Datenschutz und Datensicherheit

Bei einem grossen Teil der in Anwendungsfällen zu erfassenden Datenströme, wie bspw. Abrechnungsdaten, Kundendaten, Netzkonfigurations- oder Netzbauplanungsdaten handelt es sich um Personendaten, bei deren Bearbeitung datenschutzrechtlichen Vorgaben zu beachten sind. Zu beachten ist dabei, dass sobald ein Datensatz geschützte Personendaten enthält, die datenschutzrechtlichen Anforderungen für den ganzen Datensatz Anwendung finden. Die Sicherheit der Daten muss insbesondere aus Gründen der Versorgungssicherheit im Netzbereich gewährleistet werden während sie aus Datenschutzgründen im Verbraucher- bzw. Prosumerbereich gewährleistet werden muss.

In der Schweiz besteht im Bereich des Datenschutzes eine Parallelität von Bundesrecht und kantonalem Recht. Nebst dem bundesrechtlichen Datenschutzgesetz, welches unter Privaten und gegenüber Bundesbehörden gilt, haben auch Kantone eigene Datenschutzgesetze, die mit Bezug auf kantonale Behörden zur Anwendung kommen. Da sehr viele Netzbetreiber zur kantonalen Verwaltung im weiteren Sinne zählen (Kantonswerke), würden auf solche Netzbetreiber kantonale Gesetze zur Anwendung kommen. Die sich daraus ergebende Rechtszersplitterung im Datenschutz kann insbesondere im Anwendungsbereich des Smart Metering sowohl auf Seiten der Netzbetreiber aber auch auf Seiten der Konsumenten zu Rechtsunsicherheit führen und z. B. eine einheitliche Regelung im Zusammenhang mit Meter-Daten verunmöglichen. Auch im Smart Grid können sich Unsicherheiten längerfristig in Abhängigkeit der konkreten Ausgestaltung der Anwendungsfälle ergeben. Solche Rechtsunsicherheiten hindern Investitionen und können einer optimalen Nutzung des Potenzials im Wege stehen.

Eine mögliche Anwendbarkeit eines Datenschutzgesetzes (z.B. jenes des Bundes), welches für Datensicherheit aber auch für Datenschutz Regelungen trifft, führt bereits bei den hier untersuchten Anwendungsfällen zu Rechtsunsicherheiten. Namentlich enthält die Datenschutzgesetzgebung in der Regel keine sektorspezifischen, sondern allgemeine Regeln, deren Anwendung in einem konkreten Fall u.U. erhebliche Interpretationsspielräume offen lässt.

Um die Datensicherheit und den Datenschutz in Bezug auf Vertraulichkeit (C), Integrität (I) und Verfügbarkeit (A) mittel- bis langfristig zu gewährleisten, lassen sich Anforderungen gemäss Tabelle M3 abgrenzen, die von den IKT System erfüllt werden müssen. Für die Festlegung der konkreten und angemessenen Massnahmen pro Bereich und der dahingehend ggf. zu erarbeitenden oder zu konkretisierenden Standards ist eine fallbezogene Risikoanalyse (Eintrittswahrscheinlichkeit und Auswirkungsgrad) zielführend. Diese Risikobetrachtung sollte vor einer Festlegung bzw. Erarbeitung der Standards für die abgegrenzten Kategorien erfolgen. Zusätzlich zu diesen Anforderungen sollten gewisse übergeordnete, betriebliche und technische Anforderungen und Anforderungen zur Nachvollziehbarkeit berücksichtigt werden, die derzeit auf einer europäischen Ebene empfohlen werden (ENISA, 2012).

Bereich	Anforderungen and Datenschutz und Datensicherheit
Vertraulichkeit (C)	• Entsorgung von Komponenten Systemen • Accountmanagement • Zugriffsschutz • Geschützter Fernzugriff • Netzwerktrennung • Sichere Kommunikation
Integrität (I)	• Konfigurationsmanagement • Wartung der Komponenten und Systeme

	• Informationssicherheit (Schutz gegen Angriffe von aussen)
Verfügbarkeit (A)	• Unterbrechungsfreier Betrieb • Kommunikationssysteme für Ereignisfälle

eneinander Tabelle M3: Anforderungen an die fortschreitende Standardisierung im Bereich Datensicherheit und Datenschutz in Smart Grids gemäss CIA-Analyse.

abgrenzen, die von den IKT System erfüllt werden müssen. Für die Festlegung der konkreten und angemessenen Massnahmen pro Bereich und der dahingehend ggf. zu erarbeitenden oder zu konkretisierenden Standards ist eine fallbezogene Risikoanalyse (Eintrittswahrscheinlichkeit und Auswirkungsgrad) zielführend. Diese Risikobetrachtung sollte vor einer Festlegung bzw. Erarbeitung der Standards für die abgegrenzten Kategorien erfolgen. Zusätzlich zu diesen Anforderungen sollten gewisse übergeordnete, betriebliche und technische Anforderungen und Anforderungen zur Nachvollziehbarkeit berücksichtigt werden, die derzeit auf einer europäischen Ebene empfohlen werden (ENISA, 2012). Aufgrund der Heterogenität der Netzbetreiber in der Schweiz wird eine Umsetzung, welche schliesslich die Anforderungen erfüllt, je nach Grösse des Netzbetreibers variieren.

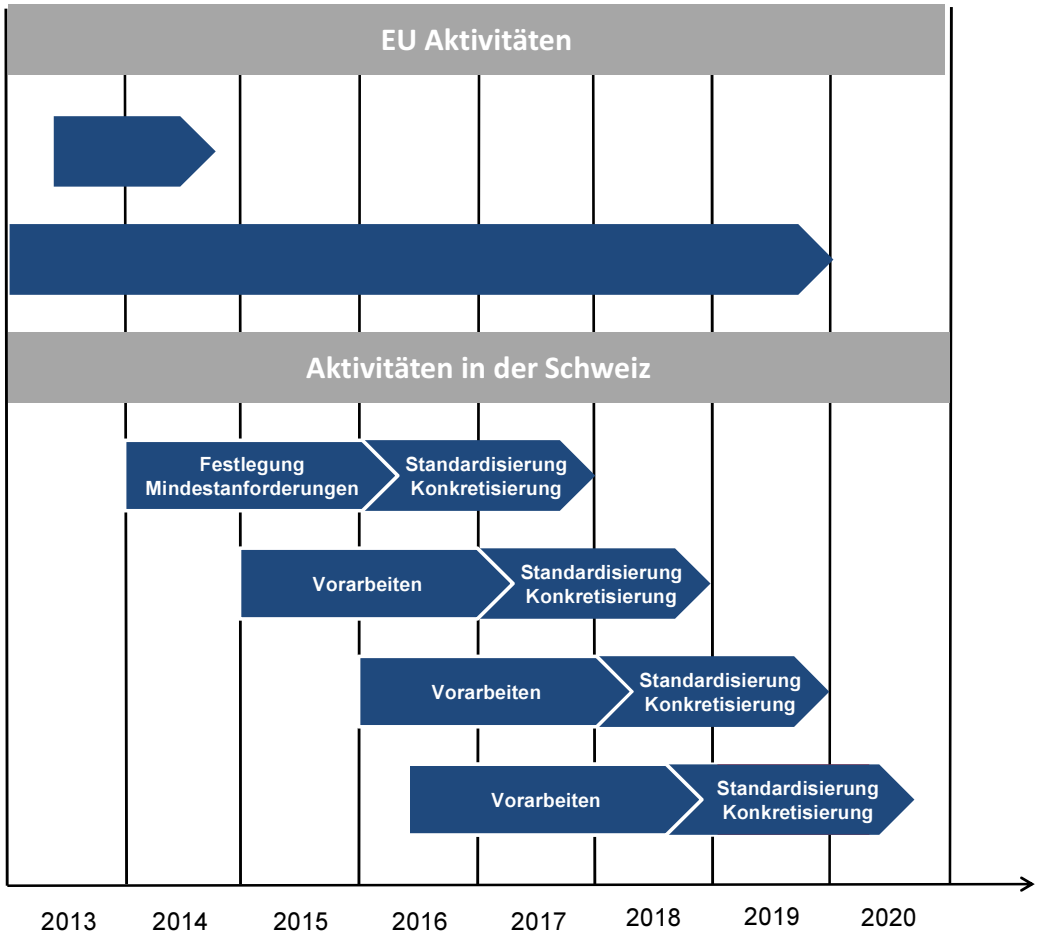


Abbildung M2: Zeitliche Anordnung der regulatorischen Massnahmen zu Smart Grids.

Aus diesen Überlegungen lässt sich grob ein Zeitplan für weitere technische Standardisierungsarbeiten sowie dafür ggf. regulatorische Anpassungen im Rahmen von Smart Grids ableiten, der gesamthaft in Abbildung dargestellt ist. Standardisierungsarbeiten laufen auf europäischer Ebene bereits in allen ausgewiesenen Standardisierungskategorien. Hierbei stehen jedoch Arbeiten in der Schweiz im Bereich der intelligenten Messsys-

teme beim Endverbraucher sowie im Umgang mit den Prosumerdaten im Vordergrund (Europäische Kommission, 2011; CEN-CENELEC-ETSI Smart Grid Coordination Group, 2012b). Gerade hinsichtlich des Umgangs mit den Prosumer Daten besteht ein Handlungsbedarf, da im Umgang mit diesen Daten bisher noch wenig geregelt ist und datenschutzrelevante Fragen hier treibend sind. Eine Einführung von intelligenten Messsystemen, wie sie in der Schweiz vorgesehen ist, würde durch ungeklärte Fragen in diesem Bereich gehindert werden. Aufgrund eines zukünftig vollständig geöffneten, schweizweiten Marktes sind harmonisierte, nationale Regelungen in diesen beiden Standardisierungskategorien als prioritär zu betrachten. Des Weiteren sind aber auch in den anderen Kategorien entsprechende Arbeiten durchzuführen. Innerhalb der Schweiz ist zu geeigneten Fragestellungen, die in Vorarbeiten zu identifizieren sind, ein Standardisierungsprozess in Gang zu setzen. Hierbei sollten Anwendungsfälle identifiziert werden wofür vorhandene Standards vor allem im Bereich Datensicherheit konkretisiert werden, die die genannten Anforderungen erfüllen. Eine Einigung auf gewisse Standards ist Schweizweit wichtig. Dieser Prozess ist vor allem subsidiär anzustreben aber zu gewissen Fragestellungen von öffentlichem Interesse und bei absehbaren Marktversagen kann der Bund Vorgaben machen.

Alle Standardisierungsarbeiten sind vor dem Hintergrund der internationalen Standardisierungsarbeiten zu sehen. Hier ist insbesondere der Standardisierungsprozess auf europäischer Ebene zu nennen, der bereits läuft. Im Mandat 490 wird eine Referenzarchitektur erarbeitet, ein Rahmen für relevante Standards im Bereich Smart Grids erstellt und ein fortlaufender Normungsprozess aufgesetzt. Des Weiteren werden grundlegenden Empfehlungen für Informationssicherheit im Bereich Smart Grids getroffen. Hierbei konnten schon zahlreiche Ergebnisse erzielt und international gültige Standards publiziert werden.

3. Aktuelle Arbeiten und Dokumente

Im Rahmen dieser Studie wurden bestehende Studien und Berichte, auch der umliegenden Länder, berücksichtigt, insofern sie für die Erarbeitung von schweizerischen Vorgaben und Standards zielführend und anwendbar sind. Die Studie referenziert daher insbesondere auf bestehende Analysen und Empfehlungen der EU bezüglich Datenschutz und Datensicherheit. Ebenfalls wurde die Entwurfsfassung der Smart Grid Roadmap Schweiz einbezogen.

Die Betrachtung der europäischen Arbeiten im Rahmen des Mandats M/490 [1], welche erste Vorgaben zu einer Referenzarchitektur, Use Cases und Standards hervorgebracht haben, sind hervorzuheben.

Smart Grid Coordination Group – Smart Grid Reference Architecture

In diesem Bericht der Smart Grid Coordination Group (SG-CG) [6] wird eine Referenzarchitektur für Smart Grids beschrieben, mit Fokus auf folgende Aspekte:

- Ermöglichung einer gemeinsamen Diskussionsbasis bezüglich einer Smart Grid Architekturansicht und einer gemeinsamen diesbezüglichen Sprache.
- Integration eines state-of-the-art Ansatzes mit europäischen Eigenheiten.
- Aufführung von Basismethoden zur Analyse und Evaluierung alternativer Implementierungen im Rahmen der Referenzarchitektur.
- Unterstützung bei Änderungen von bestehenden Architekturen hin zu einer Smart Grid Architektur.

- Bereitstellung von Kriterien zur Sicherstellung der Konformität mit identifizierten relevanten Standards und mit Anforderungen an die Interoperabilität.

Smart Grid Coordination Group – Sustainable processes

In diesem Bericht [7], welcher ebenfalls durch das Mandat M/490 in Auftrag gegeben wurde, sind die mögliche Use Cases im Smart Grid aufgeführt.

- Beschreibung des Aufbaus, der Strukturierung und der Klassifizierung der Use Cases sowie der Prozesse zum Aufbau und zur Pflege der Use Cases.
- Entwicklung von Smart Grid Use Case Gruppierungen.
- Beschreibung der dort entwickelten Use Case Management Repository (UCMR).

Die auf einer hohen Flughöhe beschriebene Use Cases der SG-CG Studie sind nicht auf die vorliegende Studie anwendbar, da die Use Cases im vorliegenden Bericht sich konkreter auf die darin vorkommenden Datenobjekte und Datenflüsse beziehen.

Smart Grid Coordination Group – First set of standards

In dieser Studie [5], welche ebenfalls durch das Mandat M/490 in Auftrag gegeben wurde, werden Standards aufgelistet, welche im Smart Grid Umfeld je nach Technologie zur Anwendung kommen sollten. Diese Auflistung führt sämtliche zu standardisierende Themenfelder im Smart Grid Umfeld auf, wobei die Informationssicherheit ebenfalls ein Bestandteil ist. In der Studie werden Standards aufgeführt, welche für die Smart Grid Technologien angepasst werden sollten.

ENISA – Appropriate security measures for smart grids

Der Bericht der ENISA (European Network and Information Security Agency) [3] stellt eine Wegleitung dar, zur Festlegung minimaler Sicherheitsanforderungen und -Massnahmen in einem Smart Grid System. Das Vorgehen und die zu definierenden Massnahmen wurden für die vorliegende Studie kontextbezogen adaptiert und wo sinnvoll übernommen.

BFE – Zustandsanalyse und Entwicklungsbedarf von Technologien für ein Schweizer Smart Grid

In dieser Studie [8] wurden Technologien im Smart Grid Umfeld analysiert und kategorisiert. Dabei wurden sowohl neue als auch bereits bekannte Technologien bezüglich der anstehenden Herausforderungen betrachtet. Die ICT-relevanten Technologien dienten in der vorliegenden Studie als Basis für die Anwendungsfälle (Use Cases).

4. Vorgehen

4.1. Vorgehensmethodik

Die Studie wurde in drei Arbeitspakete aufgeteilt. Die Zwischenresultate der Arbeitspakete wurden jeweils in einer Arbeitsgruppe mit Vertretern verschiedener Interessensgruppen diskutiert, ergänzt und bereinigt.

Arbeitspaket 1: ICT Architektur Smart Grids

Als erstes wurden die für die Datensicherheit und den Datenschutz im Smart Grid relevanten zukünftigen Anwendungsfälle identifiziert und als Use Cases detailliert beschrie-

ben. Die Use Cases enthalten die relevanten Informationen zu den involvierten Rollen und deren Aufgaben, den eingesetzten Komponenten sowie die benötigten Datenobjekte und Datenflüsse. Aus den einzelnen Use Cases wurde anschliessend eine konsolidierte Gesamtübersicht der Datenflüsse sowie eine übergreifende ICT-Architektur erstellt, inklusive den konsolidierten Rollen und Datenflüssen.

Arbeitspaket 2: Richtlinien und Standards

Im zweiten Arbeitspaket wurden zunächst die bestehenden Standards und Richtlinien in der Schweiz sowie im internationalen Umfeld bezüglich Datensicherheit in Smart Grids beigezogen und auf Basis der Berichte der Smart Grid Coordination Group [4], [5] und ENISA [3], [4] der aktuelle Stand in diesem Zusammenhang ermittelt.

Zur Eruierung möglicher Massnahmen in Bezug auf Datensicherheit im Smart Grid Umfeld dienten die auf Best-Practice basierenden ENISA-Anforderungen (Kapitel 9.2).

Anschliessend wurde eine Beurteilung nach CIAN (Kapitel 4.4.1) in der Gesamtübersicht der Use Cases auf die einzelnen bzw. thematisch gruppierten Datenobjekte vorgenommen. Daraus resultierte eine Gesamtsicht des Datensicherheitsbedarfs im Smart Grid, welcher Gegenstand des zukünftigen Standardisierungsbedarfes im Umfeld der Datensicherheit ist.

Aus diesem gesamten Standardisierungsbedarf konnten Kategorien abgeleitet werden, nach welchen zukünftige Standards und Richtlinien bzgl. Datensicherheit in Smart Grids gegliedert werden sollten. Die Ausarbeitung dieser Standards und Richtlinien ist jedoch nicht Gegenstand der vorliegenden Studie.

Arbeitspaket 3: Datenschutz

Im dritten Arbeitspaket wurden die aktuellen Gesetze und Richtlinien sowie Erfahrungswerte aus der Schweiz und dem internationalen Umfeld analysiert.

Anschliessend wurden pro Use Case die Datenobjekte, wo sinnvoll zusammengefasst, hinsichtlich des Datenschutzes identifiziert und beschrieben. Dabei wurden sowohl der Dateninhalt, die Datenverwendungszwecke sowie die beteiligten Rollen einbezogen. Basierend auf dieser Analyse wurden die relevanten Datenschutzfragestellungen und entsprechende Lösungsansätze analysiert.

4.2. Use Cases

In einem ersten Schritt wurden mögliche Use Cases und die zugehörigen Rollen, Datenobjekte und Datenflüsse, Kommunikationswege und Komponenten identifiziert. In Kapitel 5 sind die zwölf für die Datensicherheit und den Datenschutz identifizierten relevanten Use Cases beschrieben und grafisch dargestellt. Der grafische Aufbau der Use Cases ist exemplarisch in Abbildung 1 aufgezeigt.

In den folgenden Abschnitten werden die Inhalte der einzelnen Bestandteile der Darstellung beschrieben.

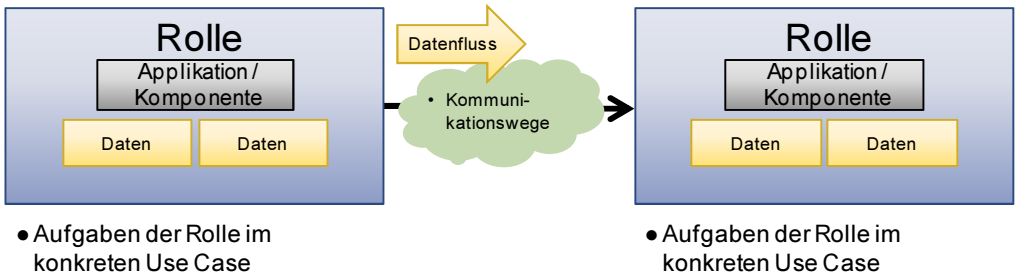


Abbildung 1: Darstellung der Use Cases

Rollen

Die Rollen beschreiben die zur Ausführung der Use Cases erforderlichen primären Aufgaben im Kontext dieser Studie. Die Rollen zeigen auf, bei wem Daten anfallen können, die einen allfälligen Datensicherheits- oder Datenschutzbedarf aufweisen. Es wird keine Aussage dazu gemacht, welche Akteure diese Rollen ausführen werden. In einigen Fällen ist es denkbar, dass ein Akteur mehrere Rollen wahrnehmen kann, oder eine in dieser Studie identifizierte Rolle zukünftig auf mehrere Akteure aufgeteilt wird. Zum Beispiel werden im Rahmen dieser Studie die Rollen „Datenmanager“ und „Verteilnetzbetreiber“ getrennt betrachtet, im Sinne zukünftiger möglicher Rollenvarianten. Es ist jedoch nicht Absicht der Studie, zukünftige diesbezügliche Richtungsentscheide oder Analysen vorwegzunehmen. Die identifizierten Rollen sind:

Rolle	Beschreibung
Prosumer / Verbraucher	Der Prosumer ist gleichzeitig der Einspeiser (**Pro**ducer) und der Endverbraucher (Con**sumer**) ins Stromnetz und befindet sich normalerweise in der Netzebenen 5 oder 7. Unter diesem Begriff werden im Bericht sowohl reine Endverbraucher, reine dezentrale Einspeiser als auch deren Kombination zusammengefasst. Die beim Prosumer anfallenden Datenobjekte, also innerhalb der Geräte ab Netzanschluss der Netzebenen 5-7 (z.B. in den Messsystemen), werden für diese Studie zwecks Analyse des Datenschutz- und Datensicherheitsbedarfs ihm zugeordnet.
Datenmanager (DM)	Der Datenmanager stellt die Schnittstelle für die Energie- und Netzdaten des Prosumers dar, welche von ihm gemessen, verwaltet, verarbeitet und an die relevanten Datenempfänger übermittelt werden. Er empfängt Daten und gibt Daten weiter, je nach Anwendungsfall aggregiert oder anonymisiert. Diese Rolle kann sowohl eigenständig sein, aber auch auf eine oder mehrere andere Rollen verteilt werden. Heute ist die Rolle des Datenmanagers dem Verteilnetzbetreiber zugeordnet.
Verteilnetzbetreiber	Der Verteilnetzbetreiber ist für den Betrieb und Unterhalt des Verteilnetzes zuständig und verantwortet als Solcher die Versorgungssicherheit in seinem Netzgebiet.

Übertragungsnetzbetreiber	Der Übertragungsnetzbetreiber ist für den Betrieb und Unterhalt des Übertragungsnetzes zuständig und verantwortet die Versorgungssicherheit im Übertragungsnetz.
Erzeuger	Der zentrale Erzeuger erzeugt elektrische Energie und speist diese in die Netzebenen 1-3 ein.
Systemdienstleistungs-Verantwortlicher (SDV)	Der SDV ist verantwortlich für die kommerzielle und operative Planung und Ausführung der SDL und die entsprechende Verteilung der abgerufenen Regelenergie auf die beteiligten leistungsvorhaltenden Anlagen.
Energielieferant	Der Energielieferant ist zuständig für die Energielieferung an seine Endkunden (Prosumer).
Dienstleister Gebäudeautomation	Der Dienstleister Gebäudeautomation ist eine mögliche zukünftige Rolle, welche mittels Anbindung an die Gebäudeautomation Hausautomations-Dienstleistungen anbieten kann.
Marktpartner	Weitere Marktpartner können zukünftig beliebige weitere Dienstleistungen anbieten und werden entsprechend unter dem Sammelbegriff „Marktpartner“ subsumiert. Da die Marktpartner auch auf diverse Smart Grid Datenobjekte zugreifen müssen, sind deren Datensicherheit und der Datenschutz zu berücksichtigen. Heutiges Beispiel solcher Marktpartner ist der Bilanzgruppenverantwortliche.

Applikation / Komponente

Die Komponenten sind Hard- oder Software und dienen dazu, die Daten innerhalb einer Rolle zu speichern, verwalten, aufnehmen, messen und bearbeiten. Den Komponenten sind sowohl physische Komponenten (z.B. Transformatoren und Messsysteme) als auch Applikationen (z.B. fürs Datenmanagement oder für Optimierungsberechnungen) zugeordnet.

Für diese Studie wird angenommen, dass die Qualität und Richtigkeit der Daten innerhalb der Komponenten gegeben ist, z.B. dass die Datenobjekte in den Messsystemen korrekt und in der geforderten Präzision erstellt und vorgehalten werden. Eichrechtliche relevante Betrachtungen werden nicht weiter betrachtet und als Voraussetzung angenommen.

Daten / Datenfluss

Als Datenobjekt werden alle Informationen bezeichnet, die erfasst, übertragen, gespeichert und verarbeitet werden. Im Rahmen dieser Studie sind in einem Datenobjekt mehrere thematisch subsumierte Informationen innerhalb des jeweils beschriebenen Verwendungszwecks repräsentiert. So werden z.B. im Datenobjekt „Meteringdaten“ sowohl die heute schon gemessene Wirkleistung, als auch weitere denkbare am Zähler entstehenden Informationen zusammengefasst, wie die Blindleistung oder weitere Kennzahlen zur Spannungsqualität. Diese Verallgemeinerungen wurden aus Gründen der Komplexität gewählt, indem eine für die Beurteilung der Datensicherheit und des Datenschutzes ausreichende Detailtiefe mit deren entsprechend grundsätzlichen Inhalt gewählt wurde.

Des Weiteren können der Umfang und der Detaillierungsgrad der Daten jeweils pro Rolle unterschiedlich sein, auch wenn es sich um dieselbe Bezeichnung handelt. So können dem Prosumer über sein Messsystem im Datenobjekt „Meteringdaten“ mehr Informatio-

nen zur Verfügung gestellt werden, als anderen Marktpartnern. Die Beurteilung des Datensicherheits- und Datenschutzbedarfs wurde pro Rolle vorgenommen, womit diese Unterschiede berücksichtigt wurden.

Kommunikationswege

Die Datenobjekte werden über Kommunikationsinfrastrukturen und –Technologien zwischen den Rollen und deren Komponenten übermittelt. Im Rahmen dieser Studie wird davon ausgegangen, dass die heute verfügbaren Technologien auch zukünftig eingesetzt und keine gesetzlichen Vorgaben einzelne Technologien im Smart Grid festlegen werden. Die Akteure werden also die aus wirtschaftlichen und technischen Perspektiven sinnvollen Technologien einsetzen, solange sie die nötigen Funktionalitäten in den Use Cases erfüllen und die zukünftig festzulegenden Sicherheitsanforderungen erfüllen.

Die möglichen Kommunikationstechnologien sind

- Unternehmenskommunikation (WAN):
  - Layer 1, Layer 2
  - Legacy
- Endkundenkommunikation (Access, z.B. Local Metrological Network):
  - Shared Internet Access
  - Dedicated Access
  - Shared Mobile Access
- Inhouse-Bereich (LAN / Haus-LAN):
  - Cabled LAN / Haus-LAN
  - Wireless LAN / Haus-LAN
  - Shortrange Wireless LAN / Haus-LAN

Die Bezeichnungen werden in den nachfolgenden Use-Cases zu Darstellungszwecken zusammengefasst.

4.3. ICT Architektur

Die Use Cases wurden zu einem Gesamtbild der ICT Architektur zusammengeschlossen. Dafür wurden alle Komponenten und Datenobjekte der Rollen zusammengeführt und alle Datenflüsse und ihre Kommunikationswege zwischen den Rollen aufgezeigt. Die ICT Architektur zeigt die Zusammenhänge zwischen den Rollen und Komponenten auf und gibt einen Überblick über die Datenmengen sowie die zahlreichen Datenflüsse. Dabei wird sowohl die domänenbasierte Referenzarchitektur gemäss der Smart Grid Coordination Group [6] als auch die Datenfluss-Architektursicht dargestellt. Auf Basis dieser ICT Architektur wurde der Datensicherheitsbedarf, der Datenschutz sowie der Standardisierungsbedarf ermittelt.

4.4. Standardisierungsbedarf

4.4.1. Einschätzung der Datensicherheit und des Datenschutzes

Der Datenschutz ist ein wesentlicher Bestandteil der Beurteilung ob und in welchem Mass Daten einen Sicherheitsbedarf aufweisen. Im Folgenden wird darauf eingegangen, wie mit der Datensicherheitsbedarf ermittelt und beurteilt werden kann.

Generell wird die Beurteilung und die daraus resultierenden Sicherheitsmassnahmen pro Datenobjekt präziser, je genauer die die Funktionalitäten und Inhalte der Use Cases definiert sind.

Der Datensicherheitsbedarf wurde gemäss Best-Practice anhand der Sicherheitskriterien Confidentiality - „C“ (Vertraulichkeit), Integrity – „I“ (Integrität), Availability – „A“ (Verfügbarkeit) und Non-repudiation – „N“ (Nachvollziehbarkeit) beurteilt. Diese Beurteilung wird kurz „CIA“ oder „CIAN“ genannt. Dabei wurde jeweils analysiert, ob die Daten aus Sicht der Versorgungssicherheit oder des Datenschutzes sicherheitsrelevant sind:

- Versorgungssicherheit: Es ist notwendig, dass die Daten zum Beispiel kontinuierlich und korrekt an den relevanten Stellen zur Verfügung stehen, damit die Versorgung zu jeder Zeit gewährleistet werden kann. Die Daten sind zur Gewährleistung der Versorgungssicherheit im betroffenen Netzgebiet von hoher Relevanz.
- Datenschutz: Die Informationen betreffen schützenswerte Personen- oder Firmendaten, welche vor Zugriff durch unberechtigte geschützt werden müssen. Die Daten sind aus juristischen Gründen im Sinne des Datenschutzes schützenswert.

Für die Beurteilung wurden die Daten jeweils pro Kriterium in die Kritikalitätsstufen „kritisch“ oder „unkritisch“ eingestuft. Auf detailliertere Abstufungen wurde im Rahmen dieser Studie verzichtet, da der grundsätzliche Bedarf und nicht die konkreten Massnahmen eruiert werden sollen. Nachfolgend werden die Sicherheitskriterien und zugewiesenen Kritikalitätsstufen erläutert:

- „C“ – Vertraulichkeit:
  Schutz der Daten vor Zugriff durch Unbefugte. Der Schutz umfasst alle technischen und organisatorischen Massnahmen gegen unberechtigte und unzulässige Einsicht, sowie Bekannt- und Weitergabe von Daten über deren gesamten Lebenszyklen hinweg.

  Kritisch:

  Die betroffenen Daten sind als vertraulich einzustufen, indem sie aus juristischen Gründen (Datenschutz) oder aus Sicht der (Gefährdung der) Versorgungssicherheit im betroffenen Netzgebiet nicht öffentlich zugänglich sein dürfen. Geschäftssensible Daten mit wettbewerblichen Auswirkungen (Vertriebsdaten, Handelsdaten etc.) und ohne Datenschutzauswirkungen gelten in diesem Sinne nicht als kritisch.

  Unkritisch:

  Die betroffenen Daten sind nicht als vertraulich einzustufen. Bei Offenlegung besteht keine Gefährdung der Versorgungssicherheit und es bestehen keine juristischen Einschränkungen.

- „I“ – Integrität:
  Schutz der Daten vor unerlaubter Manipulation. Der Schutz umfasst alle technischen und organisatorischen Massnahmen gegen unberechtigtes und unzulässiges Erzeugen, Verändern oder Entfernen von Daten über deren gesamten Lebensdauer (erstellen, speichern, kopieren, übertragen, löschen, …) hinweg. Die Integrität impli-

ziert die Korrektheit (Unversehrtheit), Zuverlässigkeit und Vollständigkeit von Daten sowie die korrekte Funktionsweise datenverarbeitender Systeme und Diensten.

Kritisch:

Die betroffenen Daten müssen vertrauenswürdig und vor Manipulation geschützt sein. Mangelnde Integrität kann eine Verletzung des Datenschutzes oder eine Gefährdung der Versorgungssicherheit im betroffenen Netzgebiet nach sich ziehen.

Unkritisch:

Bei Manipulation der betroffenen Daten besteht keine Gefährdung der Versorgungssicherheit oder des Datenschutzes im betroffenen Netzgebiet.

- „A“ – Verfügbarkeit:
  Sicherstellen, dass die Daten über deren gesamten Lebenszyklen hinweg auf Anfrage eines berechtigten Subjekts (Person, System oder Dienst) zugänglich und benutzbar sind. Die Verfügbarkeit impliziert den Schutz gegen Zerstörung und Verlust sowie die Zuverlässigkeit und die korrekte Funktionsweise von datenverarbeitenden Systemen und Diensten.

  Kritisch:

  Die betroffenen Daten müssen in einem definierten Mass[5] zur Verfügung stehen. Kurzzeitige Ausfälle können bereits negative Auswirkungen auf die Versorgungssicherheit im betroffenen Netzgebiet nach sich ziehen.

  Unkritisch:

  Kurzzeitige Ausfälle haben keine Auswirkungen auf die Versorgungssicherheit im betroffenen Netzgebiet.

- „N“ – Nachvollziehbarkeit:
  Sicherstellen, dass die Zugriffe auf Daten, die Ein- und Weitergabe von Daten, sowie das Erzeugen, Ändern, Entfernen und Löschen von Daten rückverfolgbar, nachweisbar und zurechenbar sind. Nachvollziehbarkeit umfasst auch die Änderungen (Changes) an datenverarbeitenden Systemen und Diensten.

  Kritisch:

  Die Arbeit an und der Zugriff zu den betroffenen Daten müssen aufgrund des sensiblen Charakters der Daten zwingend nachvollzogen werden können (zumindest wer, wann und was durchgeführt hat). Dabei gilt die Nachvollziehbarkeit als kritisch, falls entweder „C“, „I“ oder „A“ als kritisch eingestuft werden.

  Unkritisch:

  Weder „C“, noch „I“ oder „A“ werden für die betroffenen Daten als kritisch eingestuft.

4.4.2. Standardisierungskategorien

Der Standardisierungsbedarf wurde nach der Beurteilung des Datensicherheits- und Datenschutzbedarfs ermittelt. Basierend auf bestehenden Standards und Richtlinien in der Schweiz und in Europa wurde das Gesamtbild der Use Cases für den Zweck dieser Studie in Standardisierungskategorien unterteilt. Die Unterteilung in Kategorien wurde thematisch unter Berücksichtigung der angenommenen Entwicklung gewählt, so dass bestehende Standards und geplante Technologien jeweils in einer Kategorie abgebildet werden können. Von einer Standardisierungskategorie können beliebig viele Technologien und damit auch Standards betroffen sein, da es sich um eine übergreifende Katego-

[5] Die Bestimmung der erforderlichen Verfügbarkeiten ist nicht Gegenstand der vorliegenden Studie.

risierung handelt Die Gliederung soll die Priorisierung und den zeitlichen Ablauf bei der Standardisierung unterstützen.

Die Standardisierungskategorien sollen aufzeigen, in welchen prinzipiellen Themenblöcken weitere zukünftige Standards und Richtlinien zur Datensicherheit und zum Datenschutz zu erstellen sind. Auf Basis des europäischen ENISA-Dokumentes [3] werden mögliche prinzipielle Typen von Anforderungen an die Datensicherheit aufgezeigt. Diese sind jedoch nur als Hilfestellung gedacht – die Festlegung der zukünftigen Anforderungen ist nicht Teil dieser Studie, sondern soll im Rahmen der zukünftigen Standarderstellung vorgenommen werden. Eine diesbezüglich mögliche Standardisierungs-Roadmap wird entsprechend aufgezeigt.

5. Use Cases

Basierend auf den bestehenden sowie den antizipierten Technologien im zukünftigen Netz wurden die jeweiligen Anwendungsfälle, sogenannte Use Cases, entwickelt. Diejenigen Use Cases welche mit Informations- und Kommunikationstechnologien funktionieren werden als Datensicherheitsrelevant, resp. Datenschutzrelevant eingestuft und müssen entsprechend näher betrachtet werden.

In den folgenden Kapiteln werden zwölf für die Datensicherheit und den Datenschutz relevante Use Cases beschrieben, welche die Umsetzung der Funktionalitäten unterstützen. Diese setzen sich zusammen aus

- Rollen, welche im Anwendungsfall beteiligt sind
- Komponenten, welche die Ausführung des Anwendungsfalls unterstützen
- Datenobjekten, welche für den Anwendungsfall benötigt werden
- Kommunikationswege mit Datenflüssen, welche die Datenobjekte zwischen den Rollen und Komponenten übermitteln. Die Pfeile der Datenflüsse geben dabei jeweils die Datenflussrichtung an.

Durch die einzelne Betrachtung der Use Cases lässt sich anschliessend eine Gesamtübersicht zu den relevanten Datenobjekten und Datenflüssen im Smart Grid zusammenstellen, zwecks Analyse der Datensicherheit.

5.1. Use Case 1 – Datenmanagement

5.1.1. Definition

Dieser Use Case beinhaltet die Automatisierung und Optimierung des Austauschs und der Aufbereitung der Energie- und Netzdaten (Meteringdaten) zur Weiterverwendung zu Abrechnungs- und Prognosezwecken.

Der Datenmanager empfängt Meteringdaten aus dem Messsystem des Prosumers. Diese werden vom Datenmanager aufbereitet und den Zielrollen Energielieferanten, Verteilnetzbetreiber und weitere Marktpartner (z.B. Bilanzgruppenverantwortliche) zugesandt. Je nach Empfänger können die Datenobjekte unterschiedlich aggregiert zur Verfügung gestellt werden. Der Verteilnetzbetreiber und der Energielieferant verwenden die Meteringdaten primär zu deren Abrechnungs- und Prognosezwecken. Die primäre Aufgabe des Datenmanagers ist die Aufbereitung und die Zustellung der Daten so dass alle Vorgaben und Gesetze zum Schutz des Prosumers eingehalten werden.

Abbildung 2 auf Seite 30 stellt diesen Use Case dar.

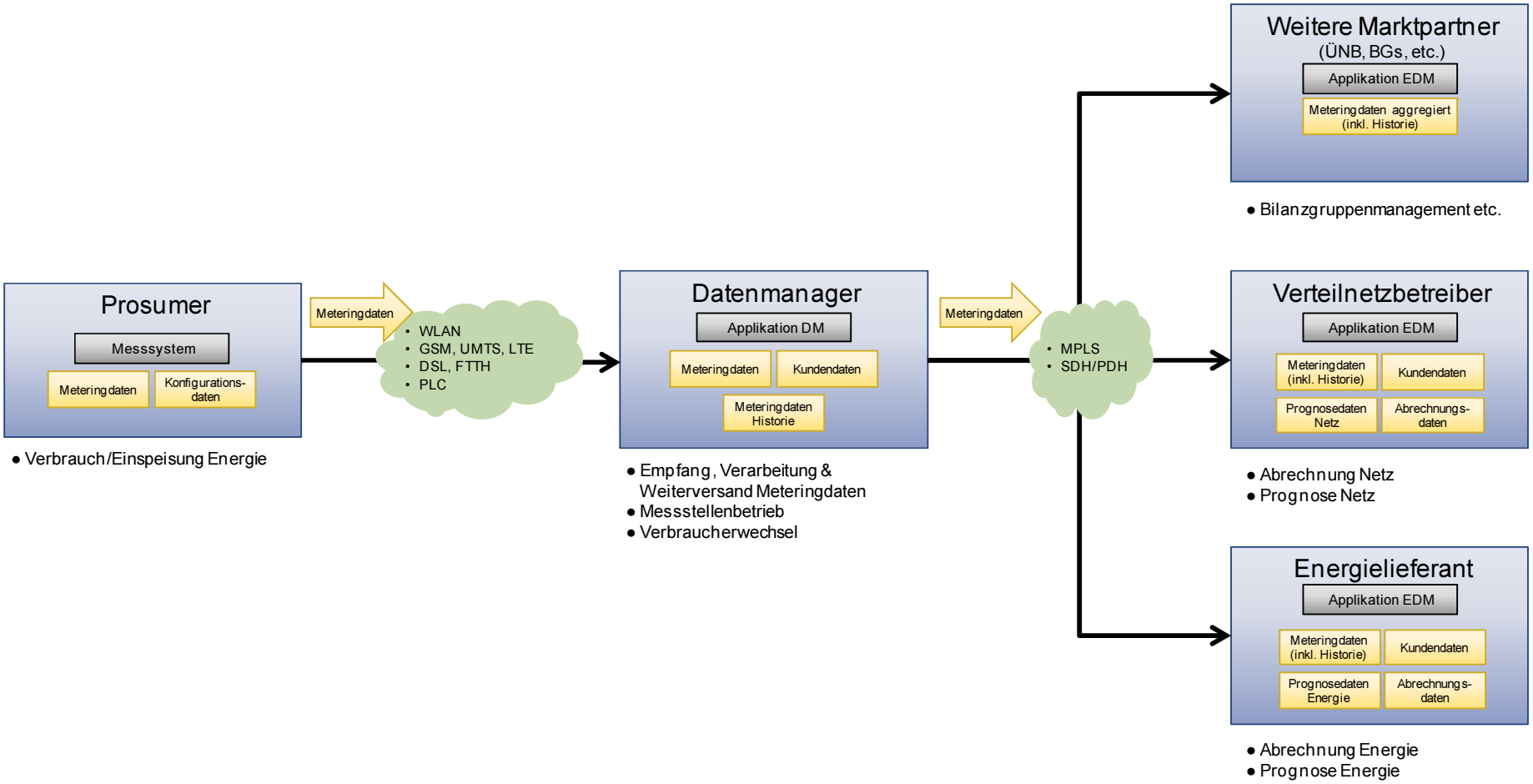


Abbildung 2: Use Case 1 – Datenmanagement

5.1.2. Rollen

Datenmanager:

Der Datenmanager empfängt die Meteringdaten (Energiedaten und Netzdaten) der Prosumer. Diese werden je nach Zweck aggregiert und anonymisiert. Anschliessend werden die aufbereiteten Meteringdaten an die Zielstelle weitergeleitet. Je nach Zielstelle können diese Datenobjekte in unterschiedlicher Granularität oder Umfang zur Verfügung gestellt werden.

Des Weiteren ist der Datenmanager für den Messstellenbetrieb und die Kundenwechselprozesse beim Prosumer zuständig.

Wie oben erwähnt, werden im Rahmen dieser Studie die Rollen „Datenmanager“ und „Verteilnetzbetreiber“ im Sinne zukünftiger möglicher Rollenvarianten getrennt betrachtet, obwohl sie heute identisch sind. Es ist nicht Absicht der Studie, zukünftige diesbezügliche Richtungsentscheide oder –Analysen vorwegzunehmen.

Prosumer/Verbraucher:

Ein Messsystem misst beim Netzanschluss des Prosumers dessen Energieverbrauch, seine Energieeinspeisung sowie ggf. weitere Daten, welche für das elektrische Netz und dessen Management sinnvoll sein könnten. Die so generierten Meteringdaten werden an den Datenmanager weitergeleitet

Verteilnetzbetreiber

Erhält die für seine Rolle relevanten und aufbereiteten Meteringdaten der Prosumer über den Datenmanager. Diese Messdaten werden anschliessend zu Abrechnungs- und Prognosezwecken weiterverwendet.

Energielieferant sowie weitere Marktpartner

Vom Datenmanager können der Energielieferant und weitere Marktpartner die jeweils spezifisch für den Verwendungszweck relevanten und aufbereiteten Meteringdaten beziehen. Je nach Aufgabe des Marktpartners werden die Daten für unterschiedliche Zwecke weiterverwendet.

5.1.3. Komponenten

Messsystem – Prosumer:

Die Messsysteme messen die Ein- und Ausspeisung beim Prosumer. Neuere und zukünftige Messsysteme können Informationen auch bidirektional übermitteln und so zu einer Steuerung der Ein- und Ausspeisung beitragen.

Das Messsystem liefert Meteringdaten an den Datenmanager. Die Periodizität und Qualität der Daten können je nach Zweck und Bestimmung unterschiedlich ausgelegt sein.

Applikation DM – Datenmanager:

Die Applikation Datenmanagement empfängt die Meteringdaten vom Prosumer.

Die Meteringdaten werden durch den Datenmanager verwaltet, aufbereitet und gespeichert sowie den jeweiligen Empfängern weitergeleitet. Je nach Zweck werden die Daten vor der Weiterleitung aggregiert oder anonymisiert.

Applikation EDM – Verteilnetzbetreiber, Energielieferanten und weitere Marktpartner:

Die Applikation Energiedatenmanagement empfängt und verwaltet die Prosumer Daten und bereitet sie für die Weiterverwendung oder Archivierung auf. Im Gegensatz zum Datenmanager erhält die Applikation EDM je nach Aufgabe und Verwendung aggregierte Daten z.B. in geringerer Granularität.

Die Meteringdaten werden beim Verteilnetzbetreiber und dem Energielieferanten für den Zweck der Abrechnung und Prognose aufbereitet. Bei allen Marktpartnern werden die Meteringdaten je nach Bestimmung dem Zweck entsprechend aufbereitet.

5.1.4. Datenobjekte

Meteringdaten – Messsystem, Applikation DM, Applikation EDM:

Die Meteringdaten können alle am Messpunkt gemessenen Datenobjekte enthalten. Dazu gehören sowohl die Wirkleistung, als auch die Blindleistung und weitere Kennzahlen zur Spannungsqualität, wie zum Beispiel Flickerwerte, 15-Minuten Werte (Spannung, Frequenz), etc.

Es ist offen, wem welche Datenobjekte in welcher Granularität in Zukunft zur Verfügung gestellt werden können. Grundsätzlich ist jedoch davon auszugehen, dass die Datenobjekte zweckmässig erhoben werden. Beim Prosumer können umfangreiche Datenobjekte erfasst und gespeichert werden. Je nach Bestimmungszweck werden die notwendigen Datenobjekte an den Datenmanager weitergeleitet, welcher diese Datenobjekte für die Zielstelle aufbereitet. Die Zielstelle erhält die Datenobjekte im Umfang und in der Granularität, welche für deren Zweck notwendig ist. Die Zielstellen speichern und verwalten die Datenobjekte im Sinne von historischen Meteringdaten.

Konfigurationsdaten – Messsystem

Beim Messsystem fallen Konfigurationsdaten an (z.B. Zugriffsberechtigungen), die nicht zuletzt für Sicherheitszwecke verwendet werden.

Kundendaten – Applikation DM, Applikation EDM

Die Kundendaten enthalten die Informationen zu den Kunden, die für den Verwendungszweck erfasst wurden (Name, Adresse etc.).

Abrechnungsdaten – Applikation EDM

Die Abrechnungsdaten enthalten abrechnungsrelevante Datenobjekte, die für die Abrechnung der Energielieferung oder Netznutzung verwendet werden.

Prognosedaten Netz / Energie – Applikation EDM

Beim Verteilnetzbetreiber und bei dem Energielieferanten werden Prognosewerte erstellt, die für deren netz- und energiewirtschaftlichen Planungen und Optimierungen verwendet werden.

Zur Berechnung der Prognosewerte dienen sowohl aktuelle als auch historische Meteringdaten.

5.1.5. Kommunikation

Die Kommunikation zwischen dem Datenmanager und dem Prosumer erfolgt über bestehende Kommunikationstechnologien im Access-Bereich. Die Kommunikation zwischen dem Datenmanager und den restlichen Rollen erfolgen primär über bestehende WAN-Technologien.

5.2. Use Case 2 – Demand Side Response

5.2.1. Definition

Mit dem Demand Side Response sollen Möglichkeiten zur Verfügung gestellt werden, um die Verbraucherpartizipation mittels Anreizsignalen und Systemzustandsdaten aktiv zu beeinflussen. Je nach Automatisierungsstufe in den Komponenten oder geeignetem Verhalten des Prosumers, kann auf die Signale reagiert und so die Versorgungssicherheit optimiert werden. Anreizsignale können dabei dynamische Tarife, Energiepreise, Verhaltensstatistiken oder weitere beliebige Signale zur Steuerung eines nachhaltigen Konsumverhaltens darstellen. Systemzustandsdaten sollen dem Prosumer die Möglichkeit geben, unter Berücksichtigung seiner Präferenzen zugunsten des Versorgungssystems zu agieren.

Abbildung 3 auf Seite 34 stellt diesen Use Case dar.

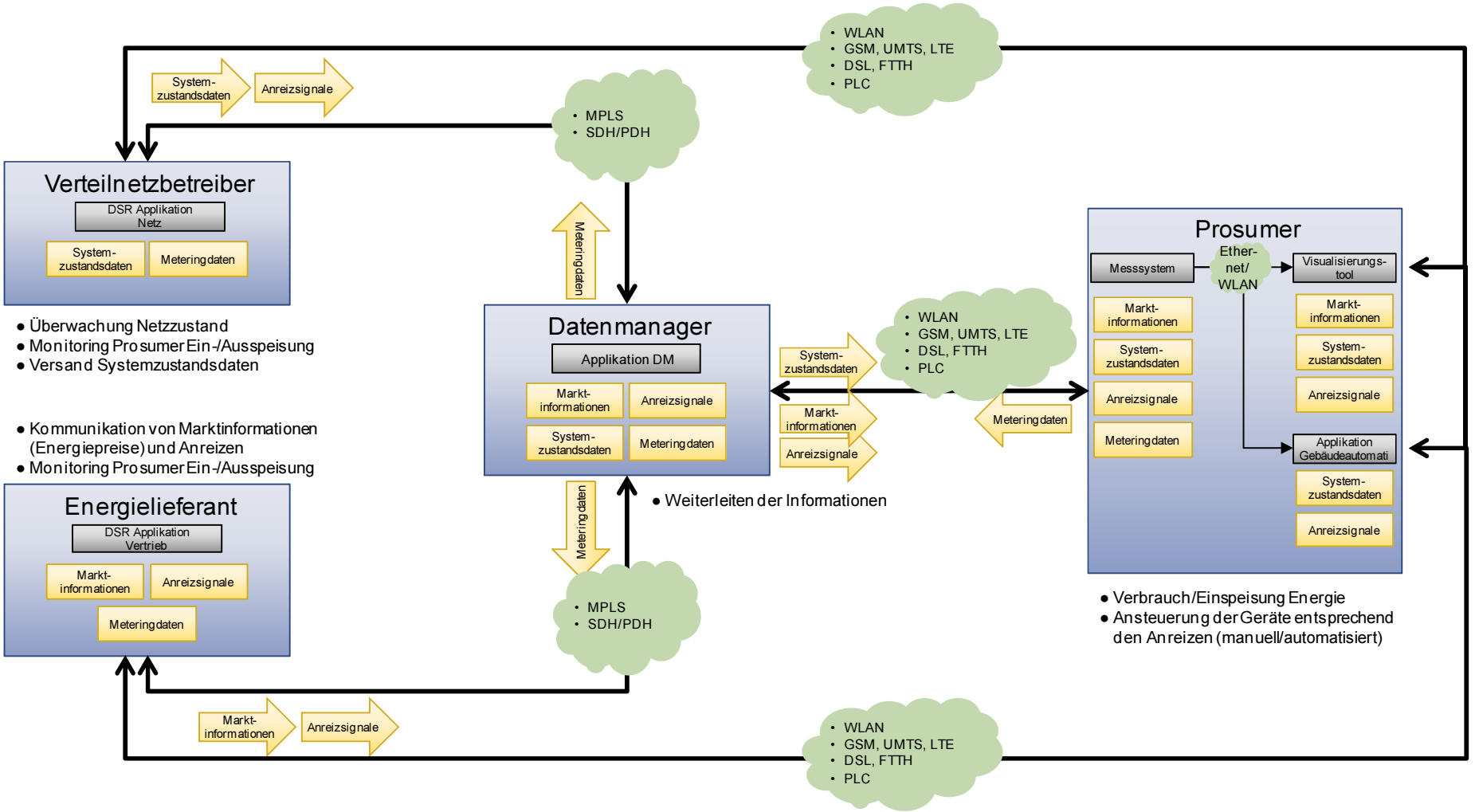


Abbildung 3: Use Case 2 – Demand Side Response

Die Partizipation des Prosumers kann derart das Ein-/Ausspeiseverhalten und dementsprechend die Netzauslastung beeinflussen und somit gezielt durch den Verteilnetzbetreiber oder Energielieferanten zur Optimierung eingesetzt werden. Es muss darauf geachtet werden, dass die Stimulierung durch Anreizsignale und weiteren Informationen durch die unterschiedlichen Rollen ohne Konflikte bezüglich der Versorgungssicherheit erfolgt. Dazu können z.B. die Datenübermittlungen abgestimmt, Grenzwerte festgelegt, oder klare Prioritäten zugeordnet werden. Es interagieren dazu also zumindest der Verteilnetzbetreiber und der Energielieferant. Vorstellbar sind jedoch auch andere Rollen, die aus Marktgründen auf das DSM Potenzial zugreifen. Eine Abstimmung mit dem VNB ist jedoch wichtig/zwingend.

5.2.2. Rollen

Verteilnetzbetreiber:

Der Verteilnetzbetreiber kann aus den Meteringdaten und den internen Netzzustandsdaten mögliche Optimierungen des Netzbetriebs berechnen. Mittels Systemzustandsdaten oder weiteren Anreizsignalen erhält der Prosumer direkt oder via Datenmanager Informationen, auf die er reagieren kann.

Energielieferant:

Der Energielieferant kann aus den Meteringdaten und der aktuellen Marktsituation Optimierungsmöglichkeiten für das Prosumerverhalten berechnen. Mittels Marktinformationen oder beliebigen Anreizsignalen erhält der Prosumer direkt oder via Datenmanager Informationen, auf die er reagieren kann.

Datenmanager:

Je nach Kommunikationsweg der Datenobjekte erhält der Datenmanager die Systemzustandsdaten und die Anreizsignale vom Verteilnetzbetreiber und dem Energielieferanten und leitet diese an die Prosumer weiter.

Generell werden die Daten von und zum Prosumer durch den Datenmanager verwaltet, aufbereitet und gespeichert sowie den jeweiligen Empfängern weitergeleitet. Je nach Zweck werden die Daten vor der Weiterleitung aggregiert oder anonymisiert.

Prosumer.

Der Prosumer empfängt Anreizsignale und/oder weitere Informationen zum Systemzustand. Auf diese wird automatisiert oder manuell durch den Prosumer gemäss dessen Konfigurationen oder Bedürfnissen reagiert.

5.2.3. Komponenten

DSR Applikation – Verteilnetzbetreiber

In der DSR Netzapplikation werden aus den vorhandenen Datenobjekten (interne Daten des Verteilnetzbetreibers, sowie Meteringdaten) die Optimierungsmöglichkeiten (Potentiale, Wahrscheinlichkeiten und Systemantworten) vor allem bezüglich der technischen und sicherheitsrelevanten Einflüsse abgeschätzt.

DSR Applikation – Energielieferant

In der DSR Vertriebsapplikation werden aus den vorhandenen Datenobjekten (interne Daten des Energielieferanten, Marktdaten sowie Meteringdaten) die Optimierungsmög-

lichkeiten (Potentiale, Wahrscheinlichkeiten, Systemantworten) hinsichtlich der technischen und sicherheitsrelevanten sowie finanziellen Einflüsse abgeschätzt.

Applikation DM – Datenmanager

Mit der Datenmanager-Applikation werden Datenobjekte vom Energielieferanten und vom Verteilnetzbetreiber an den Prosumer weitergeleitet.

Generell werden die Prosumerdaten durch den Datenmanager verwaltet, aufbereitet und gespeichert sowie den jeweiligen Empfängern weitergeleitet. Je nach Zweck werden die Daten vor der Weiterleitung durch die Applikation aggregiert oder anonymisiert.

Messsystem, Applikation Gebäudeautomation, Visualisierungstool – Prosumer

Der Prosumer empfängt die Anreizsignale, Marktdaten und Systemzustandsdaten. Es ist nicht vorgegeben, welche Komponenten hier exakt zum Einsatz kommen sollen. Prinzipiell wird es sich um ein Zusammenspiel des Messsystems, möglicher Visualisierungstools zur Darstellung der Informationen sowie gebäudeautomatisierender Applikationen handeln. Die Komponenten können entweder automatisiert oder mit Einwirken des Prosumers auf die Signale reagieren.

5.2.4. Datenobjekte

Systemzustandsdaten – DSR Applikation Netz, Applikation DM, Komponenten beim Prosumer

Die Systemzustandsdaten werden für die Berechnung der Optimierungsmöglichkeiten mit Demand Side Response in der Netzapplikation einbezogen und nach Bedarf dem Prosumer direkt oder via Anreizsignal zur Verfügung gestellt.

Marktinformationen – DSR Applikation Vertrieb, Applikation DM, Komponenten beim Prosumer

Die Marktinformationen (in der Regel Energiepreise) werden für die Optimierungsmöglichkeiten des Demand Side Response in der Vertriebsapplikation aufbereitet und nach Bedarf dem Prosumer direkt oder via Anreizsignal zur Verfügung gestellt.

Meteringdaten – Messsystem, Applikation DM

Die Meteringdaten können alle am Messpunkt gemessenen Daten enthalten. Für die Berechnung von Signalen, welche zur indirekten Steuerung der Prosumer beitragen können, werden die aktuellen Meteringdaten beigezogen.

Anreizsignale

Die Anreizsignale können auf beliebigen Ebenen (z.B. soziale, finanzielle, ideologische Anreize) den Prosumer zu einer Reaktion auffordern. Mit den Anreizsignalen wird bewusst keine direkte Steuerung vorgenommen, d.h. dem Prosumer wird die Wahl zur Reaktion überlassen.

5.2.5. Kommunikation

Die Kommunikation zwischen dem Prosumer und dem Datenmanager, dem Verteilnetzbetreiber oder dem Energielieferanten erfolgt über bestehende Kommunikationstechnologien im Access-Bereich. Die Kommunikation zwischen dem Datenmanager und dem Verteilnetzbetreiber und Energielieferanten erfolgt primär über bestehende WAN-Technologien.

Use Case 3 – Gebäudeautomatisierung

5.2.6. Definition

Dieser Use Case stellt die Integration des Gebäudes in das elektrische Netz dar. Beliebige Hausanwendungen und Endgeräte lassen sich hier potentiell über eine Gebäudeautomatisierung steuern, welche interoperable Schnittstellen zum elektrischen Netz aufweist. Durch die Interoperabilität wird gewährleistet, dass beliebige Marktanbieter Geräte mit den entsprechenden Schnittstellen anbieten können. Externe Dienstleister im Gebäudeautomationsumfeld bieten dabei zukünftig diverse Dienstleistungen an, welche von Prosumern bei Bedarf in Anspruch genommen werden. Diese Dienstleistungen können rein visueller Natur sein, indem aufbereitete Informationen zur Verfügung gestellt werden, oder Steuersignale beinhalten, zwecks Automatisierung bestimmter Abläufe. Unter anderem sind auch Szenarien zur Unterstützung des Netzbetriebs denkbar. Die möglichen Dienstleistungen werden hier aber nicht weiter spezifiziert.

Abbildung 4 auf Seite 38 stellt diesen Use Case dar.

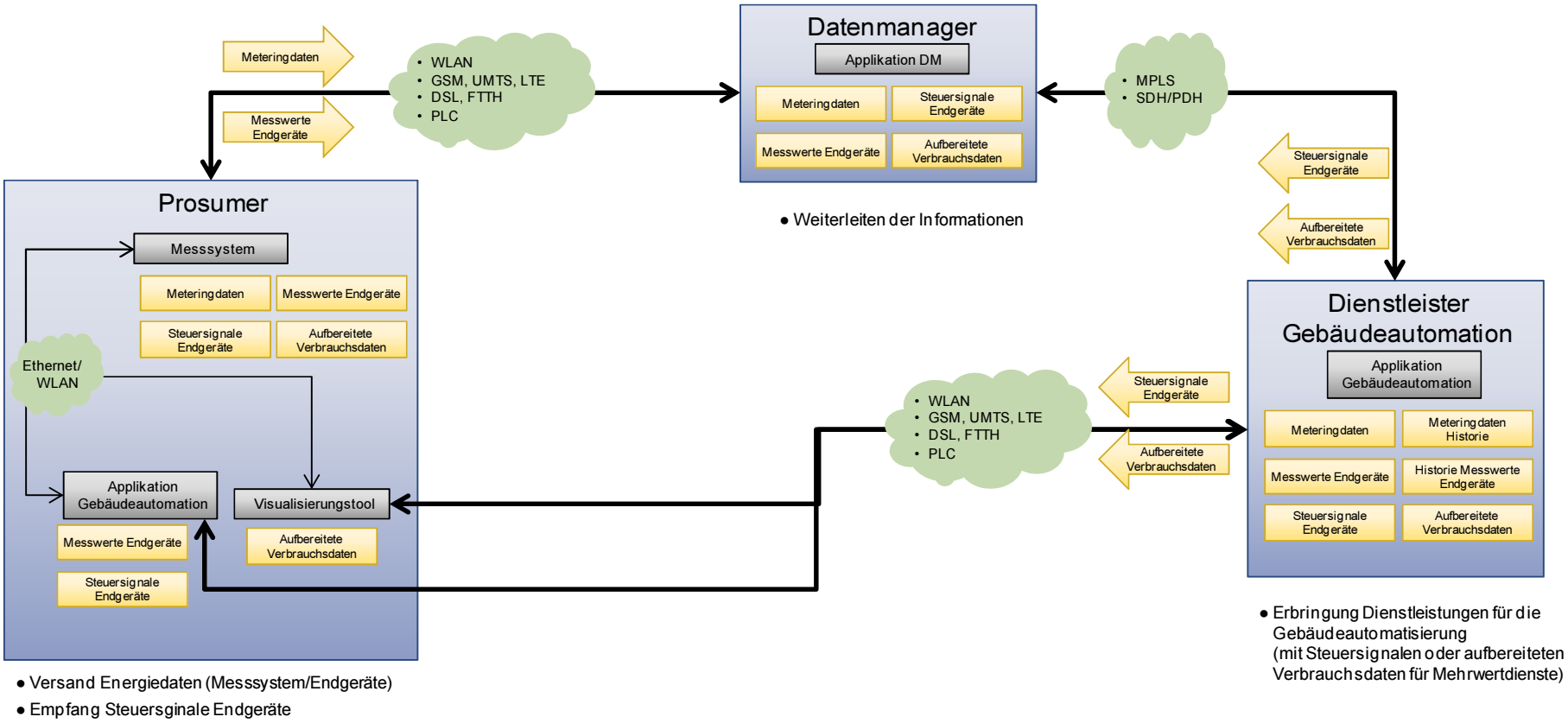


Abbildung 4: Use Case 3 – Gebäudeautomatisierung

5.2.7. Rollen

Dienstleister Gebäudeautomation

Der Dienstleister Gebäudeautomation bietet dem Prosumer Dienstleistungen im Umfeld der Hausautomation an. Diese Dienstleistungen sind nicht Bestandteil der Grundversorgung und betreffen den Einbezug von an der Gebäudeautomation angeschlossenen Geräten.

Datenmanager

Der Datenmanager kann je nach Kommunikationsweg der Datenobjekte den Datenfluss von und zum Dienstleister Gebäudeautomation bezüglich Art, Periodizität und Form steuern. Er stellt somit sicher, dass die Daten entsprechend ihres Verwendungszweckes (und nicht darüber hinaus) beim Dienstleister Gebäudeautomation zur Verfügung gestellt werden.

Prosumer

Der Prosumer kann Dienstleistungen für seine Gebäudeautomation in Anspruch nehmen.

5.2.8. Komponenten

Applikation Gebäudeautomation – Dienstleister Gebäudeautomation, Prosumer

Mit der Applikation Gebäudeautomation wird die Gebäudeautomation vom Prosumer, unter Berücksichtigung entsprechender Interoperabilität, mit der Energieversorgung gekoppelt. Mit der Interoperabilität wird gewährleistet, dass Gebäudeautomationen unterschiedlicher Hersteller und mit unterschiedlicher Konfiguration eingebunden werden können. Dadurch kann die Dienstleistung unabhängig von den jeweiligen Geräteherstellern erbracht werden. Der Dienstleister Gebäudeautomation kann über seine Applikation je nach Bedarf Anreize oder Steuersignale an die teilnehmenden Prosumer senden. Beim Prosumer stellt diese Applikation die Verbindung zwischen den externen Signalen des Dienstleisters und der internen Gebäudeautomation dar. Diese ist letztendlich mit den Endgeräten verbunden, die mit entsprechend integrierten Algorithmen auf dieses Signale reagieren können.

Visualisierungstool – Prosumer

Im Visualisierungstool können Bestandteile der Dienstleistung Gebäudeautomation angezeigt werden, beispielsweise aufbereitete Verbrauchsdaten.

Messsystem – Prosumer

Für die Erbringung von Dienstleistungen für die Gebäudeautomation werden gegebenenfalls Messsysteme als Schnittstellengeräte einbezogen.

Applikation DM – Datenmanager

Mit der Datenmanager-Applikation werden die Datenobjekte zwischen dem Gebäudeautomationsdienstleiser und dem Prosumer ausgetauscht, sofern keine direkten Anbindungen bestehen.

Generell werden die Daten von und zum Prosumer durch den Datenmanager verwaltet, aufbereitet und gespeichert sowie den jeweiligen Empfängern weitergeleitet.

5.2.9. Datenobjekte

Messwerte Endgeräte

Je nach Dienstleistung in der Gebäudeautomation ist es notwendig, die aktuellen Messwerte der angebundenen Geräte zu kennen. Diese werden beim Prosumer gemessen und dem Dienstleister Gebäudeautomation zur Verfügung gestellt. Diese Daten können sowohl direkt dem Dienstleister Gebäudeautomation oder über den Datenmanager zur Verfügung gestellt werden. Dies ist abhängig von der zukünftigen Rolle des Datenmanager. Zusätzlich lassen sich je nach Anwendung die diesbezüglichen historischen Daten verwenden.

Steuersignale Endgeräte

Je nach Dienstleistung können die an der Gebäudeautomation angeschlossenen Geräte angesteuert werden. Diese Steuersignale werden beim Prosumer entweder direkt in einer der Endgeräte empfangen oder via ein Messsystem angesteuert, welches entweder an einem Smart Meter gekoppelt ist, oder separat z.B. mit der Gebäudeautomation verbunden ist.

Aufbereitete Verbrauchsdaten

Als Dienstleistung können die Verbrauchsdaten der Endgeräte nach Bedarf aufbereitet und zur Verfügung gestellt werden. Diese werden aus den vom Dienstleister Gebäudeautomation empfangenen Prosumer Daten aufbereitet und dem Prosumer beispielsweise über ein Visualisierungstool zur Verfügung gestellt. Hierzu können auch historische Daten, sowie Informationen im Dienstleistungsbereich (Hinweise mit dem Ziel Energie zu sparen, Fehlfunktionen von Geräten, etc.) zählen

Meteringdaten

Die Meteringdaten bilden zusammen mit den Messwerten der Endgeräte die Grundlage für die Aktivitäten des Dienstleisters Gebäudeautomation. Daraus können sowohl Steuersignale als auch aufbereitete Verbrauchsdaten erzeugt werden.

5.2.10. Kommunikation

Die Kommunikation zwischen dem Prosumer und dem Gebäudeautomationsdienstleister sowie gegebenenfalls dem Datenmanager erfolgt über bestehende Kommunikationstechnologien im Access-Bereich. Die Kommunikation zwischen dem Gebäudeautomationsdienstleister und dem Datenmanager erfolgt primär über bestehende WAN-Technologien.

5.3. Use Case 4 - Systemdienstleistungen

5.3.1. Definition

Im Smart Grid lassen sich die Systemdienstleistungen optimieren, indem diese von allen Netznutzern angeboten werden können, im Einklang mit den lokalen Gegebenheiten in den Verteilernetzen. Insbesondere lässt sich durch sogenannte Aggregatoren eine Vielzahl verteilter und steuerbarer Anlagen, sowohl Produktionsanlagen als auch Lasten und Speicher, in das Systemdienstleistungsangebot integrieren. Der Aggregator übernimmt dabei als sogenannter SDL-Verantwortlicher (SDV) die Aufgaben des Angebotsmanagements gegenüber dem Regelzonenbetreiber und der Verteilung und gezielten Ansteuerung des SDL Abrufs. Anbieter von SDL können sowohl zentrale Erzeuger als auch Prosumer sein.

Abbildung 5 auf Seite 42 stellt diesen Use Case dar:

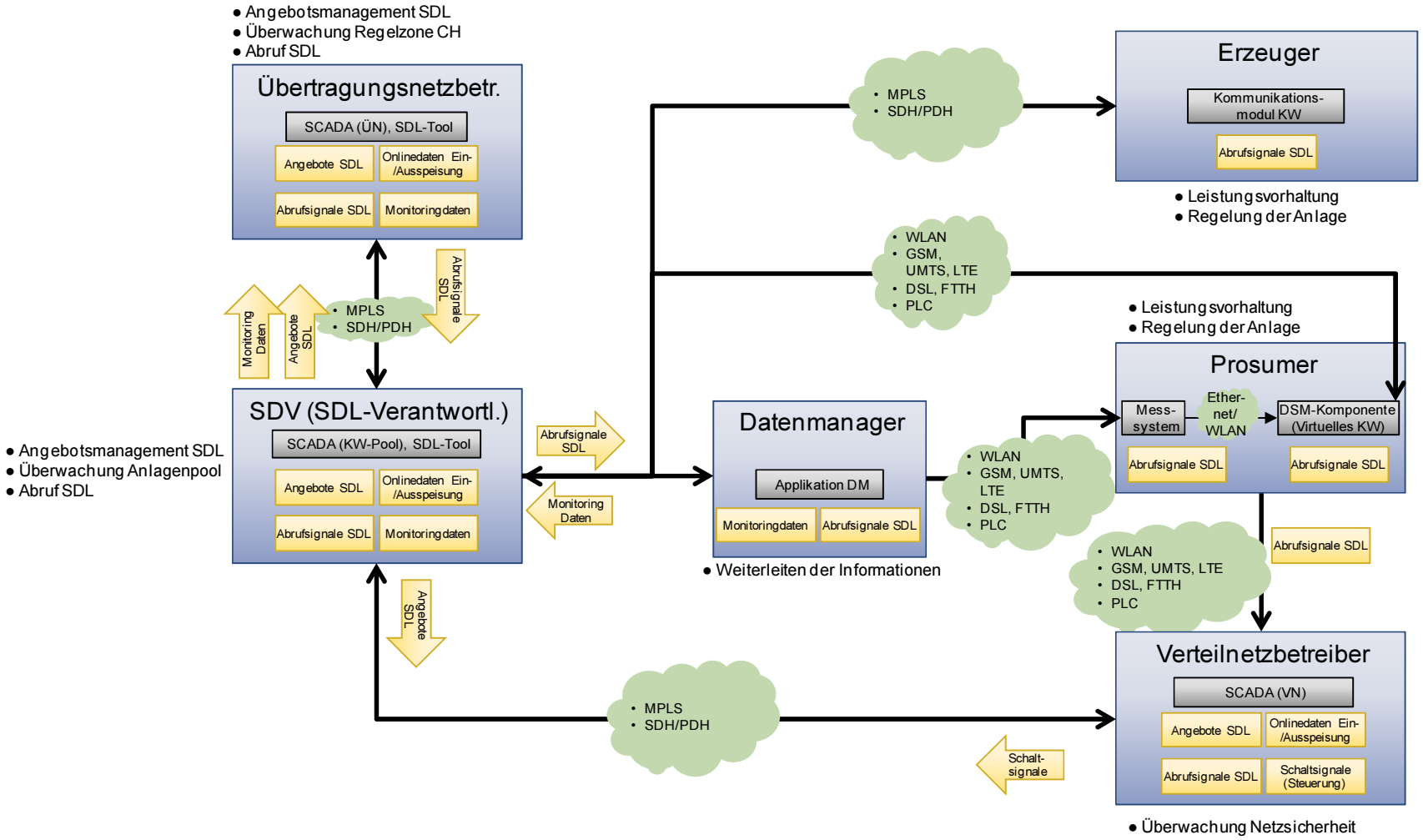


Abbildung 5: Use Case 4 – Systemdienstleistungen

5.3.2. Rollen

SDV (SDL-Verantwortlicher)

Der SDV ist verantwortlich für die kommerzielle und operative Planung und Ausführung der SDL und die entsprechende Verteilung der abgerufenen Regelenergie auf die beteiligten leistungsvorhaltenden Anlagen. Im Falle von verteilten Anlagen, welche zusammen einen Anlagenpool zur Erbringung der Systemdienstleistungen bilden, stellt der SDV den Aggregator dar.

Übertragungsnetzbetreiber

Der Übertragungsnetzbetreiber überwacht und regelt die Regelzone Schweiz und ruft für die Erhaltung der Versorgungssicherheit die Systemdienstleistungen nach Bedarf ab.

Erzeuger, Prosumer

Prosumer und zentrale Erzeuger können mit ihren Anlagen SDL anbieten, welche sie vorhalten und bei Abruf zur Verfügung stellen müssen. Sie können auch als Zusammenschluss im Sinne eines virtuellen Kraftwerks teilnehmen. Die Teilnahme am SDL Markt bedingt, dass dem SDV Monitoringdaten zur Verfügung gestellt werden, um die SDL Vorhaltung zu überprüfen.

Verteilnetzbetreiber

Der Verteilnetzbetreiber sollte, je nach Umfang der gesteuerten Anlagen, über die SDL Angebote und Abrufe in seinem Versorgungsgebiet informiert sein, zwecks Überwachung der Netzstabilität und Durchführung von die SDL-Signale übersteuernden Schalthandlungen im Bedarfsfall.

Datenmanager

Der Datenmanager ist für die Datenübertragung zwischen dem Prosumer und dem SDV zuständig, sofern diese nicht direkt untereinander angebunden sind.

5.3.3. Komponenten

SDL-Tool – SDV

Mit dem SDL-Tool werden die SDL-Angebote kommerziell geplant und verwaltet.

SCADA [6](KW Pool) – SDV

Mit dem SCADA werden die angebotenen Leistungsscheiben überwacht und bei Bedarf, d.h. bei empfangenem Abrufsignal des Übertragungsnetzbetreibers, abgerufen.

SCADA (ÜN), SDL-Tool – Übertragungsnetzbetreiber

Mittels SCADA- und SDL-Funktionalität überwacht der Übertragungsnetzbetreiber die Regelzone Schweiz und ruft die angebotenen SDL nach Bedarf ab.

Kommunikationsmodul KW, Messsystem, DSM-Komponente (Virtuelles KW) – Erzeuger, Prosumer

Diese Module und Komponenten sind für die Vorhaltung, Ansteuerung und Erbringung der SDL bei den SDL-anbietenden Anlagen verantwortlich.

[6] Unter der Komponente SCADA werden alle SCADA Daten sowie die Dienste / Applikationen des Leitsystems verstanden.

SCADA (VN)

Der Verteilnetzbetreiber erhält Informationen zu den angebotenen SDL in seinem Netzgebiet. Dadurch kann bereits im Vorfeld die Sicherheit berechnet werden und potentielle Gegenmassnahmen können frühzeitig oder spätestens im Betrieb lanciert werden. Somit kann sichergestellt werden, dass die regionale Versorgungssicherheit auch bei Einsatz der überregionalen SDL erhalten bleibt.

Applikation DM – Datenmanager

Mit der Datenmanager-Applikation werden die Datenobjekte zwischen dem SDV und dem Prosumer ausgetauscht, sofern keine direkten Anbindungen bestehen.

Generell werden die Daten von und zum Prosumer durch den Datenmanager verwaltet, aufbereitet und gespeichert sowie den jeweiligen Empfängern weitergeleitet.

5.3.4. Datenobjekte

Angebote SDL – SDV, Verteilnetzbetreiber, Übertragungsnetzbetreiber

Die Informationen zu den SDL Angeboten enthalten die kaufmännischen und leistungsbezogenen Details und werden vom SDV dem Übertragungsnetzbetreiber angeboten sowie ggf. je nach Grösse der zu steuernden Anlagen dem Verteilnetzbetreiber weitergeleitet.

Onlinedaten Ein- / Ausspeisung – SDV, Verteilnetzbetreiber, Übertragungsnetzbetreiber

Diese Onlinedaten stellen Informationen über gemessene Ein- und Ausspeisungen in Echtzeit zur Verfügung und dienen zur Überwachung der Netzstabilität und Erkennung des Bedarfs an SDL Abrufen bzw. im Falle des Verteilnetzbetreibers zur Erkennung von Netzsicherheitskonflikten bei der SDL-Erbringung.

Abrufsignale – alle beteiligte Rollen

Der Übertragungsnetzbetreiber ruft nach Bedarf SDL-Arbeit über den SDV ab. Dieser verteilt die SDL Abrufe je nach Angebot an die angeschlossenen Erzeuger und Prosumer. Zusätzlich könnte der Verteilnetzbetreiber diese Information erhalten, damit er bei Gefährdung seines regionalen Netzes gegebenenfalls Schaltsignale zur Übersteuerung der SDL Erbringung senden könnte.

Monitoringdaten – SDV, Übertragungsnetzbetreiber, Datenmanager

Die Vorhaltung der SDL bei den teilnehmenden Anlagen sollte vom SDV und dem Übertragungsnetzbetreiber laufend überwacht werden und daher sollten diese Daten dem SDV und dem Übertragungsnetzbetreiber zur Verfügung gestellt werden.

Schaltsignale – Verteilnetzbetreiber

Die Schaltsignale, welche die SDL Erbringung für einen Teil der Anlagen übersteuern, werden dem SDV mitgeteilt. Falls der Verteilnetzbetreiber solche Schaltungen durchführt, ist zusätzlich der Übertragungsnetzbetreiber über diese Eingriffe zu informieren. Generell ist in diesem Fall eine enge Abstimmung zwischen Verteilnetzbetreiber und Übertragungsnetzbetreiber wichtig, damit der Übertragungsnetzbetreiber darüber informiert ist, dass nicht seine vollumfänglich abgerufene Leistung vorliegt und demzufolge den SDV keine Schuld trifft.

5.3.5. Kommunikation

Die Kommunikation an der Prosumer-Schnittstelle (SDV, Verteilnetzbetreiber sowie gegebenenfalls Datenmanager) erfolgt über bestehende Kommunikationstechnologien im Access-Bereich. Die Kommunikation zwischen SDV, Übertragungsnetzbetreiber, Verteilnetzbetreiber, Erzeuger sowie gegebenenfalls Datenmanager erfolgt primär über bestehende WAN-Technologien.

5.4. Use Case 5 – Regionale Flexibilitäten

5.4.1. Definition

Zur Entlastung von regionalen Kapazitätsengpässen im Verteilnetz können Informationen des Netzes sowie der Ein- und Ausspeiser zusammengetragen werden. Mit diesen Informationen kann ein netzseitig optimierter Betrieb berechnet und mittels Steuerungen der Ein- und Ausspeisung, auch ausserhalb der nationalen Systemdienstleistungen, angestrebt werden. Mit diesem Use Case entsteht insbesondere die Möglichkeit regionale Leistungsflüsse zu beeinflussen.

Abbildung 6 auf Seite 46 stellt diesen Use Case dar:

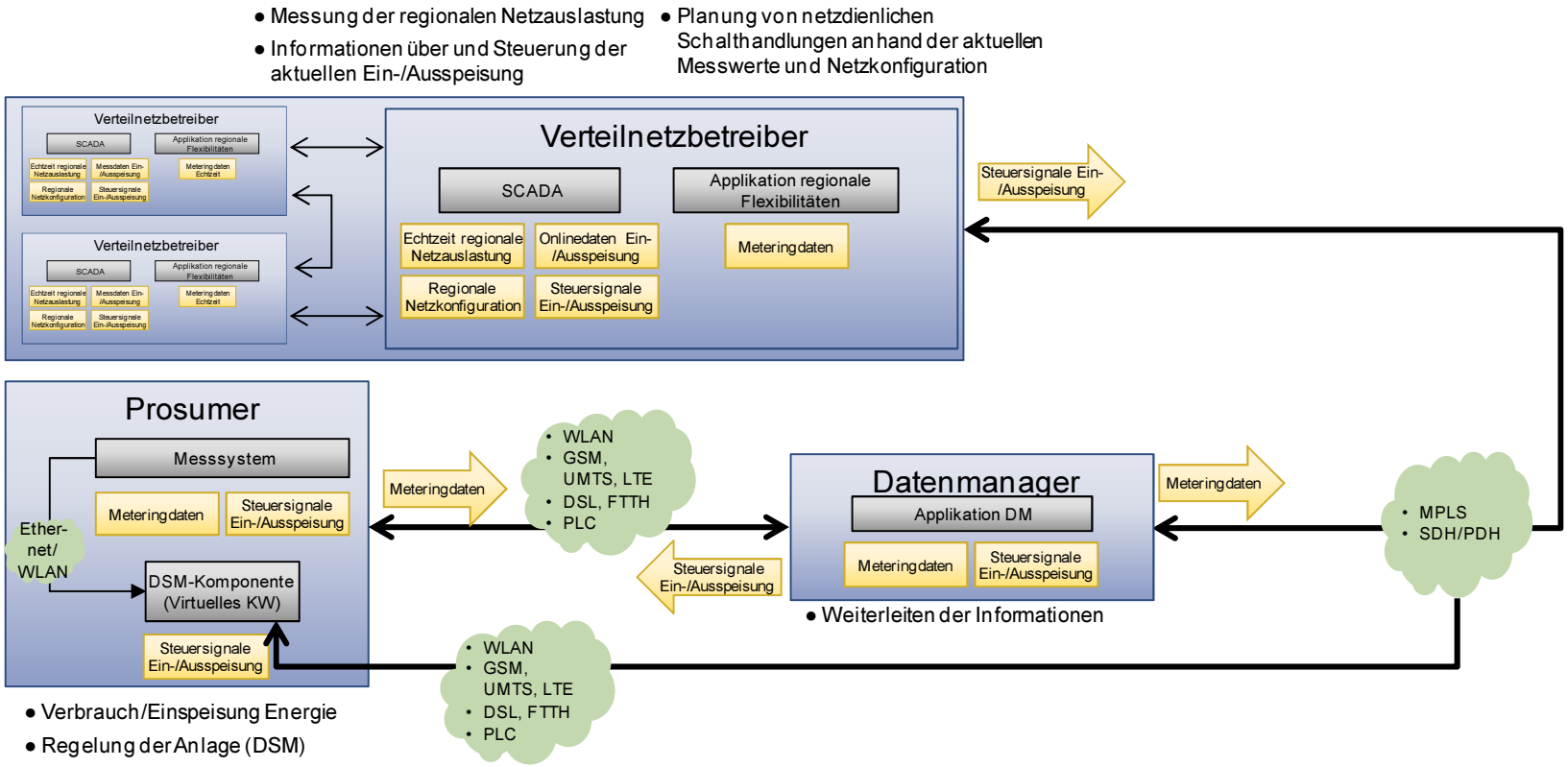


Abbildung 6: Use Case 5 – Regionale Flexibilitäten

5.4.2. Rollen

Verteilnetzbetreiber

Der Verteilnetzbetreiber misst die regionale Netzauslastung und berechnet aufgrund des aktuellen Zustands und der aktuellen Meteringdaten der Prosumer die Optimierungsmöglichkeiten für den Netzbetrieb. Für die vorausschauende Planung des Betriebs ist dies wichtig, da Eingriffe des Verteilnetzbetreibers in den Netzbetrieb reduziert werden können. Für die Umsetzung der Optimierungsmöglichkeiten sendet der Verteilnetzbetreiber Steuersignale direkt oder indirekt über den Datenmanager an die Prosumer.

Prosumer

Der Prosumer hat die Möglichkeit, auf die Steuersignale des Verteilnetzbetreibers netzdienlich mittels Demand Side Management (DSM) automatisiert oder manuell zu reagieren. Die Steuersignale werden bei ihm intern entweder über ein zentrales Messsystem oder direkt an die DSM-Komponente übermittelt.

Datenmanager

Der Datenmanager leitet die Meteringdaten und gegebenenfalls die Steuersignale jeweils zwischen dem Prosumer und dem Verteilnetzbetreiber weiter.

5.4.3. Komponenten

SCADA[7] – Verteilnetzbetreiber

Im SCADA System des Verteilnetzbetreibers wird der aktuelle Zustand des Netzes überwacht und die netzbetriebsrelevanten Informationen zusammengetragen. Aus dem Gesamtbild des Netzes können Instabilitäten oder Kapazitätsengpässe erkannt werden. Ebenfalls einzubeziehen sind hier die Netzkonfigurationsdaten, welche üblicherweise in GIS-Systemen verwaltet werden.

Applikation regionale Flexibilitäten – Verteilnetzbetreiber

Mit dem Gesamtbild zum Netzzustand, inklusive den Meteringdaten der Prosumer auf der untersten Netzebene, werden mit dieser Applikation detaillierte Analysen zur Netzauslastung sowie zu möglichen flexiblen Optimierungsmöglichkeiten vorgenommen. Zur Optimierung des Lastflusses können Steuersignale zur Steuerung der Ein- und Ausspeisung bei den Prosumern gesendet werden.

Messsystem, DSM-Komponente (Virtuelles KW) – Prosumer

Beim Prosumer werden mittels Messsystem die Meteringdaten dem Verteilnetzbetreiber zur Optimierung des Netzbetriebes zur Verfügung gestellt. Die vom Verteilnetzbetreiber berechneten Steuersignale für die Ein- und Ausspeisung werden anschliessend beim Prosumer entweder über das Messsystem oder direkt an einer DSM-Komponente empfangen.

Applikation DM – Datenmanager

Die Applikation DM leitet die Meteringdaten und die Steuersignale zwischen dem Prosumer und dem Verteilnetzbetreiber weiter.

[7] Unter der Komponente SCADA werden alle SCADA Daten sowie die Dienste / Applikationen des Leitsystems verstanden.

Generell werden die Daten von und zum Prosumer durch den Datenmanager verwaltet, aufbereitet und gespeichert sowie den jeweiligen Empfängern weitergeleitet.

5.4.4. Datenobjekte

Regionale Netzauslastung (Echtzeit), Onlinedaten Ein-/Ausspeisung, Regionale Netzkonfiguration – Verteilnetzbetreiber

Die aktuellen Zustandsdaten des Netzbetriebs werden beim Verteilnetzbetreiber zur Berechnung möglicher Optimierungen zusammengetragen.

Meteringdaten – Verteilnetzbetreiber, Prosumer, Datenmanager

Die Meteringdaten werden beim Prosumer erfasst und über den Datenmanager zum Verteilnetzbetreiber weitergeleitet. Dieser kann diese Datenobjekte für die Berechnung der Netzoptimierungen einbeziehen.

Steuersignale Ein-/Ausspeisung – Verteilnetzbetreiber, Prosumer, Datenmanager

Der Verteilnetzbetreiber berechnet für die Netzbetriebsoptimierung die relevanten Steuersignale für die Ein- und Ausspeisungen bei den Prosumern. Diese übermittelt er entweder über den Datenmanager oder direkt an den Prosumer.

5.4.5. Kommunikation

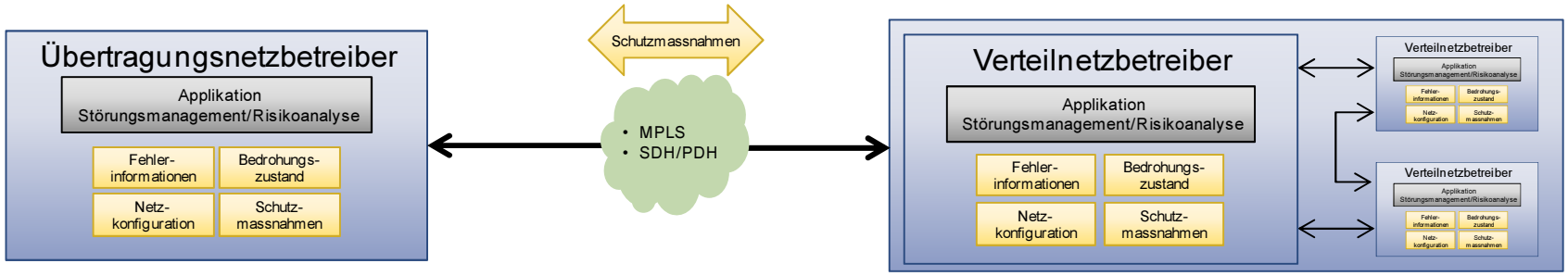
Die Kommunikation zwischen Prosumer und Verteilnetzbetreiber sowie gegebenenfalls dem Datenmanager, erfolgt über bestehende Kommunikationstechnologien im Access-Bereich. Die Kommunikation zwischen dem Verteilnetzbetreiber und dem Datenmanager erfolgt primär über bestehende WAN-Technologien.

5.5. Use Case 6: Schutzerhalt von Netzsystem und Daten

5.5.1. Definition

Für die Erkennung und Bekämpfung von Angriffen von aussen auf das Übertragungs- und Verteilnetz, sollen in diesem Use Case die relevanten Komponenten und ICT-Systeme im Netz überwacht und die sicherheitsrelevanten Daten analysiert werden. Derart soll jederzeit der aktuelle Bedrohungszustand des Netzes einschätzbar sein. Mit einer automatisierten Überprüfung von Zugriffen und Unregelmässigkeiten sollen systemrelevante, physische Schwachstellen identifiziert, Angriffe oder unter Umständen auch Schwachstellen frühzeitig erkannt und Gegenmassnahmen rechtzeitig und automatisiert ergriffen werden können.

Abbildung 7 auf Seite 49 stellt diesen Use Case dar.



- Überwachung und Meldung von Störungen
- Bewertung Bedrohungszustand
- Identifizierung Schutzmechanismen
- Durchführung von Schutzmassnahmen

- Überwachung und Meldung von Störungen
- Bewertung Bedrohungszustand
- Identifizierung Schutzmechanismen
- Durchführung von Schutzmassnahmen

Abbildung 7: Use Case 6 – Schutzerhalt von Netzsystem und Daten

5.5.2. Rollen

Übertragungsnetzbetreiber und Verteilnetzbetreiber

Der Übertragungsnetzbetreiber und der Verteilnetzbetreiber überwachen die vorhandenen Daten und Informationen und schützen ihre Systeme und Umsysteme vor Angriffen.

5.5.3. Komponenten

Applikation Störungsmanagement / Risikoanalyse

Diese Applikation führt die Risikoanalyse durch und initiiert die geeigneten Massnahmen. Der aktuelle Sicherheitszustand wird analysiert, Störfälle erkannt, sowie Risikoanalysen durchgeführt. Die Applikation identifiziert auf diese Weise die Schwachstellen. Daraus werden Handlungsoptionen und mögliche Schutzmassnahmen hergeleitet und vorgeschlagen, welche für den Erhalt des Netzbetriebs und der Netzstabilität sowie für den Schutz vor Angriffen notwendig sind.

5.5.4. Datenobjekte

Fehlerinformationen, Bedrohungszustand, Netzkonfiguration – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Auf diesen Daten basieren die Analysen und Auswertungen, welche den Zustand des Gesamtsystems beschreiben. Aus den vorhandenen und ausgetauschten Informationen können grossflächige Störungen oder Feststellungen schnell eruiert und gezielter analysiert werden.

Schutzmassnahmen – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die Applikation Störungsmanagement / Risikoanalyse generiert Daten zu Schutzmassnahmen, welche die Fehler- oder Schwachstellen minimieren sollen. Diese Schutzmassnahmen werden zwischen dem Verteilnetzbetreiber und dem Übertragungsnetzbetreiber ausgetauscht, um gegenseitige Einflüsse sowie systematische Angriffe frühzeitig zu erkennen.

5.5.5. Kommunikation

Die Kommunikation zwischen Übertragungsnetzbetreiber und Verteilnetzbetreiber erfolgt primär über bestehende WAN-Technologien.

5.6. Use Case 7: Fehlererkennung und Netzrekonfiguration

5.6.1. Definition

Um im Netz Fehler und Ausfälle zu erkennen und darauf zu reagieren, können Fehler- und Schaltinformationen untereinander ausgetauscht werden. Der Übertragungsnetzbetreiber sowie der Verteilnetzbetreiber identifizieren ihre jeweiligen Netzfehler und führen in erster Linie Schalthandlungen in ihren Netzen aus. Diese Schaltinformationen können zwischen den Netzbetreibern ausgetauscht, sofern sie sich gegenseitig beeinflussen. Zusätzlich werden beim Prosumer oder Erzeuger auftretende Fehlerinformationen dort identifiziert und dem Verteilnetzbetreiber zur Verfügung gestellt. Dieser verwendet diese Informationen, beispielsweise bei einem Teilausfall für die Netzrekonfiguration und kann so schneller den Betrieb wieder aufnehmen.

Abbildung 8 auf Seite 52 stellt diesen Use Case dar.

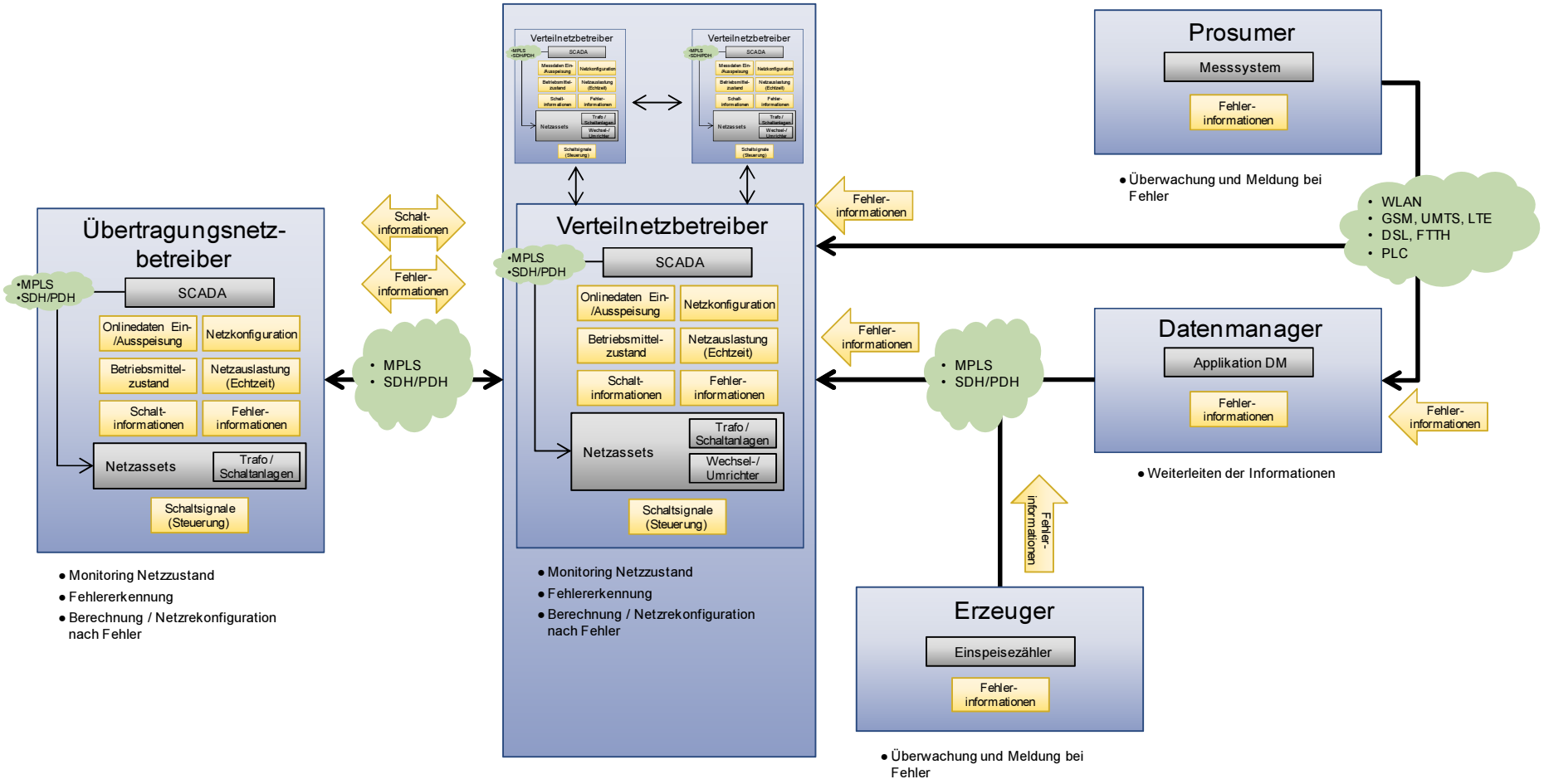


Abbildung 8: Use Case 7 – Fehlererkennung und Netzrekonfiguration

5.6.2. Rollen

Übertragungsnetzbetreiber

Der Übertragungsnetzbetreiber erkennt die Fehler in seinem Netz und stellt den Netzbetrieb bei einem Ausfall schnellstmöglich wieder her. Er tauscht die Schalt- und Fehlerinformation für die Netzrekonfiguration gegebenenfalls mit dem Verteilnetzbetreiber aus.

Verteilnetzbetreiber

Der Verteilnetzbetreiber erkennt, unter Einbezug der Fehlerinformationen von Erzeugern und Prosumern, aus den unteren Netzebenen die Fehler in seinem Netz und stellt den Netzbetrieb bei einem Ausfall schnellstmöglich wieder her. Er tauscht die Schalt- und Fehlerinformation für die Netzrekonfiguration gegebenenfalls mit dem Übertragungsnetzbetreiber aus.

Erzeuger / Prosumer

Die Erzeuger und Prosumer informieren den Verteilnetzbetreiber über Störungen im Netz am Hausanschluss / KW-Anschluss und unterstützen damit die schnelle Netzrekonfiguration zur Stabilisierung des Netzes.

Datenmanager

Der Datenmanager leitet die Fehlerinformationen vom Prosumer zum Verteilnetzbetreiber gegebenenfalls weiter, sofern keine Direktverbindung existiert.

5.6.3. Komponenten

SCADA[8] – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Im SCADA werden die internen Mess- und Zustandsdaten bezüglich Fehler und Ausfällen in einer ersten Instanz ausgewertet, so dass Alarme und technische Meldungen möglichst schnell erkannt werden. Zusätzlich werden die ausgetauschten Fehler- und Schaltinformationen bei der Analyse und Massnahmenbestimmung einbezogen.

Netzassets – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die Netzassets führen die beim Übertragungsnetzbetreiber (Trafo- und Schaltanlagen) und Verteilnetzbetreiber (Trafo-, Schaltanlagen, Wechsel-/Umrichter) notwendigen Schalthandlungen aus, welche für die Netzrekonfiguration notwendig sind.

Einspeisezähler/Messsytem – Erzeuger, Prosumer

Die Fehlerinformationen werden vom Einspeisezähler beim Erzeuger bzw. Messsystem beim Prosumer erkannt und an den Verteilnetzbetreiber weitergeleitet.

Applikation DM

Die Applikation DM erhält die Fehlerinformation vom Prosumer und leitet diese an den Verteilnetzbetreiber weiter.

Generell werden die Daten von und zum Prosumer durch den Datenmanager verwaltet, aufbereitet und gespeichert sowie den jeweiligen Empfängern weitergeleitet.

[8] Unter der Komponente SCADA werden alle SCADA Daten sowie die Dienste / Applikationen des Leitsystems verstanden.

5.6.4. Datenobjekte

Onlinedaten Ein-/Ausspeisung, Netzkonfiguration, Netzauslastung, Betriebsmittelzustand – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Diese Daten dienen dazu, im SCADA den Betriebszustand bezüglich eines Fehlers oder eines Ausfalls zu analysieren und Massnahmen zu definieren. Die Massnahmen werden als Schaltsignale an die internen Netzassets gesendet.

Schaltsignale – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die Schaltsignale werden vom SCADA zu den internen Netzassets gesendet. Damit werden die Schalthandlungen zur Netzstabilisierung oder Netzrekonfiguration ausgeführt.

Schaltinformationen – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die Schaltinformationen enthalten die Informationen zu den für eine allfällige Netzstabilisierung oder Netzrekonfiguration vorgenommenen Schalthandlungen. Diese Schaltinformationen können unter den Netzbetreibern ausgetauscht werden, falls die Informationen gegenseitig relevant sind.

Fehlerinformationen – alle Rollen

Fehlerinformationen werden jeweils vor Ort erfasst. Die Fehlerinformationen des Erzeugers oder des Prosumers werden an den Verteilnetzbetreiber weitergeleitet. Die Fehlerinformationen des Verteilnetzbetreibers oder des Übertragungsnetzbetreibers können untereinander ausgetauscht werden, falls die Informationen gegenseitig relevant sind.

5.6.5. Kommunikation

Die Kommunikation zwischen Prosumer und Verteilnetzbetreiber sowie gegebenenfalls dem Datenmanager, erfolgt über bestehende Kommunikationstechnologien im Access-Bereich. Die Kommunikation zwischen den restlichen Rollen erfolgt primär über bestehende WAN-Technologien.

5.7. Use Case 8: Steuerung Wirk- und Blindleistung

5.7.1. Definition

Dieser Use Case hat die aktive Steuerung der Wirk- und Blindleistung im Übertragungs- und Verteilnetz zum Inhalt. Die Verteilnetzbetreiber können den Prosumer und den Erzeuger diesbezüglich einbinden und gezielt ansteuern, so dass deren Ein- / Ausspeisung die Spannungsqualität im Netz verbessert, z.B. mittels bedarfsgerechter Blindleistungsbereitstellung. Dazu werden die Ein- und Ausspeisungen beim Erzeuger und Prosumer gemessen. Der Verteilnetzbetreiber analysiert und überprüft den Netzzustand, steuert und regelt diesen nach Möglichkeit mit seinen eigenen Netzassets und zieht für punktuelle Korrekturen die Erzeuger oder die Prosumer mit ein.

Abbildung 9 auf Seite 55 stellt diesen Use Case dar.

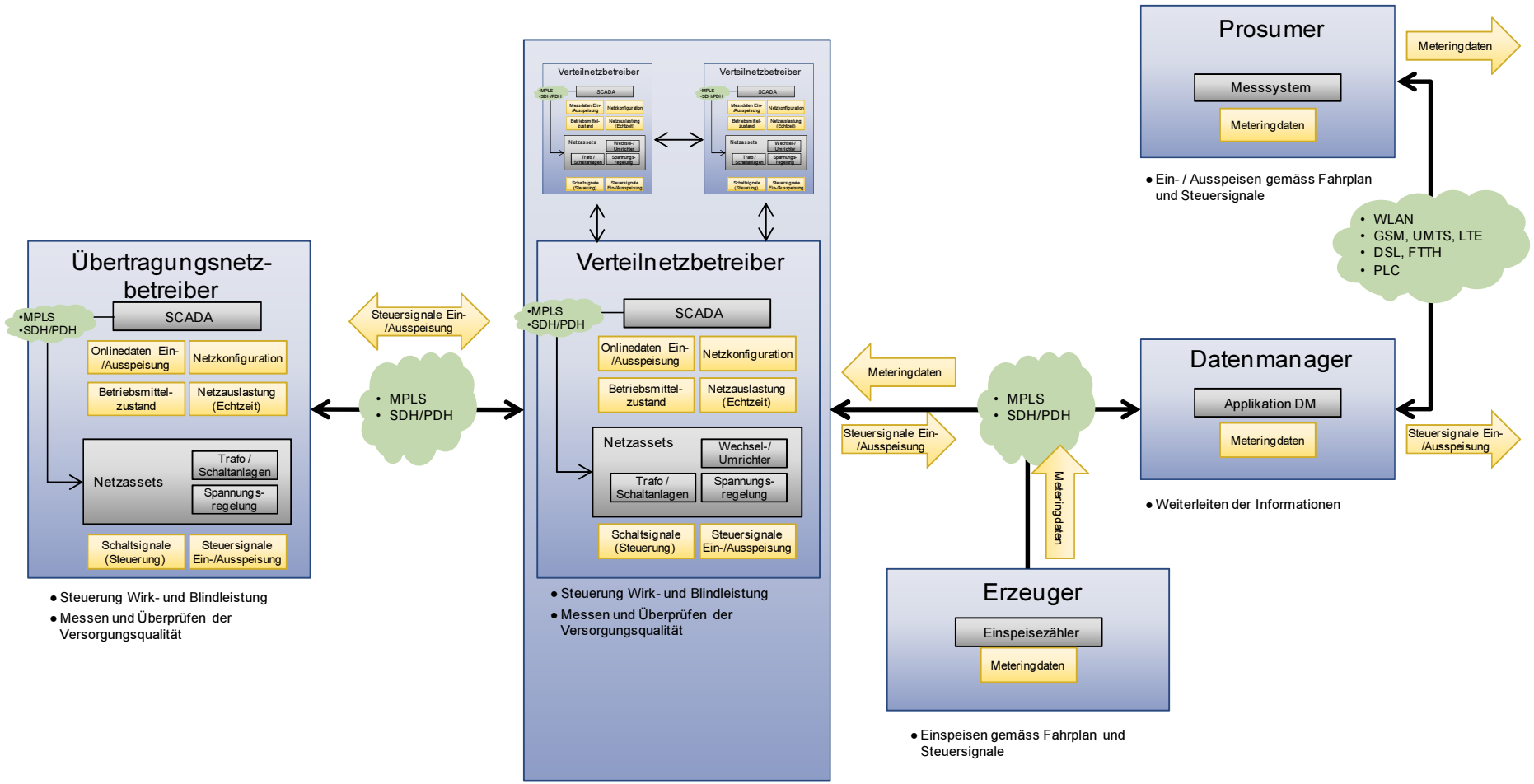


Abbildung 9: Use Case 8 – Steuerung Wirk- und Blindleistung

5.7.2. Rollen

Übertragungsnetzbetreiber, Verteilnetzbetreiber

Beim Übertragungsnetzbetreiber und beim Verteilnetzbetreiber wird die Spannungsqualität überwacht und gesteuert. Dazu dienen einerseits die internen SCADA Daten und andererseits die überwachten Daten der Erzeuger und Prosumer.

Erzeuger, Prosumer

Die Erzeuger und Prosumer stellen die gemessenen Daten zur Ein-/Ausspeisung dem Verteilnetzbetreiber zur Verfügung und werden von diesem entsprechend den berechneten Steuersignalen zu Wirk- und Blindleistung angesteuert.

Datenmanager

Der Datenmanager leitet die Meteringdaten des Prosumer an den Verteilnetzbetreiber weiter.

5.7.3. Komponenten

SCADA[9] – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Im SCADA werden die vorhandenen Daten zusammengetragen und analysiert. Ergibt sich ein Handlungsbedarf z.B. bezüglich Spannungsqualität, Überlastung o.ä, können die Netzassets angesteuert werden. Der Verteilnetzbetreiber kann ausserdem Steuersignale an die Erzeuger oder Prosumer senden, um diese bei lokalen Schwankungen gezielt einzusetzen.

Netzassets – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die Netzassets können zur Unterstützung des stabilen Netzbetriebs bezüglich Wirk- und Blindleistung angesteuert werden.

Einspeisezähler, Messsystem – Erzeuger, Prosumer

Beim Erzeuger bzw. Prosumer werden die Meteringdaten erfasst und dem Verteilnetzbetreiber zur Verfügung gestellt.

Applikation DM – Datenmanager

Die Applikation DM leitet die Messdaten vom Prosumer an den Verteilnetzbetreiber weiter. Generell werden die Daten von und zum Prosumer durch den Datenmanager verwaltet, aufbereitet und gespeichert sowie den jeweiligen Empfängern weitergeleitet.

5.7.4. Datenobjekte

Onlinedaten Ein-/Ausspeisung, Netzkonfiguration, Betriebsmittelzustand, Netzauslastung – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Diese meist im SCADA Umfeld vorhandenen Datenobjekte (teilweise aus dem GIS-Umfeld) werden dazu verwendet, den aktuellen Systemzustand zu analysieren und die Optimierungsmöglichkeiten bezüglich Wirk- und Blindleistung zu eruieren. Diese Daten werden durch die gemessenen Ein-/Ausspeisedaten der Erzeuger und Prosumer ergänzt.

[9] Unter der Komponente SCADA werden alle SCADA Daten sowie die Dienste / Applikationen des Leitsystems verstanden.

Schaltsignale, Steuersignale – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Für die Steuerung der Wirk- und Blindleistung werden die eigenen Netzassets angesteuert. Dabei werden je nach Asset direkte Schaltsignale, beispielsweise an die Transformatoren, gesendet. Oder es werden Einflussparameter übermittelt, beispielsweise mit Steuersignalen an die Wechselrichter, mit denen bei der Steuerung des Wechselrichters die notwendigen Regelungsparameter ermittelt werden.

Meteringdaten – Erzeuger, Prosumer

Die Meteringdaten zur Ein-/Ausspeisung werden beim Erzeuger bzw. Prosumer erfasst und dem Verteilnetzbetreiber zur Verfügung gestellt.

5.7.5. Kommunikation

Die Kommunikation zwischen Prosumer und Verteilnetzbetreiber sowie gegebenenfalls dem Datenmanager, erfolgt über bestehende Kommunikationstechnologien im Access-Bereich. Die Kommunikation zwischen den restlichen Rollen erfolgt primär über bestehende WAN-Technologien.

5.8. Use Case 9: Instandhaltung

5.8.1. Definition

Die Instandhaltung für die kurz- und mittelfristige Erhaltung des Betriebs und der Betriebsmittel soll im Smart Grid optimiert und effizienter geplant werden können. Bei der Planung von Instandhaltungs-Massnahmen werden Netzauslastung und Betriebsmittelzustände antizipiert und berechnet. Zusätzlich lassen sich Prosumer- und Erzeuger-Informationen in die Instandhaltungs-Planung einbeziehen, indem dort identifizierte Betriebszustände zur Erkennung von zukünftigen Schwachstellen oder Betriebsmängel dem Verteilnetzbetreiber kommuniziert und von diesem in den Berechnungen berücksichtigt werden Die Informationen zu den Instandhaltungs-Massnahmen werden je nach Auswirkung zwischen dem Verteilnetzbetreiber und dem Übertragungsnetzbetreiber ausgetauscht.

Abbildung 10 auf Seite 58 stellt diesen Use Case dar.

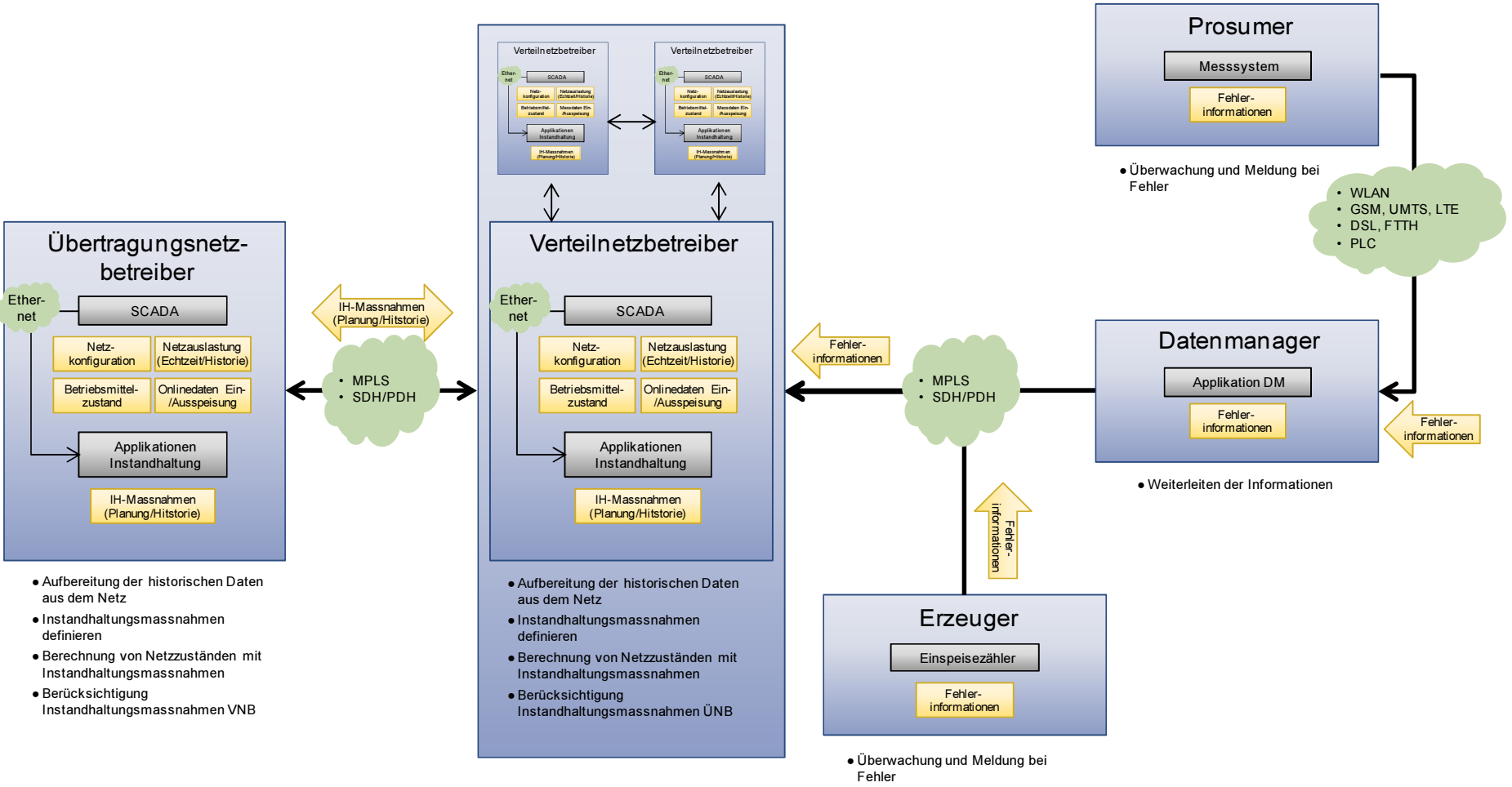


Abbildung 10: Use Case 9 – Instandhaltung (IH)

5.8.2. Rollen

Übertragungsnetzbetreiber, Verteilnetzbetreiber

Der Übertragungsnetzbetreiber und der Verteilnetzbetreiber berechnen die zukünftigen Betriebsmittel- und Netzzustandsprognosen und leiten die Planung von Instandhaltungs-Massnahmen daraus ab.

Erzeuger, Prosumer

Der Erzeuger und der Prosumer informieren den Verteilnetzbetreiber über Fehler am Anschlussknoten, da diese Fehler auf defekte Betriebsmittel hinweisen können. Diese Informationen werden vom Verteilnetzbetreiber in der Instandhaltungs-Planung berücksichtigt. Dies kann auch automatisiert erfolgen.

Datenmanager

Der Datenmanager leitet die Fehlerinformationen des Prosumer an den Verteilnetzbetreiber weiter, sofern keine direkte Anbindung besteht und die Informationen automatisiert erzeugt und übermittelt werden.

5.8.3. Komponenten

SCADA[10] – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die SCADA Systeme tragen die vorhandenen Informationen aus der Netzüberwachung zusammen. Diese Daten werden der Instandhaltungsapplikation zu Berechnungszwecken zur Verfügung gestellt.

Applikationen Instandhaltung – Übertragungsnetzbetreiber, Verteilnetzbetreiber

In der Applikation Instandhaltung werden alle vorhanden Daten zusammen getragen, die Instandhaltungs-Berechnungen und –Simulationen durchgeführt und Instandhaltungs-Massnahmen definiert. Die Datenbasis der Betriebsmittel wird ggf. angepasst, sodass z.B. eine Lernkurve entsteht oder weitere Analysen durchgeführt werden können.

Einspeisezähler, Messsystem – Erzeuger, Prosumer

Im Einspeisezähler und dem Messsystem des Erzeugers bzw. Prosumers werden Fehler überwacht und Fehlerinformationen für den Verteilnetzbetreiber erzeugt sowie übermittelt.

Applikation DM – Datenmanager

Die Applikation DM leitet die Fehlerinformationen vom Prosumer zum Verteilnetzbetreiber. Generell werden die Daten von und zum Prosumer durch den Datenmanager verwaltet, aufbereitet und gespeichert sowie den jeweiligen Empfängern weitergeleitet.

5.8.4. Datenobjekte

Netzkonfiguration, Netzauslastung (aktuell und historisch), Betriebsmittelzustand, Onlinedaten Ein-/Ausspeisung– Übertragungsnetzbetreiber, Verteilnetzbetreiber

[10] Unter der Komponente SCADA werden alle SCADA Daten sowie die Dienste / Applikationen des Leitsystems verstanden.

Diese meist im SCADA Umfeld vorhandenen Datenobjekte (teilweise aus dem GIS-Umfeld) werden für die Berechnungen und Simulationen der Instandhaltungs-Massnahmen in der Applikation Instandhaltung einbezogen.

Instandhaltungs-Massnahmen – Übertragungsnetzbetreiber, Verteilnetzbetreiber

In den Instandhaltungs-Massnahmen werden die geplanten Massnahmen mit all ihren Details (Aktivität, Termine, Betriebsmittel etc.) festgehalten, unter Berücksichtigung deren Einfluss auf das Netz. Je nach Instandhaltungs-Massnahme mit gegenseitigen Abhängigkeiten werden die Informationen an den Übertragungsnetzbetreiber bzw. Verteilnetzbetreiber weitergeleitet.

Fehlerinformationen – Erzeuger, Prosumer

Die Fehlerinformationen des Erzeugers und des Prosumers geben einen Hinweis auf Fehler am Anschlusspunkt. Diese können auf defekte Betriebsmittel zurückzuführen sein, was den Verteilnetzbetreiber bei der schnellen Fehlerbehebung unterstützt.

5.8.5. Kommunikation

Die Kommunikation zwischen Prosumer und Verteilnetzbetreiber sowie gegebenenfalls dem Datenmanager, erfolgt über bestehende Kommunikationstechnologien im Access-Bereich. Die Kommunikation zwischen den restlichen Rollen erfolgt primär über bestehende WAN-Technologien.

5.9. Use Case 10: Reduktion Netzverluste

5.9.1. Definition

Im Smart Grid wird die Identifizierung der zeitlichen und örtlichen Verteilung der Netzverluste und derart eine Optimierung der Netzverlustreduktion ermöglicht. Mit den gemessenen Daten können der Übertragungsnetzbetreiber und der Verteilnetzbetreiber Optimierungsmöglichkeiten im Netzbetrieb ermitteln und entsprechende Handlungsoptionen für die Minimierung der Netzverluste durch eine geeignete Verteilung der Lastflüsse berechnen. Die netzeigenen Betriebsmittel werden entsprechend angesteuert. Je nach Einflussgebiet werden die Informationen zwischen dem Verteilnetzbetreiber und dem Übertragungsnetzbetreiber ausgetauscht.

Abbildung 11 auf Seite 61 stellt diesen Use Case dar.

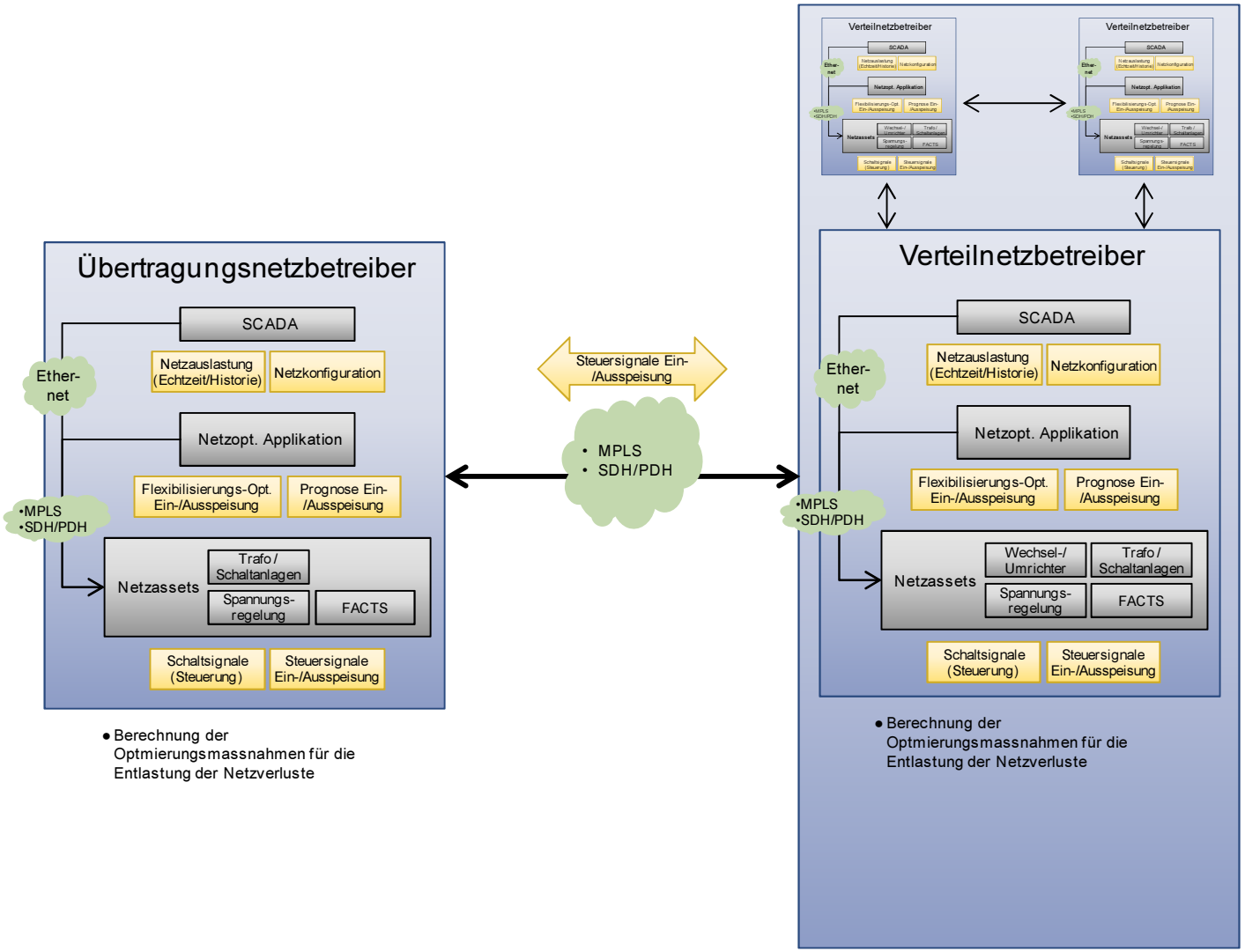


Abbildung 11: Use Case 10 – Reduktion Netzverluste

5.9.2. Rollen

Übertragungsnetzbetreiber, Verteilnetzbetreiber

Der Übertragungsnetzbetreiber und die Verteilnetzbetreiber berechnen die Optimierungsmassnahmen für die Reduzierung der Netzverluste und steuern ihre Netzassets mit den entsprechenden Steuersignalen an.

5.9.3. Komponenten

SCADA[11] – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Das SCADA liefert die Grundlagendaten für die Berechnung und Analyse der aktuellen und prognostizierten Lastflüsse und Netzverluste.

Netzoptimierungs-Applikation – Übertragungsnetzbetreiber, Verteilnetzbetreiber

In der Netzoptimierungs-Applikation werden die Prognosen und Flexibilisierungsoptionen der Ein- und Ausspeisungen simuliert und entsprechende Handlungsoptionen zur Reduzierung der Netzverluste berechnet.

Netzassets – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die Netzassets werden zur Umsetzung der in der Netzoptimierungs-Applikation berechneten Flexibilisierungsoption mittels Schaltungen angesteuert.

5.9.4. Datenobjekte

Netzkonfiguration, Netzauslastung – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die aktuellen und historischen Datenobjekte der Netzkonfiguration und –auslastung werden im SCADA erfasst und liefern die Grundlagen für die Simulationen in der Netzoptimierungs-Applikation.

Flexibilisierungs-Option Ein- / Ausspeisung – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die Flexibilisierung-Optionen sind das Resultat der in der Netzoptimierungs-Applikation berechneten Handlungsoptionen zur Steuerung der zukünftigen Lastfüsse.

Prognose Ein-/Ausspeisung – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die Prognosen der Ein- und Ausspeisungen weisen auf zukünftige Netzauslastungen hin und dienen als Input zur Berechnung der zukünftigen Lastflüsse.

Schaltsignale, Steuersignale Ein-/Ausspeisung – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die Schalt- und Steuersignale dienen dazu, die Optimierungsmöglichkeiten umzusetzen. Die Signale werden von der Netzoptimierungs-Applikation erstellt und an die Netzassets gesendet. Zusätzlich werden die Information zu den Steuersignalen bei gegenseitigen Abhängigkeiten zwischen dem Übertragungsnetzbetreiber und dem Verteilnetzbetreiber ausgetauscht.

[11] Unter der Komponente SCADA werden alle SCADA Daten sowie die Dienste / Applikationen des Leitsystems verstanden.

5.9.5. Kommunikation

Die Kommunikation zwischen Übertragungsnetzbetreiber und Verteilnetzbetreiber erfolgt primär über bestehende WAN-Technologien.

5.10. Use Case 11: Betriebsmitteleinsatzplanung

5.10.1. Definition

Im Use Case Betriebsmitteleinsatzplanung werden die Betriebsmittel langfristig schonend eingesetzt, um eine möglichst lange Lebensdauer zu gewährleisten. Das Smart Grid unterstützt diese Optimierung, indem auf Grund der Verfügbarkeit einer umfassenden Datenbasis detaillierte Berechnungen und Simulationen für den Einsatz und die Planung der Betriebsmittel durchgeführt werden können. Die Use Cases Instandhaltung (9) und Betriebsmitteleinsatzplanung (11) haben das gemeinsame Ziel die Betriebsmittel zu erhalten. Deswegen können diese Use Cases auch zusammen betrachtet werden.

Abbildung 12 auf Seite 64 stellt diesen Use Case dar.

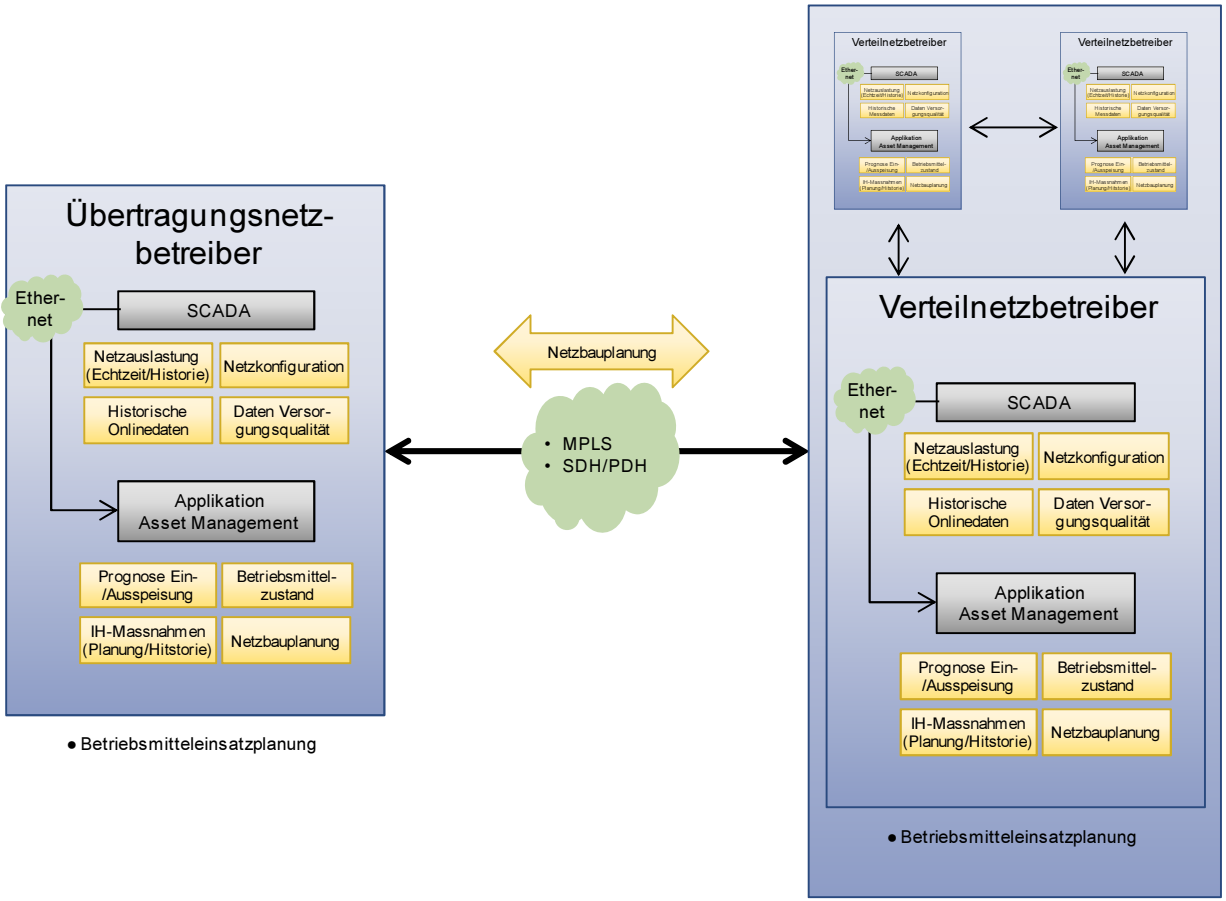


Abbildung 12: Use Case 11 – Betriebsmitteleinsatzplanung

5.10.2. Rollen

Übertragungsnetzbetreiber, Verteilnetzbetreiber

Der Übertragungsnetzbetreiber und die Verteilnetzbetreiber eruieren auf Grund der aktuellen Zustandsdaten und umfassender Kenntnis über das Gesamtsystem den optimierten Einsatz der Betriebsmittel. Informationen zu langfristigen Netzbauplanungen werden zwischen den Verteilnetzbetreibern und dem Übertragungsnetzbetreiber bei gegenseitigen Abhängigkeiten ausgetauscht.

5.10.3. Komponenten

SCADA[12] – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Im SCADA werden die aktuellen und historischen Netzzustandsdaten gemessen und gespeichert (unter teilweise Einbezug von GIS-Datenobjekten). Diese Datenobjekte werden der Applikation Asset Management zur Berechnung des optimalen Einsatzes der Betriebsmittel zur Verfügung gestellt.

Applikation Asset Management – Übertragungsnetzbetreiber, Verteilnetzbetreiber

In der Applikation Asset Management wird unter Berücksichtigung der Instandhaltungs-Massnahmen und der bisherigen Netzbauplanung sowie den mittel- bis langfristigen Prognosewerten der Betriebsmitteleinsatz geplant.

5.10.4. Datenobjekte

Netzauslastung, Netzkonfiguration, Historische Onlinedaten, Daten Versorgungsqualität – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die SCADA Datenobjekte zu den aktuellen und historischen Auslastungen, Ein- und Ausspeisungen sowie Kennzahlen zur Versorgungsqualität (Störungen) werden gemessen und gespeichert und als Grundlagen der Applikation Asset Management zur Verfügung gestellt.

Prognose Ein-/Ausspeisung – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die mittel- bis langfristigen Ein- und Ausspeisungen werden prognostiziert und für die Berechnung der Belastungen und Kapazitätsengpässen berücksichtigt. Dies dient als Input für die Berechnung des optimalen und effizienten Betriebsmitteleinsatzes.

Betriebsmittelzustand – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Der Betriebsmittelzustand liefert Informationen zur Lebensdauer und Belastungen, als Input zur zuverlässigkeitsbasierten Ermittlung des zukünftigen Einsatzes.

Instandhaltungs-Massnahmen, Netzbauplanung – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die historischen oder bereits geplanten Instandhaltungs-Massnahmen (kurzfristige Aktivitäten) sowie die Netzbauplanung (langfristige Aktivitäten) müssen bei der Betriebsmitteleinsatzplanung berücksichtigt werden. Die ermittelte Netzbauplanung wird bei gegenseitigen Abhängigkeiten zwischen den Übertragungsnetzbetreiber und dem Verteilnetzbetreiber ausgetauscht.

[12] Unter der Komponente SCADA werden alle SCADA Daten sowie die Dienste / Applikationen des Leitsystems verstanden.

5.10.5. Kommunikation

Die Kommunikation zwischen Übertragungsnetzbetreiber und Verteilnetzbetreiber erfolgt primär über bestehende WAN-Technologien.

5.11. Use Case 12: Zeitliche Flexibilisierung Ein-/Ausspeisung

5.11.1. Definition

Unter der zeitlich flexiblen Ein- und Ausspeisung werden der Einsatz von beispielsweise Kühlräumen, Boiler, Batterien und BHKW verstanden, welche kurzfristig zu- oder weggeschalten werden können, ohne erkennbare Komforteinbussen beim Konsumenten. Bei der zeitlichen Flexibilisierung der Ein- und Ausspeisung kommunizieren die Netzteilnehmer ihre flexible Last/Erzeugung an die Verteilnetzbetreiber. Diese können je nach Netzbelastung die flexiblen Ein- und Ausspeisungen ansteuern, um einen kurzfristig optimierten Betrieb bei Kapazitätsengpässen zu erhalten. Durch diese Flexibilität können Erneuerungen hinausgezögert oder sogar verhindern werden. Dadurch werden Überkapazitäten minimiert und somit der Einsatz der Betriebsmittel schonend und deshalb langfristig optimiert.

Abbildung 13 auf Seite 67 stellt diesen Use Case dar.

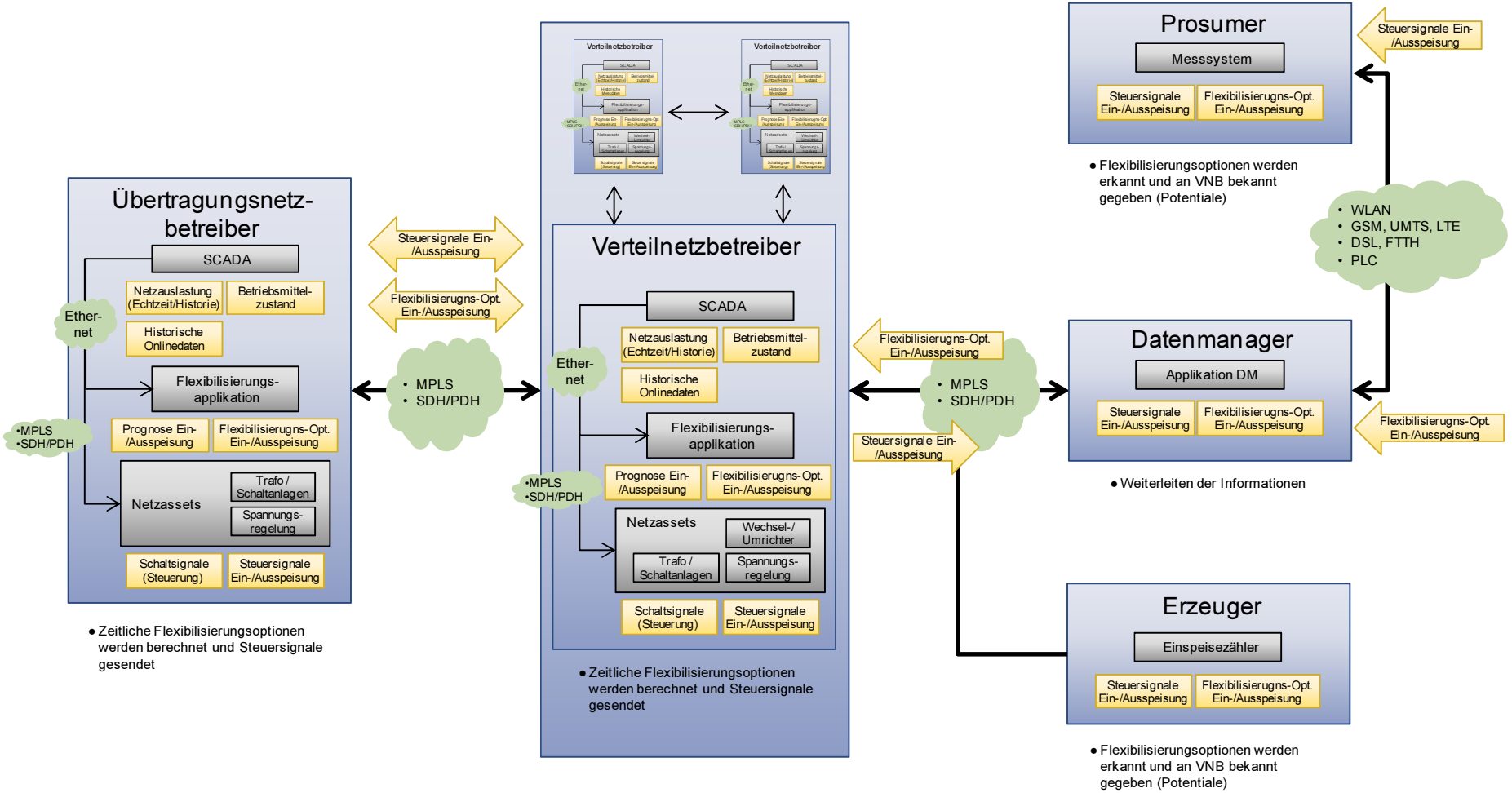


Abbildung 13: Use Case 12 – Zeitliche Flexibilisierung Ein- / Ausspeisung

5.11.2. Rollen

Übertragungsnetzbetreiber, Verteilnetzbetreiber

Der Übertragungsnetzbetreiber und die Verteilnetzbetreiber empfangen die Flexibilisierungsoptionen der Netzteilnehmer und können bei Bedarf diese Flexibilisierung zur Steuerung und Optimierung des Betriebs sowie des Betriebsmitteleinsatzes nutzen. Dies könnte auch auf Basis eines marktbasierten Verfahrens geschehen.

Prosumer, Erzeuger

Prosumer und Erzeuger eruieren ihre zeitlich flexiblen Ein – und Ausspeisungen oder liefern relevanten Daten für Dritte, die dies übernehmen. Die Informationen zur Flexibilisierung werden dem Verteilnetzbetreiber zur Verfügung gestellt.

Datenmanager

Der Datenmanager leitet die Flexibilisierungs-Optionen des Prosumers an den Verteilnetzbetreiber weiter. Eine weitere Funktion des Datenmanager (z.B. Anonymisierung) ist für diese Daten nicht vorgesehen.

5.11.3. Komponenten

SCADA[13] – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Im SCADA stehen die Grundlagendaten zur Berechnung des Netzzustands zur Verfügung. Diese werden in der Flexibilisierungsapplikation benötigt.

Flexibilisierungsapplikation – Übertragungsnetzbetreiber, Verteilnetzbetreiber

In der Flexibilisierungsapplikation werden aus den Grundlagendaten des Netzzustandes und den Informationen zu den Flexibilitäten der Netzteilnehmer mögliche Optimierungen berechnet und die entsprechenden Schalt- und Steuersignale erstellt.

Zusätzlich werden die Steuersignale und Flexibilisierungsoptionen zwischen den Verteilnetzbetreibern und dem Übertragungsnetzbetreiber ausgetauscht, zwecks Abstimmung der gegenseitigen Auswirkungen.

Netzassets – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die Netzassets erhalten die Schalt- und Steuersignale von der Flexibilisierungsapplikation und führen diese aus.

Messsystem, Einspeisezähler – Prosumer, Erzeuger

Die Flexibilisierungsoptionen der Ein- und Ausspeisung am Anschlusspunkt der Prosumer bzw. Erzeuger werden berechnet und dem Verteilnetzbetreiber übermittelt.

5.11.4. Datenobjekte

Netzauslastung, Betriebsmittelzustand, Historische Onlinedaten – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Diese SCADA Daten sind die Grundlage zur Berechnung des Optimierungsbedarfs. Diese werden der Flexibilisierungsapplikation zur Verfügung gestellt.

[13] Unter der Komponente SCADA werden alle SCADA Daten sowie die Dienste / Applikationen des Leitsystems verstanden.

Prognose und Flexibilisierungsoptionen Ein-/Ausspeisung – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Mit den Prognosewerten und den Flexibilisierungsoptionen zu den Ein- und Ausspeisungen in ihrem Netzgebiet können die Verteilnetzbetreiber und Übertragungsnetzbetreiber die kurzfristige Netzbelastung abschätzen und bei Bedarf die Flexibilisierungsoptionen nutzen.

Schaltsignale, Steuersignale Ein- und Ausspeisung – Übertragungsnetzbetreiber, Verteilnetzbetreiber

Die Schalt- und Steuersignale werden von der Flexibilisierungsapplikation erzeugt und den Netzassets sowie den Prosumern und Erzeugern zur Ausführung übermittelt. Die Steuersignale werden je nach gegenseitiger Abhängigkeit zwischen den Verteilnetzbetreiber und dem Übertragungsnetzbetreiber kommuniziert, damit diese wiederum in die Berechnungen der Netzzustände einbezogen werden können.

Steuersignale Ein- und Ausspeisung – Prosumer, Erzeuger

Die Steuersignale, welche vom Verteilnetzbetreiber an die Prosumer und Erzeuger versendet werden, werden am Anschlusspunkt empfangen und führen die gemäss Flexibilisierungsoption möglichen Steuerungen durch.

Flexibilisierungsoptionen – Prosumer, Erzeuger

Die Flexibilisierungsoptionen können beim Prosumer und beim Erzeuger festgelegt und kontrolliert und dem Verteilnetzbetreiber angeboten werden. Diese Optionen bieten möglichst viel Flexibilität zur Steuerung der Ein- und Ausspeisungen, mit möglichst geringen Komforteinbussen bei den Anbietern. Beispielsweise können dabei Tageszeiten, Abwesenheiten sowie spontane manuelle Zu- und Wegschaltung berücksichtigt werden.

5.11.5. Kommunikation

Die Kommunikation zwischen Prosumer und Verteilnetzbetreiber sowie gegebenenfalls dem Datenmanager, erfolgt über bestehende Kommunikationstechnologien im Access-Bereich. Die Kommunikation zwischen den restlichen Rollen erfolgt primär über bestehende WAN-Technologien.

6. Datenschutz für Smart Metering und Smart Grids

6.1. Einleitung

Dieser Abschnitt des Berichts beschäftigt sich mit Datenschutzaspekten des Smart Grid.

Smart Meters generieren Verbrauchsdaten von Haushalten und Unternehmen. Im Rahmen eines Smart Grid-Systems können diese Messdaten in verschiedenen Formen und von verschiedenen Marktteilnehmern genutzt werden. Als Erstes wird deshalb die Frage der Anwendbarkeit der bestehenden Schweizer Datenschutzgesetzgebung aufgeworfen. Es werden die Voraussetzungen für die Anwendbarkeit analysiert und dargelegt, inwiefern beim Aufbau eines Smart Grids mit Smart Meters sowie bei den aus heutiger Sicht möglichen Businessmodellen (12 Use Cases) die Datenschutzgesetzgebung beachtet werden muss (Kapital 6.2).

Da in der Schweiz je nach Anwendungsfall auch kantonale Datenschutzgesetze zu beachten sind, werden Lösungsansätze für eine einheitliche Regelung für Smart Grids dargelegt, und es wird für eine bundesrechtlich einheitliche Regelung des Datenschutzes im Bereich Smart Grid plädiert (Kapitel 6.3).

Als nächstes werden Implikationen der Anwendbarkeit der (bundesrechtlichen) Datenschutzgesetzgebung aufgezeigt. Dabei wird auf die Rolle und die Pflichten des Dateninhabers eingegangen sowie auf die Rechte der betroffenen Privatpersonen und Unternehmen. Weiter wird auf die sich aus der Datenschutzgesetzgebung ergebenden Lösungsansätze hingewiesen (Kapitel 6.4).

In einem weiteren Kapitel (Kapitel 6.5) werden Lösungsansätze für den Datenschutz im Zusammenhang mit Smart Metering in Österreich, England und Deutschland dargestellt. Da in den Niederlanden der flächendeckende Rollout aufgrund von Konflikten mit dem Datenschutz gescheitert ist, wird auch dieses Land in den Länderbericht aufgenommen. Die Länderberichte enthalten auch die von diesen Staaten festgelegten Regeln zur Datenschutzsicherheit.

Zum Schluss werden im Sinne eines Management Summary unter Berücksichtigung der Erfahrungen und Lösungsmodelle aus dem Ausland sowie der Rechtslage in der Schweiz die Lösungsoptionen für den Schweizer Gesetzgeber aufgezeigt (Kapitel 6.7).

6.2. Anwendbarkeit des Bundesgesetzes über den Datenschutz (DSG)

Das schweizerische Datenschutzgesetz (DSG)[14] schützt gemäss seinem Zweckartikel die Privatsphäre, die Persönlichkeit und die Grundrechte im Zusammenhang mit der Bearbeitung von Daten. Im Rahmen der zugehörigen Botschaft erklärte der Bundesrat die Zielsetzung wie folgt: "*Jedermann soll, soweit die Rechtsordnung nichts anderes vorsieht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen und frei über die Aufnahme und Gestaltung seiner Informations- und Kommunikationsbeziehungen entscheiden können.*"[15] Die seit dem Erlass getätigten Revisionen tragen dieser grundsätzlichen Stossrichtung ebenfalls Rechnung und stärken die Stellung der betroffenen Personen, indem mehr Transparenz bei der Bearbeitung von Personen-

[14] Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1.; zum Verhältnis zu kantonalen Datenschutzgesetzen vgl. Kapital 6.3.

[15] *Bundesrat*, Botschaft vom 23. März 1988 zum Bundesgesetz über den Datenschutz (DSG), BBl 1988 II 413, S. 418.

daten geschaffen und die grenzüberschreitende Datenbekanntgabe neu geregelt wurde.[16]

In den Geltungsbereich des Gesetzes fallen gemäss Art. 2 Abs. 1 DSG das *Bearbeiten* von *Daten natürlicher und juristischer Personen* sowohl durch *private Personen* als auch durch *Bundesorgane*.[17] Für die Beantwortung der Frage, ob Smart Metering- bzw. Smart Grid-Daten dem Anwendungsbereich des DSG unterstehen, müssen insbesondere die in Art. 2 Abs. 1 DSG genannten Begriffe ausgelegt werden.

6.2.1. Bearbeiten

Nach Art. 3 lit. e DSG wird unter Bearbeiten "*jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten*" verstanden. Der Begriff des Bearbeitens wird demnach sehr umfassend verstanden, bei der Aufzählung der Tätigkeiten (Beschaffen, Aufbewahren…) handelt es sich lediglich um eine nicht abschliessende Liste.[18] So stellt bspw. auch das Anonymisieren von Personendaten ein Bearbeiten im Sinne der vorliegenden Bestimmung dar.[19] Wie bereits aus der Legaldefinition hervorgeht, sind die für das Bearbeiten angewandten Mittel und Verfahren irrelevant. Keine Rolle spielt somit, ob die Daten manuell oder automatisiert bearbeitet werden oder welche technischen Verfahren eingesetzt werden.[20]

In den 12 Use Cases werden Daten auf verschiedenen Stufen von verschiedenen Marktteilnehmern bearbeitet im Sinne von Art. 3 lit. e DSG. Indem bspw. im Rahmen des Energiedatenmanagements Meter-Daten und historische Meter-Daten vom Smart Meter-Gerät aufgezeichnet, gespeichert, anonymisiert und an einen Datenmanager oder ein Verteilnetzbetreiber weitergeleitet werden, liegt eine Bearbeitung von Daten nach Art. 2 Abs. 1 i.V.m. Art. 3 lit. e DSG vor (Use Case 1). Dieses allgemein formulierte Beispiel verdeutlicht, dass beinahe sämtliche Datenbearbeitungsvorgänge in den 12 Use Cases eine Bearbeitung im Sinne von Art. 3 lit. e DSG darstellen. Keine Bearbeitung liegt lediglich dann vor, wenn keine Personendaten vorliegen. Erstellt also bspw. ein Lieferant mithilfe von in anonymisierter Form erhaltener Daten Prognosen für die Energiebeschaffung und Preisberechnung, liegt keine Bearbeitung i.S.d. DSG vor. Bearbeiter sind dagegen diejenigen Akteure, welche diese Daten zuvor gesammelt, anonymisiert und an den Lieferanten gesendet haben.[21]

6.2.2. Daten/Personendaten

6.2.2.1. Gesetzliche Begriffsbestimmung der Personendaten

Gemäss der Legaldefinition in Art. 3 lit. a DSG sind Personendaten "*alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen*". Der Begriff der Personendaten ist dabei von zentraler Bedeutung, da die Anwendung des DSG ausnahmslos davon abhängt, ob Personendaten bearbeitet werden oder nicht.[22] Gemäss Literatur und Rechtsprechung ist der Begriff der Personendaten weit zu verstehen.[23] Der Begriff der

---

16 Vgl. *Bundesrat*, Botschaft vom 19. Februar 2003 zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung, BBl 2003 2101, S. 2102.

17 Zu den vorliegend nicht relevanten Ausnahmen des Anwendungsbereichs siehe Art. 2 Abs. 2 DSG.

18 *Jöhri/Rosenthal,* Handkommentar zum Datenschutzgesetz, 2008, Art. 3 N. 63; *Belser*, in: Maurer-Lambrou/Vogt, Basler Kommentar zum Datenschutzgesetz, 2006, Art. 3 N. 26.

19 *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 63.

20 *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 66.

21 Vgl. *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 68.

22 *Belser* (Anm. 18), Art. 3 N. 3.

23 Vgl. etwa *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 72, BVGer A-7040/2009 vom 30. März 2011, E. 7.2.

Person bezieht sich dabei nicht nur auf natürliche Personen, für Personendaten kommen sämtliche natürlichen und juristischen Personen infrage.[24] Vom DSG erfasst sind insbesondere auch die Personendaten privatrechtlicher Körperschaften des kantonalen Rechts und öffentlich-rechtlicher Anstalten und Körperschaften der Kantone und des Bundes.[25]

Unter den Begriff Personendaten fallen sämtliche Angaben, die sich auf eine Person beziehen, welche bestimmt oder bestimmbar ist.[26] Bei den Angaben kann es sich sowohl um Tatsachenfeststellungen als auch um Werturteile handeln. Unerheblich ist, in welcher Form die Informationen auftreten (etwa als Zeichen, Wort, Bild, Ton oder eine Kombination davon) und wie der Datenträger beschaffen ist. Entscheidend ist, dass sich die Angaben einer oder mehreren Personen zuordnen lassen.[27] Gemäss Rechtsprechung des Bundesgerichts ist eine Person dann bestimmt, "*wenn sich aus der Information selbst ergibt, dass es sich genau um diese Person handelt (Beispiel: Personalausweis).*"[28] Bestimmbar ist laut Bundesgericht eine Person, "*wenn sie zwar allein durch die Daten nicht eindeutig identifiziert wird, aus den Umständen, das heisst, aus dem Kontext einer Information oder aufgrund zusätzlicher Informationen auf sie geschlossen werden kann (z. B. wenn aus Angaben über Liegenschaften der Eigentümer ausfindig gemacht werden kann).*"[29] Damit eine Person bestimmbar ist, genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Bestimmbarkeit liegt dann nicht vor, wenn der Aufwand zur Identifizierung derart gross ist, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird. Dies ist jeweils im konkreten Fall zu beurteilen, wobei insbesondere auch die Möglichkeiten der Technik mitzuberücksichtigen sind, so bspw. die im Internet verfügbaren Suchwerkzeuge. Dabei ist nicht nur von Bedeutung, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuordnen zu können. Wichtig ist ebenfalls, welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat.[30] Ob Angaben einen Bezug zu einer mindestens bestimmbaren Person aufweisen, ist aus der Sicht derjenigen Personen zu beurteilen, denen die Informationen vorliegen.[31] Stellt sich also bspw. die Frage der Bestimmbarkeit von Daten aus der Sicht eines Datenbearbeiters, so ist zu prüfen, ob ihm Mittel zur Bestimmung der Identität der betroffenen Personen zur Verfügung stehen, die er vernünftigerweise einsetzen würde, wenn er an einer Identifizierung Interesse hätte.[32] Im Falle der Weitergabe von Informationen ist ausreichend, wenn der Empfänger die betroffene Person zu identifizieren vermag. Weiter ist gemäss Rechtsprechung des Bundesgerichts die Bestimmbarkeit dann zu bejahen, wenn sie sich zumindest auf einen Teil der gespeicherten Informationen bezieht, auch wenn sich gewisse Daten aus dem gesammelten Datenpacket (z.B. eine Sammlung von IP-Adressen) nicht einzelnen Personen zuordnen lassen.[33]

Hinzuweisen ist zudem auf folgende Punkte: Zur Beantwortung der Frage, ob Personendaten vorliegen, ist nicht relevant, ob die bestimmte oder bestimmbare Person die richtige Person ist. Lässt sich über Angaben oder die Umstände zwar eine Person bestimmen, handelt es sich jedoch in Tat und Wahrheit nicht um Personendaten über diese Person, so liegen dennoch (indes falsche) Personendaten vor.[34] Zudem kann eine Information auch mehreren Personen gleichzeitig zugeordnet werden. Personendaten liegen somit

24 *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 7.
25 *Jöhri/Rosenthal* (Anm. 18), Art. 2 N. 6; *Belser* (Anm. 18), Art. 2 N. 7.
26 *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 6.
27 BGE 136 II 508, E. 3.2.
28 BGE 138 II 346, E. 6.1.
29 BGE 138 II 346, E. 6.1.
30 BGE 138 II 346, E. 6.1; BVGer A-7040/2009 vom 30. März 2011, E. 7.2.
31 *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 25; BGE 138 II 346, E. 6.1.
32 *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 26.
33 BGE 138 II 346, E. 6.1; BGE 136 II 508, E. 3.5. Kritisch gegenüber den diesbezüglichen Ausführungen im letztgenannten Urteil *Probst*, Die unbestimmte "Bestimmbarkeit" der von Daten betroffenen Person im Datenschutzrecht, AJP (10/2013), S. 1429f.
34 *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 32.

auch dann vor, wenn die Information einen Sachverhalt betrifft, der in Tat und Wahrheit nur eine Person betrifft, die Information diesbezüglich aber nicht differenziert.[35]

In diesem Zusammenhang sei das Stichwort "Big Data" erwähnt. Mit diesem Ausdruck werden sehr grosse, anonymisierte Datenmengen bezeichnet, welche in unstrukturierter oder wenig strukturierter Form zur Verfügung stehen. "Big Data" sind nicht personenbezogen und werden heute von der Datenschutzgesetzgebung auch nicht erfasst. Obschon "Big Data" anonymisiert und ohne Personenbezug vorliegen, wird heute angenommen, dass durch Recherchen mit (zukünftigen) Softwarelösungen und in grossen Datenmengen solche Daten einer bestimmten Person zugeordnet werden können.[36]

6.2.2.2. Besonders schützenswerte Personendaten (Art. 3 lit. c DSG)

Besonders schützenswerte Personendaten sind gemäss Art. 3 lit. c DSG Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe und administrative oder strafrechtliche Verfolgungen und Sanktionen. Die Liste ist abschliessend. Daten über die Einkommens- und Vermögensverhältnisse fallen somit bspw. nicht unter die besonders schützenswerten Daten.[37] "*Besonders schützenswerte Personendaten können sich - anders als Persönlichkeitsprofile nach Art. 3 lit. d DSG - auch auf juristische Personen beziehen, so bei einem weltanschaulich ausgerichteten Unternehmen, bei Bestrafung oder bei politischen Tätigkeiten einer juristischen Person (z.B. Wahlspenden, Lobbyingarbeit oder Teilnahme an Vernehmlassungen des Gesetzgebers).*"[38]

6.2.2.3. Persönlichkeitsprofile

Unter einem Persönlichkeitsprofil gemäss Art. 3 lit. d DSG wird eine Zusammenstellung einer grösseren Zahl von Daten über die Persönlichkeitsstruktur, die beruflichen Fähigkeiten und Aktivitäten oder auch die ausserberuflichen Beziehungen und Tätigkeiten verstanden, welche ein Gesamtbild oder ein wesentliches Teilbild der betreffenden natürlichen Person ergeben.[39] Dabei ist entscheidend, dass die systematische Zusammenstellung von - an sich nicht besonders schützenswerten - Daten (z.B. über Essgewohnheiten, Reise- und Freizeitaktivitäten) eine Beurteilung wesentlicher Aspekte einer Persönlichkeit wie z.B. das Konsumverhalten oder die Weltanschauung zulassen.[40] Der Begriff des Persönlichkeitsprofils kann jedoch nicht generell definiert werden. So ist für die Frage, ob eine Zusammenstellung mehrerer Daten einer bestimmten Person ein Persönlichkeitsprofil ergibt, Menge und Inhalt der personenbezogenen Informationen ausschlaggebend. Daten, die über einen längeren Zeitraum zusammengetragen werden und so ein biografisches Bild ergeben (ein sog. Längsprofil), sind eher als Persönlichkeitsprofil zu qualifizieren als solche, die eine blosse Momentaufnahme darstellen (sog. Querprofil).[41]

6.2.2.4. Daten von Grosskunden im Besonderen

Im Fokus der datenschutzrechtlichen Diskussion im Zusammenhang mit Smart Grid liegen die Daten der natürlichen Personen. Dies, weil natürliche Personen gegenüber Unternehmen aus der Energie- sowie anderen involvierten Branchen in der Regel eine deutlich schwächere Verhandlungsposition haben und ihre Persönlichkeitsrechte kaum durchsetzen können. Mit Datenschutzregeln bezogen spezifisch auf Smart Grid bzw. Me-

---

35 *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 33.

36 Vgl. allgemein zum Thema *Bäriswyl*, "Big Data" ohne Datenschutz-Leitplanken, in: digma (1/2013), S. 14-17.

37 *Belser* (Anm. 18), Art. 3 N. 11f., vgl. zu den einzelnen Begriffen *Belser* (Anm. 18), Art. 3 N. 13ff.

38 *Jöhri/Rosenthal* (Anm. 18), Art. 2 N. 45.

39 *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 56, 60.

40 *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 56.

41 *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 57.

ter – Daten wird versucht, Persönlichkeitsverletzungen von vornherein zu verhindern und den betroffenen Personen ein effektives Instrumentarium zur Verfügung zu stellen, Persönlichkeitsverletzungen abzuwehren (vgl. dazu Länderberichte in Kapitel 6.5).

Die Schweiz ist eine der wenigen Rechtsordnungen, in welchen auch Daten der juristischen Personen Datenschutz geniessen, weshalb diese Daten im vorliegenden Bericht behandelt werden. Im Zusammenhang mit Smart Grid stehen jedoch die Daten der juristischen Personen nicht im Fokus. Einerseits ist die Thematik des Schutzes der Meter-Daten für diese Unternehmen teilweise nicht neu. Namentlich müssen Unternehmen mit einem Stromverbrauch von über 100 MWh, die von ihrem Anspruch auf Netzzugang Gebrauch machen sowie Erzeuger, die eine Anschlussleistung über 30 kVA besitzen, mit einer Lastgangmessung mit automatischer Datenübermittlung ausgestattet sein (Art. 8 Abs. 5 i.V.m. Art. 11 StromVV). Dabei wird in der Regel im 15-min-Takt gemessen und übermittelt. Andererseits stellen die Daten zum Energieverbrauch bzw. zur Energieproduktion der juristischen Personen Geschäftsgeheimnisse dar, deren Geheimhaltung meistens in Energieversorgungsverträgen geregelt ist. Die Verletzung solcher Geschäftsgeheimnisse kann strafrechtlich geahndet werden (vgl. Art. 162 des Schweizerischen Strafgesetzbuches).

6.2.2.5. Qualifikation der Daten der Use Cases

Elektrische Geräte haben einen unterschiedlichen Energieverbrauch. Diese sog. "elektrische Signatur" der Geräte ermöglicht bei Verwendung entsprechender Software (im Rahmen von bspw. sog. Nonintrusive load monitoring (NILM) oder nonintrusive appliance load monitoring (NIALM)) grundsätzlich die Erstellung eines detaillierten Bildes der Aktivitäten im vom Smart Meter gemessenen (Gebäude-)Komplex.[42] In der Vernehmlassung wurde darauf hingewiesen, dass nach derzeitigen wissenschaftlichen Erkenntnissen die Aussagekraft der momentan geplant aufzunehmenden Daten (wahrscheinlich Viertelstundentakt) als eher gering einzuschätzen sei. Wie aussagekräftig (bzw. personenbezogen) die durch Smart Metering gewonnen Daten in den Use Cases sind, hängt insgesamt von verschiedenen Faktoren ab. So ist zunächst von Bedeutung, in welcher Granularität die Daten aufgenommen und in den Use Cases versendet werden (im Viertelstundentakt, stündlich, minütlich oder gar in Echtzeit[43]) oder aber um was für ein Gebäude es sich konkret handelt (Wohngemeinschaft mit vielen Studenten, Einpersonenhaushalt, Produktionshalle eines Unternehmens usw.). Verschiedene Studien lassen den Schluss zu, dass Aufgrund der zurzeit verfügbaren Daten Aussagen über die Grösse von Haushalten (Anzahl Bewohner, Anzahl Schlafzimmer usw.) und die Einkommensverhältnisse der Bewohner grundsätzlich ableitbar sind, dass sich jedoch die Aussagegenauigkeit bei Abnahme der Datenqualität bzw. Granularität rasch verringert.[44]

Die Analyse der 12 Use-Cases hat gezeigt, dass es sich bei einem grossen Teil der erfassten Datenströme, wie bspw. bei Abrechnungsdaten, Kundendaten, Meter-Daten und historischen Meter-Daten, Netzkonfigurationsdaten, Netzbauplanungsdaten usw., um Personendaten i.S.d. DSG handelt und bei deren Bearbeitung die Vorgaben des DSG zu beachten sind.[45] Vor allem im Zusammenhang mit den Meter-Daten können besonders schützenswerte Personendaten oder Persönlichkeitsprofile generiert werden, wobei dies

---

42 *U.S. Department of Commerce*, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, 2010, S. 27, ausführlich *Quinn*, Privacy and the New Energy infrastructure 9 (Working Paper), 2008, S. 22ff.

43 Ob Smart Meter in (naher) Zukunft konstante Online Datenflüsse erzeugen werden, ist umstritten.

44 Siehe *Beckel/Sadamori/Santini*, Automatic Socio-Economic Classification of Households Using Electricity Consumption Data, Proceedings of the 4th International Conference on Future Energy Systems (ACM e-Energy '13), 2013; *Beckel/Sadamori/Santini,* Towards Automatic Classification of Private Households Using Electricity Consumption Data, Proceedings of the Fourth ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings (BuildSys '12), 2012, S. 169-176; *Beckel/Kleiminger/Staake/Santini*, Improving Device-level Electricity Consumption Breakdowns in Private Households Using ON/OFF Events, Proceedings of the 3rd International Workshop on Networks of Cooperating Objects (CONET 2012), 2012, S. 40-52.

45 Siehe hierzu Kap. 6.4 Folgen der Anwendbarkeit des DSG.

vom Umfang und dem Zeitraum der Datensammlung abhängig ist. Bei gewissen Daten, wie bspw. Prognosedaten Energie, Messdaten Ein-/Ausspeisung oder Ein-/Ausspeiseprognosen, ist für die Frage der Personenbezogenheit von Bedeutung, zu welchem Grad die Daten anonymisiert worden sind (K-Anonymität), m.a.W. ob noch Rückschlüsse auf die einzelnen Datensätze bzw. Personen gezogen werden können. Ist dies zu verneinen, liegen keine personenbezogenen Daten vor. Bearbeiten juristische Personen intern ihre eigenen Daten, wie zum Teil bei der Echtzeit regionale Netzauslastung oder der Netzkonfiguration, fällt diese Bearbeitung nicht unter die Bestimmungen des DSG.[46] Daneben gibt es gewisse Daten, welche sehr wahrscheinlich keinen Personenbezug haben, wie bspw. die Marktinformationen, und bei denen das DSG somit nicht zur Anwendung gelangt. Bei einem Grossteil der Daten ist indes aufgrund der derzeitigen Unsicherheiten über die konkrete Ausgestaltung dieser Use Cases keine abschliessende Qualifikation der Daten möglich.

6.2.3. Bearbeitung durch private Personen und Bundesbehörden

Der persönliche Geltungsbereich des eidgenössischen Datenschutzgesetzes wird in Art. 2 DSG geregelt. Demnach gilt es für die Bearbeitung von Daten durch private Personen und Bundesorgane. Als private Personen i.S.d. DSG gelten alle natürlichen und juristischen Personen im weiteren Sinne, welche Personendaten aufgrund eines Sachverhalts bearbeiten, der seinerseits durch das Privatrecht geregelt wird.[47] Als Bundesbehörden gelten gemäss Art. 3 lit. h DSG Behörden und Dienststellen des Bundes sowie Personen, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind. Gemäss Maurer-Lambrou/Kunz gelten als Behörden und Dienststellen des Bundes sämtliche in Art. 2 RVOG erwähnten Behörden und Dienststellen der Bundesverwaltung, also auch bspw. alle dezentralisierten Verwaltungseinheiten des Bundes.[48] Werden z.B. im Rahmen des Energiedatenmanagements die Daten von Datenmanagern, Energiehändler, Lieferanten oder sonstigen privaten Marktteilnehmern bearbeitet (Use Case 1), liegt eine Bearbeitung durch Private nach Art. 2 Abs. 1 i.V.m. Art. 3 lit. h DSG vor.

Das DSG gelangt nicht zur Anwendung, wenn eine Datenbearbeitung durch kantonale öffentlich-rechtliche Körperschaften und Anstalten zur Diskussion steht und soweit die Datenbearbeitung im Rahmen der öffentlichen kantonalen Tätigkeit erfolgt, da in diesem Rahmen – unter Vorbehalt von Art. 37 DSG – das kantonale Datenschutzrecht eingreift.[49] So unterstehen bspw. die kantonalen Sozialversicherungsanstalten oder eine Psychiatrische Klinik nicht dem eidgenössischen DSG. Im Falle der Psychiatrischen Klinik hielt das Bundesgericht fest, dass die privatrechtliche Trägerschaft nicht ausschlaggebend sei. Vielmehr ergaben sich verschiedene Anhaltspunkte (öffentlicher Leistungsauftrag, öffentlich festgelegte Taxen und öffentliche Aufsicht), welche für eine Zuordnung zu einem Patientenverhältnis kantonal öffentlich-rechtlicher Natur sprachen, wodurch die Anwendbarkeit des Bundesdatenschutzgesetzes verneint wurde.[50]

Anwendbar ist das DSG dagegen auf Daten von privatrechtlichen Körperschaften des kantonalen Rechts und öffentlich-rechtliche Anstalten und Körperschaften der Kantone und des Bundes. Werden also Personendaten bspw. der Industrielle Werke Basel (IWB) bearbeitet, unterliegt diese Bearbeitung grundsätzlich dem DSG, bearbeitet die IWB dagegen selber Personendaten, unterliegt dies dem Gesetz über die Information und den Datenschutz des Kantons Basel-Stadt (IDG). Für das Smart Metering Projekt der IWB bei datenschutzrechtlichen Fragen ist somit der Datenschutzbeauftragte von Basel-Stadt zu-

[46] *Jöhri/Rosenthal* (Anm. 18), Art. 2 N. 13.

[47] Vgl. *Bundesrat* (Anm. 15), S. 440.

[48] *Maurer-Lambrou/Kunz*, in: Maurer-Lambrou/Vogt, Basler Kommentar zum Datenschutzgesetz, 2006, Art. 2 N. 13.

[49] BGE 122 I 153, E. 2c. Vgl. zu Möglichkeiten der Schaffung einer einheitlichen Regelung im Sinne des DSG Kap. 6.3 Vereinheitlichung der Datenschutzregelung für Smart Grid und Smart Meters durch Bundesrechtliche Regelung.

[50] Vgl. BGE 122 I 153, E. 2e und f, dazu auch *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 101.

ständig.[51] Ein weiteres Beispiel sind die Elektrizitätswerke des Kantons Zürich, welche einen Leistungsauftrag erfüllen, die Elektrizitätstarife in Form von allgemein verbindlichen Gebühren für Anschluss und Lieferung ausgestalten und der Oberaufsicht des Kantonsrates unterstehen.[52] Aufgrund ihrer Rechtsform, der Ausgestaltung der Beziehungen zu den Endverbrauchern und der Oberaufsicht sind die Elektrizitätswerke des Kantons Zürich im Bereich des Smart Grids bzw. Smart Metering dem kantonalen und nicht dem eidgenössischen Datenschutzrecht unterstellt.[53]

Schliesslich ist zu klären, ob und in welcher Form Bundesbehörden (Art. 3 lit. h DSG) am Datenaustausch teilnehmen. Da für die Datenbearbeitung durch Bundesorgane strengere und detailliertere Datenschutzregelungen gelten (vgl. dazu Kap. 6.4.4.5). als für die Datenbearbeitung durch Private, ist die Qualifikation als private Person oder als Bundesorgan von Bedeutung. Bundesorgane dürfen Personendaten grundsätzlich nur bearbeiten, wenn eine gesetzliche Grundlage besteht (Art. 17 Abs. 1 DSG). Für die Bearbeitung besonders schützenswerter Personendaten sowie von Persönlichkeitsprofilen wird zudem gemäss Art. 17 Abs. 2 DSG eine Rechtsgrundlage in einem Gesetz im formellen Sinn (Art. 3 lit. j DSG) verlangt. Eine gesetzliche Grundlage i.S.v. Art. 17 DSG muss grundsätzlich auch für das Bekanntgeben von Personendaten vorliegen (vgl. Art. 19 Abs. 1 DSG), wobei die Anforderungen an die Rechtsgrundlage für das Zugänglichmachen von Personendaten durch ein Abrufverfahren noch strenger sind (Art. 19 Abs. 3 DSG).[54] In diesem Zusammenhang ist die Einordnung der Übertragungsnetzbetreiberin Swissgrid umstritten. Einerseits wird argumentiert, dass der Übertragungsnetzbetrieb keine staatliche Aufgabe darstelle, die Swissgrid somit nicht hoheitlich handle, Rechtverhältnisse mit anderen Privaten somit privatrechtlicher Natur seien.[55] Andererseits wird vertreten, dass es sich beim Übertragungsnetzbetrieb um eine staatliche Aufgabe handle, die Swissgrid also als eine mit öffentlichen Aufgaben des Bundes betraute Person zu behandeln sei.[56] Die Frage ist derzeit nicht definitiv entschieden.

6.2.4. Inhaber einer Datensammlung

Gemäss Art. 3 lit. g DSG gilt als Datensammlung jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind. Somit ist jeder Bestand von Personendaten (bspw. elektronischer Datenträger, Ordner, Liste, Aktenablage, Kundendossier etc.), der so konzipiert ist, dass die zu einer bestimmten Person gehörenden Personendaten mit vernünftigem Aufwand aufgefunden werden können, als Datensammlung zu qualifizieren.[57]

Beim Inhaber einer Datensammlung handelt es sich um private Personen oder Bundesorgane, die über den Zweck und den Inhalt der Datensammlung entscheiden (Art. 3 lit. i DSG). Beim Zweck handelt es sich um den Zweck der Sammlung, also bspw. die Samm-

---

51 Vgl. hierzu die Mitteilung des Basler Datenschutzbeauftragten, abrufbar unter: <http://www.srf.ch/news/regional/basel-baselland/datenschutz-erlaubt-iwb-die-nutzung-der-intelligenten-stromzaehler>.

52 Vgl. Gesetz betreffend die Elektrizitätswerke des Kantons Zürich (EKZ-Gesetz) vom 19. Juni 1983, § 1 bezüglich der Rechtsform, § 8 bezüglich der Tarifgestaltung, § 9 bezüglich der Oberaufsicht; *Klaus*, DeRegulierung der netzbasierten Infrastruktur, 2009, S. 429.

53 Vgl. zu den Abgrenzungskriterien BGE 122 I 153 bezüglich einer privatrechtlich organisierten Psychiatrischen Klinik; dazu Datenschutzbeauftragter des Kantons Zürich, Tätigkeitsbericht 2009, S. 30, in welchem der kantonale Datenschutzbeauftrage den Elektrizitätswerken Zürich im Rahmen eines Pilotprojektes mit Smart Metering empfohlen hat, eine Verlängerung der Messintervalle zu prüfen.

54 *Jöhri/Rosenthal* (Anm. 18), Art. 2 N. 17. Bezüglich der Bedenken einer staatlichen Überwachung der Verbraucher (vgl. hierzu etwa der US-amerikanische Fall Kyllo, in welchem die Polizei durch die Überwachung des Stromverbrauchs eine Indoor-Hanfplantage ausfindig machte, Kyllo v. United States 533 u.s. 27 (2001)) ist auf die strafrechtlichen Bestimmungen (StGB; StPO) und das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) zu verweisen, welche die Voraussetzungen für solche Massnahmen regeln.

55 BVGer, Urteil A-3505/2011 vom 26. März 2012, E. 5.5.

56 *Walther*, Kooperative Steuerungsinstrumente im schweizerischen Stromversorgungsrecht (noch nicht veröffentlicht), S. 97f., *Hettich/Walther*, Rechtsfragen um die kostendeckende Einspeisevergütung (KEV) für Elektrizität aus erneuerbaren Energien, in: ZBl (3/2011), S. 151ff.

57 *Bracher*, Das Auskunftsrecht nach DSG - Inhalt und Einschränkung im Vorfeld eines Zivilprozesses, in: SJZ (109/2013), S. 47.

lung von Leistungsdaten von Sportlern zur Erstellung von Trainingsplänen. Mit Inhalt sind die Parameter gemeint, welche den Inhalt der Datensammlung bestimmen, wie z.B. die Art, die Detailtiefe oder der Umfang der Daten oder die Art und Weise ihrer Beschaffung und weiteren Bearbeitung. Inhaber ist m.a.W. derjenige, welcher die im konkreten Fall wesentlichen datenschutzrechtlichen Parameter einer Datensammlung kontrolliert. Kontrolle meint dabei eine (anhaltende) Herrschaft über diese wesentlichen Parameter. Zu beachten ist jedoch, dass diese Kontrolle durch die den betroffenen Personen zustehenden Instrumente (z.B. Auskunfts-, Berichtigungsrechte etc.) eingeschränkt werden kann.

Inhaber einer Datensammlung können auch mehrere natürliche und oder juristische Personen gemeinsam sein, und zwar dann, wenn sie die Parameter gemeinsam festlegen. Dies gilt auch dann, wenn sie mitunter unterschiedliche Zwecke verfolgen, wobei die Datensammlung in diesem Fall mehreren Zwecken dient. Entscheidend ist hier, dass die verschiedenen Personen voneinander wissen und einander die Ausübung ihrer jeweiligen Kontrolle erlauben. Der Inhaber einer Datensammlung ist der primäre datenschutzrechtliche Verantwortungsträger für die Datensammlung, weshalb ihm auch vom Gesetzgeber verschiedene Sonderpflichten auferlegt werden.[58]

6.3. Vereinheitlichung der Datenschutzregelung für Smart Grid und Smart Meters durch Bundesrechtliche Regelung

Nach der hier vertretenen Auffassung erscheint es als wenig sinnvoll, dass im Bereich des Betriebs von Smart Grids verschiedene datenschutzrechtliche Bestimmungen, also neben der Bundesregelung auch kantonale Datenschutzgesetze, zur Anwendung gelangen. Da gemäss Art. 8 StromVV[59] der Netzbetreiber für das Messwesen und die Informationsprozesse verantwortlich ist, stehen die Verteilnetzbetreiber mit ihren Geschäftsbeziehungen zum Kunden aus Sicht des DSG im Fokus.[60] Ebendiese Verteilnetzbetreiber üben indes oftmals eine öffentliche kantonale Tätigkeit aus; sie sind also als Datenbearbeiter dem jeweiligen kantonalen DSG unterstellt.[61] Für eine einheitliche Unterstellung unter eine bundesweite Regelung zum Datenschutz im Bereich von Smart Grids sprechen die Elimination von bestehenden Divergenzen unterschiedlicher kantonaler Regelungen und die Schaffung einer einheitlichen Zuständigkeit. Damit einhergehen würde eine Verminderung des Aufwands auf Anbieterseite im Bereich der Sicherstellung der datenschutzrechtlichen Compliance. Sodann wird die Homogenisierung der heterogenen kantonalen Gesetze durch den anbieterseitigen Wunsch, schweizweit einheitliche Lösungen anbieten zu können, unterstützt. Eine andernfalls unter Umständen zu erfolgende geringe Skalierung lokaler Lösungen in einer entsprechend fragmentierten Schweiz würde Lösungen unnötig verteuern und wäre somit volkswirtschaftlich ineffizient.

Unterschiedliche kantonale datenschutzrechtliche Standards könnten wettbewerbsverzerrende Wirkungen aufweisen. Inwieweit jedoch die Gefahr für ein kantonales „race to the bottom“ beim Datenschutz besteht, wenn auf einheitliche Regelungen verzichtet wird, kann nicht abschliessend beantwortet werden. Sowohl strengere als auch lockerere Datenschutzbestimmungen können sich theoretisch standortfördernd für den Kanton auswirken.

Im Bereich des Betriebs eines Smart Grids, welches auch Smart Metering Funktionen beinhaltet, wird deshalb eine einheitliche Regelung auf Bundesebene bzw. die Unterstellung unter das eidgenössische Datenschutzgesetz als sinnvoll erachtet. Dazu ist zunächst zu prüfen, ob hierfür eine verfassungsmässige Bundeskompetenz vorliegt, da ansonsten die

---

58 *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 105ff. Zu den Sonderpflichten, siehe Kap. 6.4.7 Beispiel anhand des Use Cases 1.

59 Stromversorgungsverordnung vom 14. März 2008 (StromVV), SR 734.71.

60 *Leber*, Datenschutz bei digitalen Stromzählern, in: VSE Recht (9/2011), S. 58.

61 Zur Unterstellung kantonaler Einheiten vgl. auch *Leber* (Anm. 50), S. 59.

Kompetenz auf kantonaler Ebene liegen würde.[62] Zu berücksichtigen ist dabei, dass Smart Meters eine duale Funktion haben: Einerseits tragen Sie zur Senkung des Energieverbrauchs bei, andererseits dienen sie im Rahmen des Smart Grids dem effizienten Betrieb und der Sicherheit der elektrischen Netzinfrastruktur und tragen gleichzeitig zur Versorgungssicherheit bei.[63]

6.3.1. Energieeffizienz

Für die Kompetenzausscheidung im Bereich der Energiepolitik, welche insbesondere Massnahmen der Energieeffizienz mitumfasst, ist Art. 89 BV einschlägig. Die Bestimmung geht auf Art. 24^{octies} der "alten" Bundesverfassung vom 29. Mai 1874 (aBV) zurück, die bis zum 31. Dezember 1999 in Kraft stand. Gegenüber der Vorgängerbestimmung wurden in Art. 89 BV lediglich minimale sprachliche, nicht aber inhaltliche Änderungen vorgenommen.[64] Art. 89 BV bezieht sich gemäss seiner Sachüberschrift auf die "Energiepolitik" und umfasst, wie bereits Art. 24^{octies} aBV, sämtliche Energieträger und stellt damit eine übergeordnete Norm dar, die dem Querschnittscharakter der Energiepolitik Rechnung trägt. Thematisch ist die Bestimmung neben der Energieversorgung schwergewichtig auf den Energieverbrauch, insbesondere den Endverbrauch, ausgerichtet.[65]

Art. 89 Abs. 3 Satz 1 BV begründet einen sachlich auf den *Energieverbrauch von Anlagen, Fahrzeugen und Geräten* begrenzten, in diesem Bereich jedoch umfassenden Gesetzgebungsauftrag an den Bund.[66] Diese Kompetenz erlaubt dem Bund bspw. Bestimmungen über energietechnische Prüfverfahren, die Angabepflichten über den Energieverbrauch sowie Vorschriften zur Reduktion des Energieverbrauchs zu erlassen.[67] Dieser Verpflichtung ist der Bund unter anderem mit dem Erlass des EnG nachgekommen, in dessen drittem Kapitel die entsprechenden Regelungszuständigkeiten festgehalten sind.[68] Gestützt auf Art. 8 Abs. 1 lit. c EnG kann der Bundesrat die Anforderungen an das Inverkehrbringen von serienmässig hergestellten Geräten, insbesondere auch deren Standby-Verbrauch, sofern sie elektrisch betrieben werden, regeln. Die Regelungskompetenz des Bundes im Bereich des Energieverbrauchs von Haushaltsgeräten ist wie gesagt umfassend.[69] Im Bereich der Vorschriften zur Reduktion des Energieverbrauchs von Geräten könnte man somit argumentieren, dass der Bund die Kompetenz hat, notwendige Standards für ein reibungsloses bzw. effizientes Zusammenspiel der Geräte zu definieren, welche im Ergebnis zu einer Verringerung des Energieverbrauchs der Geräte beitragen. Für den Betrieb eines Smart Grids unter Einsatz von Smart Metering Geräten bestünde somit gemäss diesen Überlegungen eine umfassende Bundeskompetenz in Bezug auf die Regelung des Energieverbrauchs von Geräten.

Art. 89 Abs. 4 BV hält fest, dass für Massnahmen, die den Verbrauch von Energie in Gebäuden betreffen, vor allem die Kantone zuständig sind. Damit verbleibt dem Bund zwar eine subsidiäre Kompetenz, mit dem Akzent allerdings, dass hier vor allem die Kanone zuständig sein sollen, der Bund also höchstens gewisse Grundsätze erlassen kann.[70]

---

62 Vgl. Art. 3 und 42 BV, dazu *Häfelin/Haller/Keller*, Schweizerisches Bundesstaatsrecht, 2008, N. 1052.

63 Vgl. dazu *Bundesamt für Energie*, Schlussbericht der Folgenabschätzung einer Einführung von Smart Metering im Zusammenhang mit Smart Grids in der Schweiz vom 5. Juni 2012.

64 *Schaffhauser*, in: Ehrenzeller/Mastronardi/Schweizer/Vallender (Hrsg.), Die schweizerische Bundesverfassung, Kommentar, 2008, N. 1 zu Art. 89.; zu Art. 24^{octies} aBV vgl. *Jagmetti*, in: Aubert/Eichenberger/Müller/Rhinow/Schindler (Hrsg.), Kommentar zur Bundesverfassung der Schweizerischen Eidgenossenschaft vom 19. Mai 1874, 1995, N 1. zu Art. 24^{octies}.

65 *Schaffhauser* (Anm. 65), N. 4 zu Art. 89.

66 *Biaggini*, Bundesverfassung der Schweizerischen Eidgenossenschaft, Kommentar, 2007, N. 6 zu Art. 89 BV; *Schaffhauser* (Anm. 65), N. 13 zu Art. 89 BV; vgl. *Weber*, Energie und Kommunikation, in: Aubert/Müller/Thürer, Verfassungsrecht der Schweiz, 2001, § 60 N. 8.

67 Vgl. *Bundesrat*, Botschaft zum Energiegesetz (EnG) vom 21. August 1996, BBl 1996 IV 1005, S. 1064; vgl. dazu die gegenwärtige Regelung in Art. 8 EnG.

68 *Schaffhauser* (Anm. 65), N. 13 zu Art. 89 BV; Vgl. 3. Kapitel Energiegesetz vom 26. Juni 1998 (EnG), SR 730.00; *Weber* (Anm. 67), § 60 N. 8.

69 *Biaggini* (Anm. 67), N. 6 zu Art. 89; *Schaffhauser* (Anm. 65), N. 13 zu Art. 89 BV; vgl. *Weber*, (Anm. 67), § 60 N 8.

70 *Schaffhauser* (Anm. 65), N. 15 zu Art. 89 BV.

Anderer Meinung ist Biaggini, welcher festhält, dass sich aus Art. 89 Abs. 4 BV nicht ableiten lasse, dass der Bund sich hier auf den Erlass von Grundsätzen zu beschränken habe, sondern der Bund nur zu Zurückhaltung angehalten sei. Insbesondere könne das Zurückhaltungsgebot durch andere Bundeskompetenzen überlagert werden.[71] Damit könnte argumentiert werden, dass Art. 89 Abs. 4 BV einer bundesrechtlichen Regelung nicht im Wege steht. Historisch bezieht sich Art. 89 Abs. 4 BV ohnehin vor allem auf die Wärmeisolation, den Energiemix zur Deckung des Wärmebedarfs und Vorgaben über die Angabe des Energieverbrauchs von Gebäuden,[72] was sich auch aus Art. 9 EnG ergibt, welcher die verfassungsmässige Kompetenzzuweisung konkretisiert.

6.3.2. Zuständigkeit im Bereich des Transports und der Lieferung elektrischer Energie

In Art. 91 BV findet sich sodann eine Regelungskompetenz des Bundes im Bereich des Transports und der Lieferung von elektrischer Energie. Nach umstrittener Auffassung soll die umfassende Gesetzgebungskompetenz dem Bund in Abweichung von der Wirtschaftsfreiheit die Errichtung eines vollständigen oder teilweisen Monopols der Elektrizitätsübertragung erlauben. Er soll dieses selber bewirtschaften oder mittels Konzession auf Dritte übertragen können.[73] Der Bund kann gestützt auf die Bestimmung Tarifvorschriften erlassen, Regelungen betreffend die Unternehmen der Elektrizitätswirtschaft verankern sowie Massnahmen im Bereich der Versorgungssicherheit wie z.B. Anschluss- und Lieferpflichten vorsehen.[74] Ziel dieser Regelungen ist die Gewährleistung einer möglichst sicheren, gleichmässigen und preisgünstigen Landesversorgung mit Elektrizität.[75]

Da der Bund gestützt auf Art. 91 BV eine umfassende Regelungskompetenz für den Transport und die Lieferung von elektrischer Energie hat, kann er nach hier vertretener Auffassung in diesem Bereich tätig werden und den Betrieb eines Smart Grids, welches mit dem Einsatz von Smart Metern einher geht, der Anwendung einer zu erlassenden bundesrechtlichen Regelung und/oder des eidgenössischen Datenschutzgesetzes unterstellen. Dieser Auffassung bezüglich Kompetenz im Bereich des Smart Meterings scheint auch der Bundesrat zu sein. Im Rahmen des ersten Massnahmenpakets der Energiestrategie 2050 ist, wie in der dazugehörigen Botschaft[76] beschrieben, eine Delegationsnorm vorgesehen, welche dem Bundesrat, sofern nötig, die Kompetenz zum Erlass von Vorgaben bei der Einführung von intelligenten Messsystemen und entsprechender technischer Mindestanforderungen einräumt. Der Bundesgesetzgeber hat somit bereits selbst vorgesehen, im Bereich des Smart Meterings von seiner umfassenden Gesetzgebungskompetenz Gebrauch zu machen und Detailfragen zu regeln.[77] Ob mit Bezug auf den Datenschutz eine reine Delegationsnorm den verfassungsrechtlichen Anforderungen an die Gesetzgebung genügt (vgl. Art. 164 BV), müsste jedoch im Detail geprüft werden.

---

71 *Biaggini* (Anm. 67), N. 6 zu Art. 89.

72 Vgl. zur im Wortlaut identischen Regelung in der aBV *Jagmetti* (Anm. 65), N. 63 zu Art. 24^{octies}.

73 So *Bundesrat*, Botschaft zum Elektrizitätsmarktgesetz (EMG) vom 7. Juni 1999, BBl 1999 7370, S. 7463; siehe ebenfalls *Bundesrat*, Botschaft zur Änderung des Elektrizitätsgesetzes (EleG) und zum Bundesgesetz über die Stromversorgung (StromVG) vom 3. Dezember 2004, BBl 2005 1611, S. 1674; *Schaffhauser* (Anm. 65), N. 3 zu Art. 91; differenziert: *Rechsteiner*, Gutachten zu Rechtsfragen im Zusammenhang mit der Errichtung einer schweizerischen Netzgesellschaft für die Übertragung von Elektrizität, erstattet im Auftrag des Bundesamtes für Energie, 27. November 2003, N. 30ff. Zu Recht kritisch *Biaggini* (Anm. 67), N. 3 zu Art. 91; *Aubert*, Petit commentaire de la Constitution fédérale de la Confédération suisse, 2003, N.9 zu Art. 91.

74 *Bundesrat* (Anm. 73), S. 1674. Der sogenannte "Third Party Access" wurde in Art. 13 Abs. 1 StromVG realisiert.

75 *Straub*, Der Zugang zu den Elektrizitätswerken in Europa und der Schweiz, S. 13.

76 *Bundesrat*, Botschaft zum ersten Massnahmenpaket der Energiestrategie 2050 (Revision des Energierechts) und zur Volksinitiative "Für den geordneten Ausstieg aus der Atomenergie (Atomausstiegsinitiative)", nicht amtlich publizierte Fassung.

77 *Bundesrat* (Anm. 76), S. 75.

6.3.3. Zwischenfazit

Entsprechend wäre nach hier vertretener Auffassung eine Regelung bezüglich der Unterstellung des Betriebs von Smart Grids in Verbindung mit dem Einsatz von Smart Meter unter eine einheitliche bundesrechtliche Regelung zu begrüssen, um die Einheitlichkeit der Rechtsordnung und die damit einhergehenden Vorteile sicherzustellen. Auch die duale Funktion des Smart Meterings, mithin also die allfälligen Energieeinsparungen, ändern nach hier vertretener Auffassung nichts an der Kompetenz des Bundes zum Erlass von Detailvorschriften im Bereich des Betriebs von Smart Grids unter Einsatz von Smart Metering. Einerseits ist umstritten, in welchem Ausmass der Kanton im Bereich von Art. 89 Abs. 4 legiferieren kann. Andererseits besteht im Rahmen von Art. 91 BV eine umfassende Regelungskompetenz des Bundes für den Transport und die Lieferung elektrischer Energie. Im Rahmen dieser Kompetenz wird ein allenfalls bestehendes Zurückhaltungsgebot nach Art. 89 Abs. 4 BV nach hier vertretener Auffassung überlagert,[78] da die primäre Funktion eines Smart Grids, welches mit dem Einsatz von Smart Meter einhergeht, auf Netzebene liegt[79] und somit unter die Bundeskompetenz von Art. 91 BV fällt. Zudem darf der sachliche Anwendungsbereich von Art. 89 Abs. 4 BV für den Betrieb von Smart Grids unter Einsatz von Smart Metering in Frage gestellt werden, da sich Art. 89 Abs. 4 BV bzw. der ihn konkretisierende Art. 9 EnG vor allem mit Massnahmen der Gebäudeisolation und Vorschriften im Bereich des Energiemix zur Deckung des Wärmebedarfs von Gebäuden auseinandersetzt. Darüber hinaus besteht gestützt auf Art. 89 Abs. 3 BV eine umfassende Bundeskompetenz zur Regelung des Energieverbrauchs von Anlagen, Fahrzeugen und Geräten, welche auch das Zusammenspiel von Smart Metern mit Haushaltsgeräten umfasst, um zu einer Verringerung des Energieverbrauchs ebendieser Geräte beizutragen.

Wie obenstehend dargelegt, verfügt der Bund somit in mehreren, sachlich den Betrieb von Smart Grids unter Einsatz von Smart Metern betreffenden Bereichen über umfassende Gesetzgebungskompetenzen. Eine Unterstellung des Betriebs von Smart Grids und den damit einhergehenden Smart Metern unter eine bundesrechtliche Regelung und/oder das eidgenössische Datenschutzgesetz gestützt auf die soeben dargelegte Kompetenzordnung erscheint nach hier vertretener Auffassung somit als möglich und sinnvoll. Nachfolgend wird davon ausgegangen, dass das eidgenössische Datenschutzgesetz anwendbar sein wird, sei es als ausschliessliche Regelung, sei es als Ergänzung zu einer spezifisch für Smart Grids erlassenen bundesrechtlichen Regelung.

6.4. Folgen der Anwendbarkeit des DSG

Liegen personenbezogene Daten gemäss DSG vor, hat dies für den Datenbearbeiter die Folge, dass verschiedene Vorschriften beachtet werden müssen. So hält Art. 12 Abs. 1 DSG fest, dass bei der Bearbeitung von Personendaten die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzt werden darf. Das Bearbeiten von Personendaten an sich stellt damit noch keine Persönlichkeitsverletzung dar. Eine Persönlichkeitsverletzung ist immer erst das Resultat der Art und Weise oder der Umstände einer bestimmten Datenbearbeitung.[80] Aus Art. 12 DSG ergibt sich ebenfalls, dass nicht jede Verletzung der Persönlichkeit widerrechtlich ist. Widerrechtlich ist eine Verletzung der Persönlichkeit nämlich dann nicht, wenn sie durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz, gerechtfertigt ist (vgl. hierzu: Art.

[78] Vgl. dazu auch Art. 3 Abs. 2 lit. f des Bundesgesetzes über Bauprodukte (BauPG) vom 8. Oktober 1999, SR 933.0, in welchem die Inverkehrbringung von Bauprodukten davon abhängig gemacht wird, ob die damit erstellten Gebäude die Anforderungen an eine sparsame und rationelle Energienutzung erfüllen. Diese Regelung betrifft ebenfalls den Energieverbrauch in Gebäuden i.S.v. Art. 89 Abs. 4 BV, was jedoch durch andere Bundeskompetenzen überlagert wurde.

[79] Vgl. *Bundesrat* (Anm. 76), S. 74.

[80] *Jöhri/Rosenthal* (Anm. 18), Art. 12 N. 3.

13 DSG).[81] Die Aufzählung von persönlichkeitsverletzenden Verhaltensweisen in Art. 12 Abs. 2 DSG ist nicht abschliessend, ein Nachweis einer Persönlichkeitsverletzung im Einzelfall bleibt damit jederzeit offen. Eine Persönlichkeitsverletzung i.S.d. DSG ist damit auch jede (andere) Datenverarbeitung, welche die Persönlichkeit der betroffenen Person auf eine andere Art und Weise verletzt.[82]

6.4.1. Bearbeitungsgrundsätze

Art. 12 Abs. 2 lit. a DSG legt fest, dass ein Verstoss gegen die Bearbeitungsgrundsätze von Art. 4 DSG, Art. 5 Abs. 1 DSG und Art. 7 Abs. 1 DSG immer eine Persönlichkeitsverletzung darstellt. Somit sind insbesondere die Rechtmässigkeit der Bearbeitung (Art. 4 Abs. 1 DSG), der Grundsatz der Bearbeitung nach Treu und Glauben und der Verhältnismässigkeit (Art. 4 Abs. 2 DSG), der Zweckbindungsgrundsatz (Art. 4 Abs. 3 DSG), die Transparenz (Art. 4 Abs. 1 und 4 DSG), die Richtigkeit der Daten (Art. 5 Abs. 1 DSG) und Vorgaben zur Datensicherheit (Art. 7 DSG) zu beachten.[83]

6.4.1.1. Rechtmässigkeit der Bearbeitung (Art. 4 Abs. 1 DSG)

Gemäss Art. 4 Abs. 1 DSG dürfen Personendaten nur rechtmässig bearbeitet werden, eine unrechtmässige Bearbeitung stellt somit eine widerrechtliche Verletzung der Persönlichkeit dar. Ein rechtswidriges Verhalten liegt dann vor, wenn die Bearbeitung der Daten gegen eine in der Schweiz geltende rechtlich verbindliche Norm verstösst (wie bspw. das Sammeln von Daten im Rahmen eines Hausfriedensbruchs nach Art. 186 StGB oder die Verwendung von Daten für unlautere Massenwerbung nach Art. 3 Abs. 2 lit. o UWG[84]).[85]

6.4.1.2. Grundsatz von Treu und Glauben und Verhältnismässigkeit (Art. 4 Abs. 2 DSG)

Eine Bearbeitung von Personendaten hat gemäss Art. 4 Abs. 2 DSG nach Treu und Glauben zu erfolgen. Es handelt sich hierbei um eine Generalklausel, welche dann zum Zuge kommt, wenn die anderen Bearbeitungsgrundsätze nicht greifen. Es können etwa Pflichten zur Information von Betroffenen abgeleitet werden, wenn deren Daten bearbeitet werden und sich eine Mitteilung unter den gegebenen Umständen aufdrängt.[86] Bei der Verhältnismässigkeit geht es darum, dass die Massnahmen geeignet und erforderlich sind, den verfolgten Zweck zu erreichen und dass eine Abwägung der betroffenen Interessen vorzunehmen ist.[87]

6.4.1.3. Zweckbindungsgrundsatz (Art. 4 Abs. 3 DSG)

Personendaten dürfen gemäss Art. 4 Abs. 3 DSG nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Die Bestimmung steht in einem engen Zusammenhang mit dem Transparenzgrundsatz. Der Grundsatz verlangt insbesondere, dass der Zweck der Datenbearbeitung bei der Datenbeschaffung bereits bekannt sein muss. Eine Datenbeschaffung ohne Zweckhintergrund (Datenspeicherung auf Vorrat) verstösst demnach gegen Art. 4 Abs. 3 DSG. Bei den Prozessen des Data Mining und Data Warehousing ist zu beachten, dass die so neu gewonnen Informationen sog. Sekundärdaten darstellen, die

---

81 *Jöhri/Rosenthal* (Anm. 18), Art. 12 N. 3.
82 *Jöhri/Rosenthal* (Anm. 18), Art. 12 N. 14; *Rampini*, in: Maurer-Lambrou/Vogt, Basler Kommentar zum Datenschutzgesetz, 2006, Art. 12 N. 7.
83 *Jöhri/Rosenthal* (Anm. 18), Art. 12 N. 15.
84 Bundesgesetz vom 19. Dezember 1986 gegen den unlauteren Wettbewerb (UWG), SR 241.
85 *Belser/Epiney/Waldmann*, Datenschutzrecht, 2011, § 9 N. 11ff.
86 *Belser/Epiney/Waldmann* (Anm. 85), § 9 N. 21ff.
87 *Belser/Epiney/Waldmann* (Anm. 85), § 9 N. 24.

durch den ursprünglichen Zweck nicht abgedeckt sind.[88] Schliesslich müssen sich auch Dritte, die Personendaten von einem Dateninhaber erhalten, an das Zweckbindungsgebot halten, der Grundsatz der Zweckbindung findet somit für sämtliches Bearbeiten von Personendaten Anwendung.[89] Der Datenbearbeiter muss dafür sorgen, dass die Daten nicht zu anderen Zwecken als bei der Beschaffung ersichtlich oder gesetzlich vorgesehen bearbeitet werden. Es genügt dabei, dass der Bearbeitungszweck aus den Umständen ersichtlich, m.a.W. erkennbar ist. Wer bspw. für die Bestellung eines Produkts seine Adresse angibt, muss davon ausgehen, dass die Adresse für die Abwicklung der Bestellung (Rechnungsstellung, Buchhaltung usw.) verwendet wird. Eine Information der betroffenen Person ist damit im Umkehrschluss nicht erforderlich, ebenso wenig erforderlich zur Einhaltung des Zweckbindungsgrundsatzes ist die Einwilligung der betroffenen Person.[90]

6.4.1.4. Grundsatz der Transparenz (Art. 4 Abs. 4 DSG)

Der Grundsatz der Transparenz verlangt, dass eine Beschaffung von Personendaten und insbesondere der Zweck deren Bearbeitung für die betroffene Person erkennbar sein müssen. Die Erkennbarkeit des Zwecks ist - unter Berücksichtigung des Grundsatzes von Treu und Glauben - nach den Umständen im Einzelfall zu beurteilen. Es gilt demnach zu prüfen, mit welchen Bearbeitungszwecken die betroffene Person zum Zeitpunkt der Beschaffung der Daten in guten Treuen rechnen durfte. Von einer gewissen Aufmerksamkeit bzw. einem Interesse des Betroffenen am Schicksal seiner Daten darf im Rahmen der Prüfung ausgegangen werden. Der Grundsatz der Transparenz sieht somit nicht zwingend eine aktive Informationspflicht vor; eine solche kann sich jedoch ergeben, wenn der Zweck der Bearbeitung sich aus den Umständen nicht oder nur mit Schwierigkeiten erkennen lässt. Es ist grundsätzlich davon auszugehen, dass sich die Anforderungen an die Transparenz erhöhen, je komplexer und umfassender sich eine Datenbeschaffung gestaltet. Der Grundsatz der Erkennbarkeit kommt auch bei der Beschaffung von Daten über die betroffene Person bei einem Dritten zum Tragen. Der Grundsatz der Transparenz verlangt zudem von Bundesorganen, bei Datenbeschaffungen dem Betroffenen die hierfür erforderliche gesetzliche Grundlage anzugeben. Die Bestimmung zur Transparenz wird für die Beschaffung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen mit den Informationspflichten in Art. 14 DSG (für Private) und Art. 18a DSG (für Bundesorgane) konkretisiert.[91] Ob die Weitergabe von Personendaten im Rahmen von Art. 4 Abs. 3 DSG vorgesehen ist, bestimmt sich danach, ob der ersichtliche Verwendungszweck nur ein Verwendungszweck des Datenbearbeiters ist oder auch entsprechende Zwecke Dritter umfasst.[92]

6.4.1.5. Grundsatz der Datenrichtigkeit (Art. 5 Abs. 1 und Abs. 2 DSG)

Der Grundsatz der Datenrichtigkeit beinhaltet einerseits eine Vergewisserungspflicht (Abs. 1 Satz 1), welche die Verifizierung der Richtigkeit der bearbeiteten Daten verlangt und andererseits eine Berichtigungs- bzw. Löschungspflicht (Abs. 1 Satz 2), wonach unrichtige oder unvollständige Daten berichtigt oder gelöscht werden müssen.[93] Personendaten sind richtig, wenn sie Umstände und Tatsachen sachgerecht wiedergeben.[94] An sich korrekte Angaben können als unrichtig angesehen werden, wenn sie im Hinblick auf den Bearbeitungszweck irreführend sind (Beispielsweise veraltete oder unvollständige Daten).[95] Wenige im Einzelnen richtige Daten können zudem ein verzerrtes oder unvoll-

88 Dies bedeutet, dass solche Sekundärdaten als eigenständige Daten zu behandeln sind, ihre Bearbeitung also bei der Beschaffung ebenfalls angegeben werden bzw. aus den Umständen ersichtlich oder gesetzlich vorgesehen sein muss (Art. 4 Abs. 3 DSG).
89 *Belser/Epiney/Waldmann* (Anm. 85), § 9 N. 29ff.
90 *Jöhri/Rosenthal* (Anm. 18), Art. 4 N. 33ff.
91 *Belser/Epiney/Waldmann* (Anm. 85), § 9 N. 37ff.
92 *Jöhri/Rosenthal* (Anm. 18), Art. 4 N. 41.
93 *Belser/Epiney/Waldmann* (Anm. 85), § 9 N. 45.
94 *Maurer-Lambrou*, in: Maurer-Lambrou/Vogt, Basler Kommentar zum Datenschutzgesetz, 2006, Art. 5 N. 5.
95 *Belser/Epiney/Waldmann* (Anm. 85), § 9 N. 46.

ständiges Gesamtbild wiedergeben. Solche Daten müssen somit berichtigt werden, sodass sie den Gesamtzusammenhang richtig wiedergeben.[96] Die Vergewisserungspflicht im Rahmen von Art. 5 Abs. 1 Satz 1 DSG beinhaltet kein grundsätzliches Verbot der Bearbeitung von unrichtigen Personendaten, sondern verlangt vom Bearbeiter der Daten bloss, sich über deren Richtigkeit zu vergewissern. Welche Anforderungen an das "Vergewissern" zu stellen sind, bestimmt sich nach den Gegebenheiten des Einzelfalls und hängt u.a. auch von der Schwere einer potenziellen Persönlichkeitsverletzung ab. Unrichtige und unvollständige Daten müssen gemäss Abs. 1 Satz 2 vom Datenbearbeiter berichtigt oder vernichtet werden. Die Vernichtungspflicht gilt auch für Daten, welche für den Bearbeitungszweck nicht mehr notwendig sind.

Kein Bearbeitungsgrundsatz, jedoch in diesem Zusammenhang zu erwähnen ist Art. 5 Abs. 2 DSG, welcher das Recht der betroffenen Person auf Berichtigung ihrer Daten zum Gegenstand hat. Die Ausübung des Rechts auf Berichtigung setzt das Vorhandensein unrichtiger Daten voraus.[97] Der Berichtigungsanspruch umfasst jeden noch so nebensächlichen Fehler und gilt ausnahmslos und uneingeschränkt.[98]

6.4.1.6. Datensicherheit

Gemäss Art. 7 DSG müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Ein unbefugtes Bearbeiten im Sinne von Art. 7 Abs. 1 DSG liegt vor, wenn die Bearbeitung der Personendaten unrechtmässig ist. Ein nach Art. 16 DSG gerechtfertigter Verstoss gegen die Bearbeitungsgrundsätze stellt demnach kein unbefugtes Bearbeiten dar. Die zu treffenden Schutzmassnahmen müssen angemessen, d.h. im Hinblick auf die Risiken einer Verletzung des DSG geeignet, erforderlich und zumutbar sein. Ein absoluter oder maximal möglicher Schutz ist nicht erforderlich. Nach Art. 8 Abs. 2 VDSG[99] ist dabei insbesondere der Zweck der Datenbearbeitung, die Art und der Umfang der Datenbearbeitung, die abschätzbaren Risiken für die betroffenen Personen und der gegenwärtige Stand der Technik zu berücksichtigen. In jedem Fall ist die Angemessenheit der getroffenen technischen und organisatorischen Massnahmen aber in ihrer Gesamtheit zu beurteilen. Zudem sind die Schutzmassnahmen laufend zu überprüfen und anzupassen, falls sie unter den geänderten Umständen nicht mehr genügen.[100]

Zu den denkbaren technischen Schutzmassnahmen i.S.v. Art. 7 Abs. 1 DSG gehören sowohl die klassischen IT-Sicherheitsmassnahem wie Zugriffsbeschränkungen als auch physische Schutzmassnahmen ausserhalb der Informatik. Als organisatorische Massnahmen sind zum einen konkrete Produkte und Hilfsmittel wie Reglemente und Weisungen und zum anderen Aktivitäten wie Schulungen und Kontrollen denkbar.

Ein Mangel im Bereich der Datensicherheit stellt einen Verstoss gegen materielle Bearbeitungsvorschriften des DSG dar und zieht dieselben Rechtsfolgen wie jede widerrechtliche Bearbeitung von Personendaten nach sich.[101] Wird also Art. 7 DSG ohne hinreichende Rechtfertigung verletzt, handelt der betreffende Datenbearbeiter rechtswidrig und die betroffene Person kann im Rahmen von Art. 15 bzw. Art. 25 DSG Rechtsansprüche geltend machen.[102]

---

96 *Maurer-Lambrou*, (Anm. 94), Art. 5 N. 6.
97 *Belser/Epiney/Waldmann* (Anm. 85), § 9 N. 58.
98 *Maurer-Lambrou*, (Anm. 94), Art. 5 N. 16.
99 Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG), SR 235.11.
100 *Jöhri/Rosenthal* (Anm. 18), Art. 7 N. 2ff.
101 *Pauli*, in: Maurer-Lambrou/Vogt, Basler Kommentar zum Datenschutzgesetz, 2006 , Art. 7 N. 18f.
102 *Jöhri/Rosenthal* (Anm. 18), Art. 7 N. 10.

6.4.2. Bearbeitung gegen ausdrücklichen Willen

Art. 12 Abs. 2 lit. b DSG untersagt ohne Rechtfertigungsgrund die Bearbeitung von Daten einer Person gegen deren ausdrücklichen Willen. Die betroffene Person kann die Bearbeitung ihrer Personendaten jederzeit und voraussetzungslos untersagen, die Widerspruchserklärung kann formlos und konkludent erfolgen, ist indes empfangsbedürftig. Ein Widerspruch kann auch eine zuvor erteilte Einwilligung aufheben. Falls dies zur Unzeit geschieht, kann dies jedoch zur Schadenersatzpflicht der betreffenden Person führen. Die Fortsetzung der Bearbeitung kann indes gestützt auf einen anderen Rechtfertigungsgrund nach Art. 13 Abs. 1 DSG weiterhin möglich sein.[103]

6.4.3. Weitergabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen an Dritte

Art. 12 Abs. 2 lit. c DSG bestimmt, dass ohne Rechtfertigungsgrund besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten nicht bekanntgegeben werden dürfen.

6.4.4. Weitere zu beachtende Bestimmungen

Neben Art. 12 DSG sind des Weiteren insbesondere Vorgaben hinsichtlich der grenzüberschreitende Bekanntgabe (Art. 6 DSG), bei der Bearbeitung durch Dritte (Art. 10a Abs. 2 DSG), im Rahmen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen (bspw. Art. 4 Abs. 5, Art. 11a Abs. 3 lit. a oder Art. 14 DSG) sowie bei der Bearbeitung durch Bundesorgane (Art 16ff. DSG) und die Auskunftsrechte (Art. 8 DSG) zu berücksichtigen.

6.4.4.1. Grenzüberschreitender Datenbekanntgabe Art. 6 Abs. 1 DSG

Art. 6 Abs. 1 DSG verbietet die grenzüberschreitende Bekanntgabe von personenbezogenen Daten, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. Diese Norm soll sicherstellen, dass die Weitergabe von personenbezogenen Daten an einen Datenempfänger in einem Drittland nur unter der Bedingung eines angemessenen Datenschutzniveaus im Empfängerland erfolgt.[104] Bei dieser Vorschrift handelt es sich um eine besondere Rechtmässigkeitsvoraussetzung für den grenzüberschreitenden Datenverkehr, der kumulativ zu den allgemeinen Grundsätzen und Bestimmungen des DSG anzuwenden ist.[105] Der grenzüberschreitende Datenverkehr setzt voraus, dass Personendaten von dem territorialen Anwendungsbereichs eines Datenschutzgesetzes in denjenigen eines anderen übergehen und dort bearbeitet werden. Dies gilt auch für die Übertragung von Daten innerhalb eines multinationalen Unternehmens.[106] Die Beurteilung, ob ein Datenschutzgesetz eines Drittlandes einen angemessenen Schutz bietet, ist vom Versender der Personendaten von Fall zu Fall und für jede Bekanntgabe einzeln zu prüfen. Dabei sind die Umstände der Bekanntgabe zu berücksichtigen, insbesondere die Art der Daten, der Zweck der Bearbeitung, die einschlägigen Rechtsvorschriften des betreffenden Empfängerstaates sowie der Datenempfänger bzw. die Zugangsberechtigten.[107] Als Hilfestellung hat der EDÖB eine Liste derjenigen Staaten veröffentlicht, welche über eine Gesetzgebung verfügen, die einen angemessenen Datenschutz gewährleisten (Art. 7 VDSG). Sie ist zwar keine verbindliche Feststellung der

---

103 *Jöhri/Rosenthal* (Anm. 18), Art. 12 N. 29.
104 *Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter*, die Datenübermittlung ins Ausland kurz erklärt, S. 1.
105 *Jöhri/Rosenthal* (Anm. 5), Art. 6 N. 2.
106 *Maurer-Lambrou/Steiner*, in: Maurer-Lambrou/Vogt, Basler Kommentar zum Datenschutzgesetz, 2006, Art. 6 N. 14; *Jöhri/Rosenthal* (Anm. 18), Art. 6 N. 4.
107 *Belser/Epiney/Waldmann* (Anm. 85), § 10 N. 14.

Angemessenheit des Schutzniveaus einer ausländischen Gesetzgebung, stellt aber immerhin eine - von der betroffenen Person widerlegbare - Vermutung auf, dass ein angemessener Schutz gewährleistet ist.[108]

Art. 6 Abs. 2 DSG enthält die Ausnahmevorschrift zum Grundsatz von Art. 6 Abs. 1 DSG, die es erlaubt, Personendaten auch ohne die Gewährleistung eines angemessenen Datenschutzes im betreffenden Staat ins Ausland bekannt zu geben. Der Versender der Daten kann innerhalb des Ausnamekataloges die Mittel zur Sicherstellung der Personendaten im Ausland frei wählen.[109] Der Ausnahmekatalog ist abschliessend, so dass keine anderen Rechtfertigungsgründe möglich sind.[110] Die Rechtfertigung im Falle einer Verletzung von Art. 6 Abs. 1 DSG richtet sich somit nach Art. 6 Abs. 2 DSG, welche als Spezialnorm Art. 13 DSG vorgeht.[111] Nach Art. 6 Abs. 3 DSG trifft den Versender über gewisse Aspekte der Anwendung der Ausnahmebestimmungen eine Meldepflicht.

6.4.4.2. Auskunftsrechte (Art. 8 DSG) und ihre Einschränkungen (Art. 9 DSG)

Das Auskunftsrecht gibt Personen das Recht, auf Anfrage Auskunft über eine sie betreffende Datenbearbeitung zu erhalten. Gemäss Art. 8 Abs. 1 DSG darf jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Alle natürlichen und juristischen Personen sind demnach auskunftsberechtigt. Ein besonders schutzwürdiges Interesse muss dafür nicht nachgewiesen werden. Auskunftsverpflichtet ist immer der Inhaber der Datensammlung, unabhängig davon, ob die Bearbeitung durch diesen selbst oder durch einen Dritten erfolgt (Art. 8 Abs. 4 DSG). Die Auskunftspflicht trifft den Dritten bloss, wenn der Inhaber der Sammlung durch diesen nicht bekanntgegeben wird oder der Inhaber seinen Wohnsitz ausserhalb der Schweiz hat. Gegenstand der Auskunft ist gemäss Art. 8 Abs. 2 DSG zunächst einmal die Information, ob sich überhaupt Daten der betroffenen Person in der Datensammlung befinden. Werden tatsächlich Daten des Betroffenen bearbeitet, muss ihm über sämtliche Daten Auskunft erteilt werden, vorausgesetzt, es kann eine Verbindung zwischen ihm und den betreffenden Daten hergestellt werden (die Personendaten müssen den Auskunftsberechtigten betreffen). Der Auskunftsberechtigte ist zudem insbesondere über die Herkunft der Personendaten, den Zweck der Datenbearbeitung und gegebenenfalls über die gesetzliche Grundlage der Bearbeitung zu informieren. Des Weiteren beinhaltet die Auskunft auch die Nennung der Kategorien (bspw. Oberbegriffe wie Einkommen, Adresse oder Berufstätigkeit)[112] der bearbeiteten Daten, der an der Sammlung Beteiligten und der Datenempfänger. Das Ersuchen um Auskunft durch den Auskunftsberechtigten erfolgt grundsätzlich über ein schriftliches Gesuch an den Inhaber der Datensammlung, in dem Angaben zur Identität des Gesuchstellers und zu den betroffenen Daten gemacht werden. Die Auskunft durch den Inhaber der Datensammlung hat gemäss Art. 8 Abs. 5 DSG ebenfalls schriftlich, in Form eines Ausdrucks oder einer Fotokopie, unter gewissen Umständen auch auf elektronischem Weg oder mittels direkter Einsichtnahme vor Ort zu erfolgen. Die Auskunft muss vollständig und wahrheitsgetreu, sowie für den Auskunftsberechtigten grundsätzlich kostenfrei sein. Eine Verletzung des Auskunftsrechts durch Private wird gemäss Art. 34 Abs. 1 lit. a DSG auf Antrag mit einer Busse von bis zu CHF 10'000 bestraft. Auf das Auskunftsrecht kann nach Art. 8 Abs. 6 DSG im Voraus nicht rechtsgültig verzichtet werden; diesbezügliche Abreden sind somit nichtig.[113]

Einschränkungen des Auskunftsrechts sind in Art. 9 DSG vorgesehen. Demnach können Private und Bundesorgane das Auskunftsrecht verweigern, einschränken oder aufschieben, wenn dies von einem Gesetz im formellen Sinne vorgesehen ist oder wenn über-

108 *Jöhri/Rosenthal* (Anm. 18), Art. 6 N 30.
109 *Belser/Epiney/Waldmann* (Anm. 85), § 10 N. 14.
110 *Bundesrat* (Anm. 16), S. 2128f.
111 *Jöhri/Rosenthal* (Anm. 18), Art. 13 N. 2.
112 *Jöhri/Rosenthal* (Anm. 18), Art. 11a N. 35.
113 *Belser/Epiney/Waldmann* (Anm. 85), § 9 N. 42.

wiegende Interessen Dritter es erfordern. Bundesorgane können zudem Einschränkungen vornehmen, bei überwiegenden öffentlichen Interessen (vor allem innere oder äussere Sicherheit des Landes) sowie wenn die Auskunft den Zweck einer Strafuntersuchung oder eines anderen Untersuchungsverfahren in Frage stellt. Den Privaten ist das Recht vorbehalten, die Auskunft aufgrund überwiegender eigener Interessen einzuschränken, soweit sie die Personendaten nicht an Dritte weitergeben. Alle Einschränkungen der Auskunftsrechte erfordern eine Interessenabwägung und die Anwendung des Verhältnismässigkeitsprinzips.[114]

6.4.4.3. Bearbeitung durch Dritte

Die grundlegenden Bestimmungen, welche den Datenschutz bei einer Bearbeitung von Daten durch Dritte gewährleisten, befinden sich in Art. 10a DSG. Weitere Vorschriften zur Übertragung der Bearbeitung an Dritte finden sich zudem in Teilen einiger anderer Normen.

Art. 10a DSG findet Anwendung, wenn der Inhaber einer Datensammlung eine andere natürliche oder juristische Person mit der Bearbeitung von Personendaten beauftragt. Der bearbeitende Dritte wird dabei nicht zum Inhaber der Datensammlung, sondern bearbeitet die Daten ausschliesslich für die Zwecke und im Interesse des Auftraggebers.[115] Die Übertragung der Datenbearbeitung an einen Dritten durch Vereinbarung oder Gesetz ist gemäss Art. 10a Abs. 1 DSG nur möglich, wenn die Daten vom Dritten nur in der Art und Weise bearbeitet werden, wie es der Inhaber der Datensammlung selber tun dürfte (lit. a) und keine gesetzlichen oder vertraglichen Geheimhaltungspflichten eine Bearbeitung durch Dritte verbieten (lit. b). Den Inhaber der Datensammlung trifft eine Sorgfaltspflicht im Hinblick auf die Auswahl, die Instruktion und die Überwachung des Dritten. Speziell betont wird in Art. 10a Abs. 2 DSG die Pflicht des Auftraggebers, sich zu vergewissern, dass der Dritte die Datensicherheit gewährleistet.[116] Aus Art. 10a Abs. 1 lit a ergibt sich des Weiteren, dass der Dritte die allgemeinen Datenbearbeitungsgrundsätze (v.a. Art. 4 DSG) zu beachten hat. Sofern die Voraussetzungen aus Art. 10a DSG erfüllt sind, darf der Auftraggeber besonders schützenswerte Personendaten oder Persönlichkeitsprofile an den Dritten weitergeben, ohne eine Persönlichkeitsverletzung im Sinne von Art. 12 Abs. 2 lit. c DSG zu verursachen. Die Pflicht des privaten Inhabers einer Datensammlung, diese im Falle der Bekanntgabe an Dritte beim Datenschutzbeauftragten anzumelden (Art. 11a Abs. 3 lit. b), fällt mit einer korrekten Übertragung im Sinne von Art. 10a DSG weg.[117] Die Auskunftspflicht nach Art. 8 DSG verbleibt jedoch trotz Übertragung grundsätzlich beim Inhaber der Datensammlung. Der Dritte wird bloss auskunftspflichtig, wenn er den Inhaber der Datensammlung nicht bekannt gibt, oder dieser keinen Wohnsitz innerhalb der Schweiz hat (Art. 8 Abs. 4 DSG). Sind die Voraussetzungen für eine rechtmässige Übertragung der Datenbearbeitung an Dritte nach Art. 10a DSG nicht erfüllt, führt die Übermittlung der Daten zu einer Persönlichkeitsverletzung im Sinne von Art. 12 Abs. 1 DSG.[118] Die betroffene Person kann in diesem Fall gegen den Auftraggeber oder den Dritten Ansprüche gemäss Art. 15 DSG geltend machen, sofern der Auftraggeber bzw. der Dritte sich nicht auf die Rechtfertigungsgründe in Art. 13 DSG berufen kann. Dem Dritten steht das Rechtfertigungsprivileg aufgrund von Art. 10a Abs. 3 DSG zu. Dritte, welche von Bundesorganen beauftragt wurden, können sich über Art. 17 DSG rechtfertigen.[119] Der private Inhaber einer Datensammlung darf in keinem Fall Daten an Dritte weitergeben, wenn er die Auskunft gegenüber dem Betroffenen wegen überwiegender eigener Interessen verweigert (Art. 9 Abs. 4 DSG). Falls der Auftraggeber besonders schützenswerte Daten oder Persönlichkeitsprofile nicht vom Betroffenen selbst beschafft

114 *Belser/Epiney/Waldmann* (Anm. 85), § 9 N. 43ff.
115 *Belser/Epiney/Waldmann* (Anm. 85), § 10 N. 39.
116 *Belser/Epiney/Waldmann* (Anm. 85), § 10 N. 54.
117 *Belser/Epiney/Waldmann* (Anm. 85), § 10 N. 51.
118 *Rampini* (Anm. 82), Art. 14 N. 4.
119 *Belser/Epiney/Waldmann* (Anm. 85), § 10 N. 57.

hat, muss er diesen, sofern keine Speicherung der Daten erfolgt ist, bei Bekanntgabe an den Dritten über die Datenbeschaffung informieren (Art. 14 Abs. 3 DSG).

6.4.4.4. Besonders schützenswerte Personendaten und Persönlichkeitsprofile

Strengere Vorschriften bestehen im Umgang mit besonders schützenswerten Personendaten und Persönlichkeitsprofilen. Zum einen bedarf ihre Bearbeitung nach Art. 4 Abs. 5 DSG die ausdrückliche Zustimmung der betroffenen Person. Die Ausdrücklichkeit bezieht sich dabei auf den Inhalt und nicht auf die Art und Weise der Bearbeitung, so dass sich die Tatsache der Datenbearbeitung nicht bloss implizit ergeben darf. Dies bedeutet aber nicht, dass die Einwilligung selbst ausdrücklich im formellen Sinne zu erfolgen hat.[120] Sie kann durchaus auch konkludent oder gar stillschweigend erfolgen.[121] Sammelt eine Privatperson besonders schützenswerte Personendaten und Persönlichkeitsprofile, ist sie gemäss Art. 11a Abs. 3 lit. a DSG zur Anmeldung der Sammlung beim EDÖB verpflichtet. Von der Anmeldepflicht erfasst werden Datensammlungen, die solche Daten enthalten bzw. bei denen vorgesehen ist, dass sie solche Daten enthalten sollen. Datensammlungen, die lediglich im Zusammenhang oder aus Anlass der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen entstehen oder benutzt werden, werden dagegen nicht erfasst. Weiter muss die Bearbeitung dieser Daten regelmässig vorgesehen sein. Regelmässig bedeutet dabei, dass die Bearbeitung der besonders schützenswerten Personendaten oder Persönlichkeitsprofilen nach einer bestimmten Ordnung wiederkehrend erfolgt.[122] Ob dies der Fall ist, muss aus der Sicht des Inhabers der Datensammlung beurteilt werden, denn die Pflicht zur Anmeldung der Datensammlung entsteht gemäss Art. 11a Abs. 4 DSG bereits vor ihrer Eröffnung. Die Verletzung der Anmeldepflicht wird gemäss Art. 34 Abs. 2 lit. a DSG mit Busse bestraft.

Art. 12 Abs. 2 lit. c DSG stellt die nicht widerlegbare Vermutung auf, dass die Bekanntgabe von Persönlichkeitsprofilen und besonders schützenswerten Personendaten ohne Rechtfertigungsgrund an Dritte eine Persönlichkeitsverletzung darstellt. Als Rechtfertigung gelten die Gründe aus Art. 13 DSG wie beispielsweise eine Einwilligung des Betroffenen oder das überwiegende Eigeninteresse des Bearbeiters.

Eine weitere Vorschrift betreffend besonders schützenswerten Personendaten und Persönlichkeitsprofilen ist in Art. 14 DSG enthalten. Dieser statuiert eine besondere Informationspflicht bei der Datenbeschaffung. Das Wort Beschaffung impliziert, dass nicht jedes Beschaffen von der Pflicht erfasst ist, sondern dass eine gewisse Systematik vorausgesetzt wird. Weiter muss die Bearbeitung der Persönlichkeitsprofile oder der besonders schützenswerten Personendaten bezweckt werden (vgl. Art. 14 Abs. 2 lit. c DSG). Die Informationspflicht trifft den Inhaber der Datensammlungen und gilt auch dann, wenn die Informationen von Dritten beschafft werden. Die Information an den Betroffenen muss aktiv und ausdrücklich erfolgen.[123] Es genügt jedoch, wenn sie für die betroffene Person als solche erkennbar und in zumutbarer Weise zugänglich ist. Werden die Daten direkt bei dem Betroffenen erhoben, hat die Information in zeitlicher Hinsicht vor, während oder unmittelbar nach der ersten Datenerhebung zu erfolgen. Werden die Daten bei einem Dritten beschafft, kommt Art. 14 Abs. 3 DSG zur Anwendung. Der zwingende Inhalt der Informationspflicht richtet sich nach Abs. 2. der genannten Bestimmung Wird bezüglich bereits beschaffter Daten und nach erfolgter Information der Bearbeitungszweck geändert oder erweitert, oder kommt es zu einer nicht vorgesehenen und daher nicht dargelegten Datenbekanntgabe, ist nach Art. 14 DSG keine neue Information erforderlich, da die Pflicht lediglich an die Datenbeschaffung knüpft. Ausnahmen von der Pflicht sind in

120 *Jöhri/Rosenthal* (Anm. 18), Art. 4 N. 83.
121 Vgl. BGE 98 IV 218.
122 *Jöhri/Rosenthal* (Anm. 18), Art. 11a. N 35ff.
123 *Jöhri/Rosenthal* (Anm. 18), Art. 7a N. 13.

Abs. 4 enthalten. Die Verletzung der Informationspflicht wird gemäss Art. 34 Abs. 1 DSG mit Busse bestraft.

Besonders schützenswerte Personendaten und Persönlichkeitsprofile dürfen von den Organen des Bundes gemäss Art. 17 Abs. 2 DSG nur bearbeitet werden, wenn entweder ein formelles Gesetz dies ausdrücklich vorsieht oder einer der im Datenschutzgesetz abschliessend aufgezählten Gründe gegeben ist. Der Grundsatz der gesetzlichen Grundlage gilt für das Beschaffen, das Verwenden, Aufbewahren sowie das Bekanntgeben von Personendaten durch Bundesorgane.[124] Lässt sich eine entsprechende Legitimation nicht direkt aus dem DSG selbst herleiten, ist eine bereichsspezifische bzw. spezialgesetzliche Rechtsgrundlage erforderlich. Soweit aber nicht eine abschliessende, spezialgesetzliche Vorschrift vorliegt, müssen die Bundesorgane immer die allgemeinen Bestimmungen in Art. 4ff. DSG beachten. Schliesslich sind die Grundsätze und Prinzipien des DSG auch bei der Auslegung der bereichsspezifischen Norm zu berücksichtigen.[125] Inhaltlich müssen mindestens der Bearbeitungszweck, die an der Datenbearbeitung beteiligten Datenbearbeiter und Datenempfänger, allenfalls die dabei verwendeten Mittel und das Ausmass der Datenbearbeitung im Gesetz geregelt sein. Es gilt zu berücksichtigen, dass zusätzlich zu einer gesetzlichen Grundlage alle weiteren Voraussetzungen aus Art. 36 BV kumulativ erfüllt sein müssen, wenn durch das Bearbeiten der besonders schutzwürdigen Personendaten oder Persönlichkeitsprofilen in ein Grundrecht des Betroffenen wie bspw. der Schutz der Privatsphäre sowie das Grundrecht des Art. 10 Abs. 2 BV eingegriffen wird.

6.4.4.5. Bearbeitung durch Bundesorgane

Die Vorschriften, die von Bundesorganen bei der Datenbearbeitung zu beachten sind, finden sich an zwei Stellen des Datenschutzgesetzes: Es gelten einerseits die allgemeinen Bearbeitungsgrundsätze aus Art. 4-11a DSG, andererseits bestehen in Art. 16-25bis DSG besondere (strengere) Vorschriften für Bundesorgane.

Zu den Bundesorganen im Sinne des Gesetzes gehören gemäss Art. 3 lit. h DSG Behörden und Dienststellen des Bundes sowie Personen, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind. Bundesorgane, die privatrechtlich handeln, unterstehen gemäss Art. 23 DSG den Bestimmungen für Privatpersonen (Art. 12-15 DSG). Grundsätzlich ist gemäss Art. 16 DSG jeweils das Bundesorgan für den Datenschutz verantwortlich, welches die Daten bearbeitet oder bearbeiten lässt.

Bundesorgane müssen sich beim Umgang mit Daten an das verfassungsmässige Legalitätsprinzip halten. Organe des Bundes dürfen Daten nur bearbeiten (Art. 17 Abs. 1 DSG) und/oder bekanntgeben (Art. 19 DSG), wenn dafür eine gesetzliche Grundlage besteht. Die rechtliche Grundlage muss einen angemessenen Grad an Bestimmtheit aufweisen; d.h. der Zweck, die beteiligten Organe sowie das Ausmass der Bearbeitung müssen darin mindestens festgelegt sein.[126] Für die Bearbeitung besonders schützenswerter Personendaten und von Persönlichkeitsprofilen ist gemäss Art. 17 Abs. 2 DSG grundsätzlich eine ausdrückliche Grundlage in einem Gesetz im formellen Sinn erforderlich. Art. 17 Abs. 2 lit. a-c DSG enthält eine Aufzählung von Ausnahmen, welche sich nicht nur auf das Erfordernis einer Grundlage im formellen Sinn beziehen, sondern eine Datenbearbeitung von besonders schützenswerte Personendaten sowie Persönlichkeitsprofilen ohne gesetzliche Grundlage rechtfertigen.[127] Des Weiteren gelten erleichterte Anforderungen bei der Bearbeitung von Personendaten für nicht personenbezogene Zwecke (Art. 22 DSG). Neben dem Legalitätsprinzip sind die Bundesorgane beim Umgang mit Daten auch immer an die Prinzipien des öffentlichen Interesses sowie der Verhältnismässigkeit

[124] *Jöhri/Rosenthal* (Anm. 18), Art. 17 N. 2.
[125] BGE 126 II 126, E. 5b und 5c.
[126] *Belser/Epiney/Waldmann* (Anm. 85), § 12 N. 45.
[127] *Jöhri/Rosenthal* (Anm. 18), Art. 17 N. 75.

gebunden.[128] Bei der Beschaffung von Daten haben die Bundesorgane zudem immer die Informationspflicht nach Art. 18a DSG zu beachten. Im Gegensatz zu Privaten müssen die Bundesorgane auch sämtliche Datensammlungen beim Datenschutzbeauftragten registrieren (Art. 11a Abs. 2 DSG).

Das Recht auf Auskunft der betroffenen Personen im Sinne von Art. 8 DSG besteht auch gegenüber Bundesorganen. Aus Art. 20 DSG ergibt sich ausserdem ein Anspruch der Betroffenen auf Sperrung einer Datenbekanntgabe durch Bundesorgane. Weitere Ansprüche von Betroffenen, vor allem auf Löschung oder Unterlassung der Bearbeitung von Personendaten, sind in Art. 25 DSG geregelt.

6.4.5. Rechtfertigungsgründe (Art. 12 Abs. 3 und Art. 13 DSG)

Art. 13 DSG bestimmt, wann eine Persönlichkeitsverletzung widerrechtlich und wann sie gerechtfertigt ist. Gemäss Art. 13 Abs. 1 DSG ist eine Verletzung der Persönlichkeit widerrechtlich, "*wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.*" Aufgrund des Wortlautes von 12 Abs. 2 Bst. a DSG war es umstritten, ob eine Verletzung der Bearbeitungsgrundsätze den Rechtfertigungsgründen von Art. 13 DSG unterliege. Das Bundesgericht entschied, dass "*eine Rechtfertigung der Bearbeitung von Personendaten entgegen der Grundsätze von Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG zwar nicht generell ausgeschlossen ist, dass Rechtfertigungsgründe im konkreten Fall aber nur mit grosser Zurückhaltung bejaht werden können.*"[129] Zu den einzelnen Rechtfertigungsgründen.

6.4.5.1. Einwilligung

Wer Personendaten bearbeitet, braucht hierfür keine Einwilligung der Betroffenen. Eine Einwilligung ist nur dann erforderlich, wenn sie der Rechtfertigung einer persönlichkeitsverletzenden Bearbeitung dient oder sich das Erfordernis aus anderen Rechtsgründen ergibt. Dies ergibt sich etwa aus Art. 12 Abs. 2 lit. b DSG, welcher besagt, dass eine betroffene Person die Bearbeitung bzw. die weitere Bearbeitung ihrer Personendaten untersagen kann. Tut sie dies, stellt jede weitere Bearbeitung per se eine Persönlichkeitsverletzung dar und ist damit widerrechtlich, sofern und soweit keiner der Rechtfertigungsgründe gemäss Art. 13 Abs. 1 DSG vorliegt.[130] Die Bestimmung bringt zum Ausdruck, dass im Bereich der Bearbeitung von Personendaten durch private Personen das opt-out-Prinzip gilt: Die Bearbeitung von Personendaten ist somit grundsätzlich auch ohne Einwilligung der betroffenen Person zulässig, es ist also kein opt-in erforderlich.[131] Die Voraussetzung einer gültigen Einwilligung sind in Art. 4 Abs. 5 zu finden. Sie setzt insbesondere voraus, dass eine angemessene Information bezüglich der Datenbearbeitung vorliegt und dass die Einwilligung freiwillig erfolgt.[132] Das Erfordernis einer angemessenen Information hat zum Ziel, dass die betroffene Person ihre Einwilligung in Kenntnis der Sachlage gibt, d.h. erst entscheiden muss, wenn sie sich ein Bild über die möglichen (auch negativen) Folgen ihrer Einwilligung machen konnte.[133] Kritisch ist hinsichtlich der Freiwilligkeit der Einwilligung etwa, wenn die betroffen Person in einem Abhängigkeitsverhältnis zum Datenbearbeiter steht.[134] Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss hingegen nach Art. 4 Abs. 5 Satz 2 DSG die Einwilligung immer ausdrücklich erfolgen. Ausdrücklich ist eine Einwilli-

128 *Belser/Epiney/Waldmann* (Anm. 85), § 12 N. 59f.
129 BGE 136 II 508 E. 5.2.4.
130 *Jöhri/Rosenthal* (Anm. 18), Art. 4 N. 66; *Jöhri/Rosenthal* (Anm. 18), Art. 12 N. 24.
131 *Jöhri/Rosenthal* (Anm. 18), Art. 4 N. 66; *Jöhri/Rosenthal* (Anm. 18), Art. 12 N. 25.
132 *Jöhri/Rosenthal* (Anm. 18), Art. 12 N. 68.
133 *Jöhri/Rosenthal* (Anm. 18), Art. 4 N. 72.
134 *Rampini*, (Anm. 82), Art. 13 N. 7.

gung dann, wenn sie sich ausdrücklich auf die Bearbeitung dieser Daten bezieht.[135] Im Übrigen kann die Einwilligung ausdrücklich oder konkludent erfolgen. Im letzteren Fall muss sich die Einwilligung aus den Umständen klar ergeben.[136]

Die konkludente Einwilligung ist insbesondere bei freiwillig eingegangenen Vertragsverhältnissen von Bedeutung, da dort i.d.R. nach Treu Glauben davon ausgegangen werden kann, dass die Zustimmung für die zur Vertragserfüllung notwendige Datenbearbeitung implizit erfolgt ist. Im Rahmen einer freiwilligen Teilnahme an einem Rollout oder einem Gebäudeeffizienzprogramm muss die der Einwilligung zugrunde liegende Willenserklärung somit nicht ausdrücklich geäussert werden. Die Einwilligungserklärung kann unter Umständen auch konkludent oder sogar stillschweigend erfolgen.

6.4.5.2. Überwiegendes privates oder öffentliches Interesse

Der Rechtfertigungsgrund des überwiegenden privaten Interesses erfasst einerseits die Interessen des Datenbearbeiters und andererseits die Interessen beliebiger Drittpersonen, sofern diese berechtigt sind. Die Interessen des Inhabers des Datenbearbeiters umfassen sowohl jene des Inhabers der Datensammlung als auch jene weiterer Datenbearbeiter. Zunächst werden nur die privaten Interessen an der konkret zur Diskussion stehenden Datenbearbeitung berücksichtigt. Dabei ist sowohl das Interesse am Zweck als auch an den Mitteln der Datenbearbeitung zu ermitteln. Die Mittel der Datenbearbeitung umfassen vor allem die Art und Weise der Datenbearbeitung sowie die Art und Auswahl der Personendaten.[137] Jedoch vermag nicht jedes private Interesse an der Datenbearbeitung eine Persönlichkeitsverletzung zu rechtfertigen, vielmehr muss es berechtigt d.h. schützenswert sein. Schützenswert gelten mangels einer klaren gesetzlichen Definition all jene Interessen, die vor dem Hintergrund der in Schweiz geltenden Werteordnung anerkennungswürdig (m.a.W. legitim) sind.[138] Ein legitimes Interesse stellt bspw. auch das Gewinnstreben von Unternehmen dar.[139] Die berechtigten Interessen Privater sind dann mit den berechtigten Interessen der betroffenen Person abzuwägen, wobei mit dem Nachweis einer Persönlichkeitsverletzung immer auch ein schützenswertes Interesse nachgewiesen werden muss. Die Abwägung der sich widersprechenden Interessen hat unter der Berücksichtigung aller Umstände des Einzelfalls durch eine Wertung der auf dem Spiel stehenden Güter stattzufinden.[140] Allgemein ausgedrückt liegt ein überwiegendes privates Interesse dann vor, wenn die aus der Datenbearbeitung resultierende Persönlichkeitsverletzung unter der Berücksichtigung aller Umstände das richtige Mittel für den richtigen Zweck ist.[141] Diese wertende Abwägung der Interessen im Einzelfall ist schwierig und insbesondere schwer vorhersehbar.[142] Hinzu kommt, dass die massgebliche Wertung, d.h. die verbindliche Feststellung, ob ein privates Interesse im konkreten Fall überwiegt, immer erst nachträglich durch den Richter vorgenommen wird. Ein Datenbearbeiter sollte sich deshalb nur auf den Rechtfertigungsgrund des überwiegenden privaten Interesses verlassen, wenn keine Möglichkeit besteht, eine Einwilligung einzuholen.

Als Rechtfertigungsgrund für eine Persönlichkeitsverletzung kommt gemäss Art. 13 Abs. 1 DSG zudem ein überwiegendes öffentliches Interesse in Frage. Bei dem öffentlichen Interesse handelt es sich um einen unbestimmten Rechtsbegriff, bei dem der rechtsanwendenden Behörde dementsprechend ein Interpretationsspielraum zusteht. Es gilt dabei zu berücksichtigen, dass der Begriff des öffentlichen Interesses dynamisch ist und sich in

---

135 *Jöhri/Rosenthal* (Anm. 18), Art. 4 N. 83; A.M. wohl *Bundesrat*, (Anm. 16), S. 2127. Vgl. hierzu auch Kap. 6.4.4.4 Besonders schützenswerte Personendaten und Persönlichkeitsprofile.

136 *Jöhri/Rosenthal* (Anm. 18), Art. 4 N 79l

137 *Jöhri/Rosenthal* (Anm. 18), Art. 13 N. 8.

138 *Rampini*, (Anm. 82), Art. 13 N. 22; *Jöhri/Rosenthal* (Anm. 18), Art. 13 N. 10.

139 BGE 138 II 346, E. 10.4.

140 *Rampini*, (Anm. 82), Art. 13 N. 24; *Jöhri/Rosenthal* (Anm. 18), Art.13 N. 12.

141 BGE 122 III 457; *Jöhri/Rosenthal* (Anm. 18), Art. 13 N. 16.

142 *Jöhri/Rosenthal* (Anm. 18), Art. 13 N. 6.

zeitlicher und örtlicher Hinsicht wandeln kann. Die Abwägung der öffentlichen Interessen mit dem Interesse der betroffenen Person findet nach demselben Prinzip wie die Abwägung mit berechtigten privaten Interessen statt[143]

Gemäss Botschaft zum ersten Massnahmenpaket der Energiestrategie 2050 "*sollen unter anderem der Endenergie- und der Stromverbrauch reduziert, der Anteil der erneuerbaren Energien erhöht und die energiebedingten CO2-Emissionen gesenkt werden. Dies, ohne die bisher hohe Versorgungssicherheit und die preiswerte Energieversorgung in der Schweiz zu gefährden.*"[144] Es stellt sich die Frage, ob die mit der Energiestrategie 2050 verfolgten öffentlichen Interesse Smart Meter bzw. die Datenverwendung im Smart Grid und den Gebrauch der Daten gemäss den Use-Cases rechtfertigen kann. Dies ist zu bezweifeln, da das Massnahmenpaket der Energiestrategie 2050 einen programmatischen und keinen direkt verbindlichen Charakter hat. Zudem ist aufgrund der Tragweite des potentiellen Eingriffs in die Persönlichkeitsrechte der betroffenen Personen sowie zum Schutz der Rechtssicherheit eine gesetzliche Grundlage als Rechtfertigungsgrund vorzuziehen (vgl. sogleich).

6.4.5.3. Durch Gesetz

Auf das Gesetz als Rechtfertigungsgrund kann sich berufen, wer eine Datenbearbeitung durchführt, deren Persönlichkeitsverletzung eine Gesetzesvorschrift oder eine Amts- oder Berufspflicht gebietet, für erlaubt erklärt oder stillschweigend voraussetzt.[145] Zur Rechtfertigung einer Persönlichkeitsverletzung genügt es demnach nicht, wenn das Gesetz die Bearbeitung von Personendaten an sich vorsieht. Vielmehr muss jeweils eine spezifische, mit der konkreten Datenbearbeitung verbundene Persönlichkeitsverletzung durch das Gesetz gerechtfertigt werden. Zudem greift der Rechtfertigungsgrund nur für die im Gesetz vorgesehenen Zwecke. Wie weit eine bestimmte Rechtsnorm eine Persönlichkeitsverletzung im Zusammenhang mit einer Bearbeitung von Personendaten rechtfertigt, muss durch Auslegung der betreffenden Norm ermittelt werden. So vermag nicht jede gesetzliche Pflicht, deren Erfüllung auch eine Datenbearbeitung mit sich bringt, automatisch allfällige Persönlichkeitsverletzungen zu rechtfertigen, insbesondere dann nicht, wenn die Persönlichkeitsverletzung zwar im Rahmen der Pflichterfüllung erfolgt, die Pflichterfüllung aber ohne Weiteres auch auf eine andere Weise möglich ist, welche die Persönlichkeit der betroffenen Personen nicht verletzt.[146] Grundsätzlich kann der Rechtfertigungsgrund des Gesetzes gestützt auf jede Norm des schweizerischen Rechts angerufen werden, unabhängig davon, ob es sich um Bundesrecht, kantonales oder kommunales Recht handelt. Ausländische Rechtsvorschriften stellen hingegen keinen gesetzlichen Rechtfertigungsgrund dar. Regelmässig handelt es sich jedoch bei der Befolgung ausländischer Gesetzesbestimmungen um ein berechtigtes (privates) Interesse des Datenbearbeiters oder gegebenenfalls ein öffentliches Interesse. Auch anerkannte Vorgaben, Standards und Empfehlungen von Selbstregulierungsorganisationen, Normierungsgremien oder andere staatlichen oder privaten Organisationen und Institutionen stellen keinen gesetzlichen Rechtfertigungsgrund dar, sofern sie nicht als Teil des schweizerischen Rechts gelten. Die Einhaltung dieser Vorgaben, Standards und Empfehlungen kann aber zum einen als überwiegendes privates oder öffentliches Interesse eine Persönlichkeitsverletzung rechtfertigen und zum anderen für die Auslegung der Normen des Schweizer Rechts relevant sein.[147]

Art. 8 StromVV stellt für bestimmte Anwendungen im Messwesen und für Informationsprozesse eine gesetzliche Grundlage dar. So besagt etwa Art. 8 Abs. 3 StromVV, dass die Netzbetreiber den Beteiligten die für den Netzbetrieb, das Bilanzmanagement, die

143 *Jöhri/Rosenthal* (Anm. 18), Art. 13 N. 21.
144 *Bundesrat* (Anm. 76), S. 5.
145 *Rampini* (Anm. 82), Art. 13 N. 15; *Jöhri/Rosenthal* (Anm. 18), Art. 13 N. 24.
146 *Jöhri/Rosenthal* (Anm. 18), Art. 13 N. 27.
147 *Jöhri/Rosenthal* (Anm. 18), Art. 13 N. 32.

Energielieferung, die Anlastung der Kosten, die Berechnung der Netznutzungsentgelte und die Abrechnungsprozesse notwendigen Messdaten und Informationen zur Verfügung stellen. Art. 8 Abs. 4 StromVV hält fest, dass die Netzbetreiber den Verantwortlichen von Bilanzgruppen sowie anderen Beteiligten im Einverständnis mit den betroffenen Endverbrauchern oder Erzeugern auf Begehren und gegen eine kostendeckende Abgeltung zusätzliche Daten und Informationen liefern. Es ist jedoch fraglich, ob Art. 8 StromVV und die darauf basierenden Branchendokumente[148] auch kurze Messintervalle erfassen, da bspw. für die Rechnungsstellung und den Netzbetrieb solche Daten nicht ohne weiteres notwendig sind. Auch der Bundesrat geht wohl davon aus, dass Art. 8 StromVV keine genügende Grundlage für die zwingende Einführung von intelligenten Messsystemen darstellt. Entsprechend schlägt der Bundesrat eine Delegationsnorm in Art. 17a E-StromVG vor, wonach er Vorgaben zur Einführung von intelligenten Messsystemen bei den Endverbraucherinnen und Endverbrauchern machen kann.[149]

In diesem Zusammenhang sind die Vorschriften zum informationellen Unbundling zu beachten. Gemäss Art. 10 Abs. 2 StromVG dürfen wirtschaftlich sensible Informationen, die aus dem Betrieb der Elektrizitätsnetze gewonnen werden, nicht für andere Tätigkeitsbereiche genutzt werden. Diese Vorschrift will verhindern, dass sich ein Netzbetreiber gegenüber potenziellen Konkurrenten einen Marktvorteil aus den Kenntnissen des Netzbetriebs verschafft[150]. Dies wäre bei einer kundenspezifischen Auswertung der Verbrauchsdaten und bei einer entsprechenden Ausrichtung der Dienstleistungen des Netzbetreibers der Fall. Sollten auch Netzbetreiber Dienstleistungen im Zusammenhang mit Smart Grid anbieten können, müssten die Unbundlingvorschriften für solche Fälle gelockert werden. Die angestrebte Kompatibilität mit dem europäischen Recht dürfte einer solchen Lockerung enge Grenzen setzen.

6.4.6. Folgen einer widerrechtlichen Persönlichkeitsverletzung

Die Konsequenzen einer widerrechtlichen Persönlichkeitsverletzung können zivilrechtlicher, öffentlich-rechtlicher und strafrechtlicher Natur sein. So kann, wer in seiner Persönlichkeit widerrechtlich verletzt worden ist, gestützt auf Art. 15 DSG zivilrechtliche Ansprüche (Schadenersatz, Anspruch auf Gewinnherausgabe, Genugtuung, Unterlassungsansprüche usw.) gegen jede Person geltend machen, die an der widerrechtlichen Persönlichkeitsverletzung mitgewirkt hat. Nach schweizerischem Recht kann somit auch der blosse Bearbeiter einer Datensammlung, also nicht nur der Inhaber der Datensammlung, für die Verletzung von Bearbeitungsgrundsätzen beklagt werden. Konsequenzen öffentlich-rechtlicher Art sind insbesondere im Zusammenhang mit dem EDÖB denkbar, welcher etwa die Anpassung oder Einstellung einer Datenbearbeitung empfehlen und seine Empfehlung u.U. veröffentlichen kann (Art. 29 Abs. 4 DSG; Art. 30 Abs. 2 DSG). Wird die Empfehlung nicht befolgt, kann der EDÖB diese dem Bundesverwaltungsgericht vorlegen und eine Vollstreckung verlangen (Art. 29 DSG). Strafrechtliche Konsequenzen finden sich insbesondere in Art. 179^{novies} StGB, welcher das unbefugte Beschaffen von Personendaten unter Strafe stellt, in Art. 162 StGB, welcher die Verletzung von Fabrikations- und Geschäftsgeheimnissen für strafbar erklärt, in Art. 50 FMG[151], welcher das fernmelderechtliche Verbot des unbefugten Verwendens von nichtöffentlichen Informationen statuiert sowie in Art. 34 DSG, welcher die Verletzung bestimmter sich aus dem DSG ergebenden Pflichten unter Strafe stellt und in Art. 35 DSG, welcher die Verletzung der beruflichen Schweigepflicht mit Strafe bedroht.[152]

---

148 So bspw. *Verband Schweizerischer Elektrizitätsunternehmen*, Branchenempfehlung Strommarkt Schweiz, Metering Code Schweiz, 2012, abrufbar unter: <http://www.strom.ch/uploads/media/MC-CH_2012_D_01.pdf>.

149 *Bundesrat* (Anm. 76), 75f, 157f.

150 Vgl. *Bundesrat*, Botschaft zur Änderung des Elektrizitätsgesetzes (EleG) und zum Bundesgesetz über die Stromversorgung (StromVG) vom 3. Dezember 2004, BBl 2005 1611, S. 1649.

151 Fernmeldegesetz vom 30. April 1997 (FMG), SR 784.10.

152 *Jöhri/Rosenthal* (Anm. 18), Art. 12 N. 9ff.

6.4.7. Beispiel anhand des Use Cases 1

Das im Use Case 1 installierte Smart Meter-Gerät beim Prosumer liefert die Meterdaten an den Energiedatenmanager, welcher diese Daten anschliessend an Lieferanten, den Verteilnetzbetreiber und weitere Marktteilnehmer sendet. Dabei werden nun folgende Annahmen getroffen: Der Verteilnetzbetreiber hat den Smart Meter beim Kunden eingebaut und bleibt dabei Eigentümer des Gerätes; der Kunde besitzt daneben vertragliche Vereinbarungen mit dem Energiedatenmanager und dem Lieferanten; der Energiedatenmanager betreibt zusammen mit dem Verteilnetzbetreiber eine Datensammlung, wobei beide über den Zweck und den Inhalt der Sammlung zusammen bestimmen; schliesslich werden die Daten als Personendaten an den Lieferanten und anonymisiert an die übrigen Marktteilnehmer gesendet.

Die Rechtslage würde sich in diesem Fall wie folgt präsentieren: Bearbeiter der Personendaten i.S.d. DSG sind der Verteilnetzbetreiber, der Energiedatenmanager und der Lieferant. Sie haben die in Kapiteln 6.2 – 6.4 besprochenen gesetzlichen Vorgaben zu wahren. So muss bspw. der Zweck der Datensammlung bei der Beschaffung angegeben bzw. aus den Umständen ersichtlich oder gesetzlich vorgesehen sein (Art. 4 Abs. 3 DSG), wofür also der Energiedatenmanager die Daten bearbeitet, muss ersichtlich sein für den Kunden. Auch sind etwaige unrichtige Daten zu korrigieren (Art. 5 DSG) und die Auskunftsrechte zu gewähren (Art. 8f. DSG). Zusätzlich Inhaber einer Datensammlung sind der Energiedatenmanager und der Verteilnetzbetreiber zusammen, weshalb ihnen zusätzliche Sonderpflichten zukommen. Sie haben etwa die Informationspflicht bei der Beschaffung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen (Art. 14 DSG), Pflichten bezüglich der grenzüberschreitenden Bekanntgabe von Personendaten (DSG 6 Abs. 3), die Auskunftspflicht (Art. 8 DSG), die Anmeldepflicht der Datensammlung (Art. 11a DSG), die Pflicht zur Beachtung besonderer Massnahmen im Bereich der Datensicherheit (Art. 7 DSG i.V.m. Art. 9 VDSG.), die Pflicht, unter Umständen ein Bearbeitungsreglement zu führen (Art. 11 und 21 VDSG) und die Pflicht, im Rahmen einer Bekanntgabe an einen Dritten diesen über die Aktualität und Zuverlässigkeit der Daten zu informieren (Art. 12 VDSG).[153] Da die übrigen Marktteilnehmer anonymisierte und damit keine personenbezogenen Daten erhalten, fallen sie nicht in den Anwendungsbereich des DSG. Die eigentliche Herrschaft über die Daten (Auskunfts-, Löschungs-, Berichtigungsrechte usw.) verbleibt dagegen weiterhin beim Prosumer, dessen Rechte indes durch die Rechtfertigungsgründe in Art. 13 DSG äusserst weitreichend eingeschränkt, ja u.U. gar ausgeschlossen werden können. Würde also zum Beispiel im Rahmen einer gesetzlichen Einführung von Smart Metern eine Bestimmung erlassen, welche festlegt, dass die von Smart Metern gesammelten Daten für Prognosedaten verwendet werden dürfen, könnten betroffene Haushalte oder Unternehmen die Verwendung ihrer Daten für Prognosen nicht mit einer Berufung auf das DSG verhindern, da ein gesetzlicher Rechtfertigungsgrund für die Bearbeitung gemäss Art. 13 DSG vorliegen würde.

6.5. Länderberichte Smart Metering

6.5.1. Österreich

In Österreich ist eine umfassende, schrittweise Einführung der Smart Meter bis Ende 2019 vorgesehen: Bis Ende 2015 sollen mindestens 10%, bis Ende 2017 mindestens 70% und bis Ende 2019 im Rahmen der technischen Machbarkeit mindestens 95% der ans Netz angeschlossenen Zählpunkte Smart Meter sein.

[153] *Jöhri/Rosenthal* (Anm. 18), Art. 3 N. 105.

Zunächst war in der Regierungsvorlage zum Elektrizitätswirtschafts- und Organisationsgesetz (ElWOG) 2010 die flächendeckende, verpflichtende Einführung von Smart Metern vorgesehen. Nach eindringlichen Protesten von verschiedenen Seiten (u.a. Mietervereinigung und Datenschutzrat) hat das Parlament Anfang Juli 2013 einen Abänderungsantrag angenommen, welcher, neben anderen Verbesserungen im Bereich Datenschutz, eine sogenannte opt-out Möglichkeit für Endnutzer vorsieht. Der Wunsch eines Endverbrauchers, kein intelligentes Messgerät zu erhalten, muss demnach neu vom Netzbetreiber berücksichtigt werden (§ 83 Abs. 1 ElWOG). Das Ziel, dass bis Ende 2019 mindestens 95% der ans Netz angeschlossenen Zählpunkte Smart Meter sind, wird trotz der Abschaffung der zwangsweisen Installation von intelligenten Messgeräten beibehalten.

Die Geschehnisse in Österreich zeigen, dass die zwangsmässige Einführung von Intelligenten Messgeräten auf grosse Gegenwehr aus der Bevölkerung stossen kann, welche unter Umständen eine Gefahr für das ganze Smart Meter-Projekt bedeutet. Es empfiehlt sich, die Öffentlichkeit bereits einige Zeit vor der Einführung transparent und umfassend über die Chancen und Gefahren von Intelligenten Messgeräten zu informieren, um eine breite Abstützung in der Bevölkerung zu erreichen.

6.5.1.1. Qualifizierung von Smart Meter-Daten

Die Gesetze und Verordnungen, welche für intelligente Messgeräte relevant sind, enthalten keine ausdrückliche Qualifizierung der Smart Meter-Daten. Das Elektrizitätswirtschafts- und Organisationsgesetz (ElWOG) verweist in § 83 Abs. 2 darauf, dass der Betrieb von intelligenten Messgeräten den "*datenschutzrechtlichen Bestimmungen sowie dem anerkannten Stand der Technik zu entsprechen*" hat. In § 128 Abs. 2 des Gaswirtschaftsgesetzes (GWG) findet sich dieselbe Bestimmung. Ein Anhaltspunkt zur Qualifizierung der Daten kann in § 84a Abs. 1 ElWOG erblickt werden, wonach die Auslesung und Verwendung von Viertelstundenwerten nur mit ausdrücklicher Zustimmung des Endverbrauchers erlaubt sind. Im GWG befindet sich dieselbe Regelung bezüglich Stundenwerte. Diese Bestimmungen könnten darauf hinweisen, dass zumindest Viertelstundenwerte bei Elektrizität resp. Stundenwerte beim Gas als personenbezogene Daten angesehen werden und somit eine Zustimmung im Sinne von § 1 Abs. 2 Datenschutzgesetz (ÖDSG) erforderlich ist.

Der österreichische Datenschutzrat qualifiziert die Einführung von intelligenten Messgeräten als klaren Eingriff in das Grundrecht auf Datenschutz nach § 1 ÖDSG. Diese Auffassung wird damit begründet, dass ein Smart Meter in der Lage sei, detaillierte Verbrauchswerte (u.a.: Tageswerte, Viertelstundenwerte) zu generieren. Der Detailliertheitsgrad der gemessenen Daten, so der Datenschutzrat, erlaube "*konkrete Rückschlüsse auf Lebensgewohnheiten der Verbraucher (Tagesablauf, Nutzungsverhalten etc.)*".[154] Es ist somit wohl davon auszugehen, dass der Datenschuztrat die mit einem Smart Meter gemessenen Daten als personenbezogene Daten im Sinne von § 1 ÖDSG klassifiziert.

Die Österreichische Energieagentur (Austrian Energy Agency, AEA) vertritt ebenfalls den Standpunkt, dass Messdaten als personenbezogen zu qualifizieren und somit die Bestimmungen des ÖDSG anzuwenden sind. Diese Auffassung wird damit begründet, dass "*Netzbetreiber Leistungen ausschliesslich gegenüber identifizierten Vertragspartnern*" erbringen und die Messgeräte klar einem konkreten Endkunden zugeordnet werden können. Des Weiteren sieht die AEA auch pseudonymisierte oder verschlüsselte Daten als personenbezogen an, wenn "*der Energieversorger oder Dritte im Besitz geeigneter*

[154] *Datenschutzrat*, Stellungnahme des Datenschutzrats zum Energieeffizienzpaket des Bundes, 2013, abrufbar unter: <http://www.bka.gv.at/DocView.axd?CobId=51437>.

Schlüssel oder Codelisten sind, die eine Wiederherstellung von Daten ermöglichen, zu denen Personen identifiziert und zugeordnet werden können."[155]

6.5.1.2. Umgang mit Smart Meter-Daten

Die relevanten Bestimmungen zum Umgang mit Smart Meter-Daten befinden sich grösstenteils im Elektrizitätswirtschafts- und Organisationsgesetz (ElWOG) § 81 bis § 84a und im Gaswirtschaftsgesetz (GWG) § 126 bis § 129a des Bundesministeriums für Wirtschaft, Familie und Jugend (BMWFJ). Weitere Normen zum Smart Meter finden sich ausserdem in zahlreichen Verordnungen: Die Einführung des Smart Meters ist Gegenstand der intelligente Messgeräte-Einführungsverordnung (IME-VO), während die intelligente Messgeräte-AnforderungsVO (IMA-VO) und die intelligente Gas-Messgeräte-AnforderungsVO (IGMA-VO) die technischen Anforderungen an die Smart Meter-Geräte festlegen. Die Datenformat- & VerbrauchsinformationsdarstellungsVO (DAVID-VO) enthält Regelungen zur Übermittlung der Daten durch den Netzbetreiber an die Lieferanten und zur Darstellung von Verbrauchsinformationen für den Endverbraucher.

Unabhängig von einer Messung durch intelligente oder herkömmliche Messgeräte sind Netzbetreiber und Lieferanten in Österreich gemäss § 81 Abs. 4 ElWOG resp. § 126 Abs. 5 GWG dazu verpflichtet, "*sämtliche Verbrauchs- und Abrechnungsdaten für eine Dauer von drei Jahren ab ihrer Verfügbarkeit für Zwecke der nachträglichen Kontrolle der Richtigkeit, Rechtmässigkeit und für Auskünfte gegenüber berechtigten Endverbrauchern aufzubewahren […]*."

Die Regelung im ElWOG zum Umgang mit von intelligenten Messgeräten gemessenen Daten enthält einerseits allgemeine Bestimmungen zum Umgang mit Messdaten, sieht jedoch andererseits eine Unterscheidung zwischen Tageswerten und Viertelstundenwerten vor; im GWG wird zwischen Tageswerten und Stundenwerten unterschieden.

Sämtliche Messdaten aus intelligenten Messgeräten müssen zunächst gemäss § 84 Abs. 1 ElWOG bzw. § 129 Abs. 1 GWG zu Zwecken der Verrechnung, Kundeninformation, Energieeffizienz, Energiestatistik und zur Aufrechterhaltung des sicheren und effizienten Netzbetriebs direkt auf dem Smart Meter für 60 Kalendertage gespeichert werden. Ausserdem müssen die Endkunden die Möglichkeit erhalten, ihre täglichen Verbrauchswerte über ein "*kundenfreundliches Web-Portal*" einzusehen. Das Benutzerkonto auf dem Web-Portal ist nach dem anerkannten Stand der Technik abzusichern und kann vom Verbraucher gelöscht werden (§ 84 Abs. 2 und Abs. 4 ElWOG/§ 129 Abs. 2 und Abs. 4 GWG). Die täglich erhobenen Werte, welche mithilfe eines intelligenten Messgeräts erhoben wurden, sind jeweils zu Beginn des auf die Messung folgenden Kalendermonats vom Netzbetreiber an den Lieferanten weiterzugeben (§ 84a ElWOG/ § 129a Abs. 2 GWG). Für die Verwendung von Viertelstundenwerten (ElWOG) resp. Stundenwerten (GWG) sind von Netzbetreibern spezielle Vorschriften zu beachten: Sie dürfen solche Werte nur mit ausdrücklicher Zustimmung des Endverbrauchers auslesen und verwenden (§ 84a Abs. 1 ElWOG/§ 129a Abs. 1 GWG).

Das Gesetz sieht jedoch einige Ausnahmen zu diesen Bestimmungen vor: In "*begründeten lokalen Einzelfällen*" dürfen Viertelstundenwerte/Stundenwerte auch ohne Zustimmung des Endverbrauchers verwendet werden, soweit dies für den Zweck der Aufrechterhaltung eines sicheren und effizienten Netzbetriebs unabdingbar ist. Die Daten müssen nach Erfüllung des Zwecks unverzüglich gelöscht werden (§ 84a Abs. 1 ElWOG/ § 129a Abs. 1 GWG). Die Werte dürfen des Weiteren auch für die Elektrizitätsstatistik und die Energielenkung verwendet werden, sofern sie unmittelbar mit Daten von anderen Endverbrauchern aggregiert und anschliessend anonymisiert werden (§ 84a Abs. 1 ElWOG/

[155] *Renner*, Smart Metering und Datenschutz: Umsetzung des 3. EU Binnenmarktpakets in Österreich, 2011, abrufbar unter: <http://eeg.tuwien.ac.at/eeg.tuwien.ac.at_pages/events/iewt/iewt2011/uploads/fullpaper_iewt2011/P_298_Renner_Stephan_14-Feb-2011,_10:08.pdf>.

§ 129a Abs. 1 GWG). Diese Ausnahmen stossen auf Kritik von Seiten des Datenschutzrats, welcher zwar die Verwendung der Viertelstundendaten für Zwecke der Abrechnung oder Verbraucherinformation als legitim anerkannt, die Legitimation durch "effizienten Netzbetrieb" und "Statistik" jedoch ablehnt. Der Datenschutzrat merkt an, dass die Formulierung "effizienter Netzbetrieb" einen zu grossen Auslegungsspielraum offenlasse, da das Kriterium der Effizienz sehr weitreichend sein könne (bspw. Kundenanalyse und darauf basierende Werbung für Angebote zur Steigerung der Effizienz). Vollständig abgeschafft werden sollte gemäss Datenschutzrat der Zweck der "Statistik", da sämtliche Entscheidungen betreffend Energielenkung und Netzplanung auf der Grundlage von aggregierten Summenwerten getroffen würden und eine Auslesung von Daten auf Ebene des Einzelhaushaltes somit gar nicht notwendig sei. Des Weiteren, so der Datenschutzrat, könnten Viertelstundenwerte eines einzelnen Haushalts, sollten solche tatsächlich einmal im Rahmen statistischer Erhebungen benötigt werden, auch unter freiwilliger Mitwirkung von Betroffenen erhoben werden.[156]

Viertelstundenwerte und Stundenwerte dürfen des Weiteren auch nur mit ausdrücklicher Ermächtigung des Endverbrauchers an die Lieferanten weitergegeben werden (§ 84a Abs. 2 ElWOG/ § 129a Abs. 2 GWG). Obwohl die Verwendung von Viertelstundenwerten und Stundenwerten gesetzlich von der Einwilligung der Endverbraucher abhängt, sieht der Datenschutzrat die Freiwilligkeit nicht ganzheitlich abgesichert. Es wird vorgeschlagen, einen gesetzlichen Anspruch der Endkunden auf einen Basistarif (Tarif ohne Erfordernis der Viertelstundenauslesung) zu verankern, sodass die Entscheidungsfreiheit der Endkunden nicht aufgrund des ausschliesslichen Angebots von Viertelstunden-Tarifen aufgehoben würde.[157]

6.5.1.3. Vorgaben zur Datensicherheit

Anhaltspunkte zu technischen Anforderungen bezüglich Netzsicherheit und vor allem Datensicherheit finden sich einerseits in § 83 ElWOG und § 128 GWG und andererseits in den beiden Anforderungsverordnungen (§ 3 Abs. 7 IMA-VO, § 3 Abs. 9 IGMA-VO), sowie in § 2 Abs. 2 der Datenformat- & VerbrauchsinformationsdarstellungsVO.

Die genannten Normen sehen allesamt die Absicherung der Daten durch Verschlüsselung nach dem anerkannten Stand der Technik vor. Gemäss § 3 Abs. 7 IMA-VO hat die Verschlüsselung mit einem individuellen, kundenbezogenen Schlüssel zu erfolgen. In den Erläuterungen zur Datenformat- und Verbrauchsinformationsdarstellungs VO konkretisiert die Regulierungsbehörde E-Control die Anforderungen dahingehend, dass eine "*dem Stand der Technik entsprechende, fortgeschrittene elektronische Signatur*" vorzusehen und eine standardisierte, einheitliche Lösung für ganz Österreich anzustreben sei.[158] Auch der Datenschutzrat spricht sich für eine standardisierte Vorgehensweise aus und kritisiert die Unbestimmtheit der gesetzlichen Vorgaben. In einer Stellungnahme wird daher vom Datenschutzrat vorgeschlagen, von staatlicher Seite Mindeststandards für die Sicherheit festzulegen und die Einhaltung derselben durch unabhängige Zertifizierungsstellen prüfen zu lassen.[159]

6.5.2. Grossbritannien

Grossbritannien sieht eine komplette, flächendeckende Einführung von intelligenten Messgeräten bis 2020 vor. Die Installation der Smart Meter erfolgt in zwei Phasen: Die sogenannte Basis-Phase (Foundation Stage) hat bereits im April 2011 mit der Installation

---

156 *Datenschutzrat* (Anm. 154).
157 *Datenschutzrat* (Anm. 154).
158 *E-Control*, Erläuterungen zur Verordnung Datenformat- und VerbrauchsinformationsdarstellungsVO 2012 (DAVID-VO 2012), abrufbar unter: <http://www.e-control.at/portal/page/portal/medienbibliothek/strom/dokumente/pdfs/DAVID-VO_Erl%C3%A4uterungen.pdf>.
159 *Datenschutzrat* (Anm. 154).

in ausgewählten Haushalten begonnen. Der Beginn der Massen-Installation (Mass Roll-Out) ist auf Anfang 2014 angesetzt. Es besteht in Grossbritannien kein gesetzlicher Zwang für den Endkunden, einen Smart Meter installieren zu lassen. Die Anbieter sind angehalten, für Verbraucher, die keinen Smart Meter möchten, Alternativen zur Erlangung von Informationen über den Konsum auszuarbeiten.

Bislang scheint das Smart Metering-Projekt in Grossbritannien ohne grössere Probleme zu laufen, was wohl auf grosse Transparenz, umfassende Information der Endkunden sowie den Einbezug sämtlicher Akteure in den Gesetzgebungsprozess zurückzuführen ist.

6.5.2.1. Qualifizierung von Smart Meter-Daten

In Grossbritannien existiert keine explizite Qualifizierung der Smart Meter-Daten. Die regulatorischen Vorgaben und diverse Berichte zeigen jedoch, dass die Regierung die potentiellen Gefahren im Zusammenhang mit dem Schutz von Smart Meter-Daten erkannt hat und sich damit auseinandersetzt.

In einem Dokument zu Datenzugang und Privatsphäre vom März 2011[160] nimmt die Regierung die Bedenken über die Nutzung von detaillierten Konsumdaten zur Kenntnis und betont die absolute Notwendigkeit, die Konsumenten zu schützen. Es wurden bereits im Vorfeld zahlreiche Workshops mit und Befragungen von Experten durchgeführt, um die datenschutzrechtlichen Herausforderungen zu erkennen. Besorgnis wurde im Rahmen dieser Befragungen vor allem hinsichtlich der Auslesung und Verwendung von Halbstundenwerten geäussert, da solche Werte, kombiniert mit dem Namen und der Adresse eines Individuums, personenbezogene Daten (Personal Data) im Sinne des Datenschutzgesetzes darstellen könnten. Unter dem Datenschutzgesetz gelten Daten als personenbezogen, wenn sie zur Identifikation eines lebenden Individuums gebraucht werden können.

Die Anforderungen an die Anbieter bezüglich dem Umgang mit Smart Meter-Daten (siehe unten) lassen darauf schliessen, dass Daten, welche einen Zeitraum von einem Monat wiedergeben, wohl eher nicht als personenbezogen angesehen werden, da für deren Verwendung keinerlei Einwilligung des Endverbrauchers benötigt wird. Bei den Daten bezüglich eines Zeitraums von weniger als einem Monat wird noch einmal unterschieden zwischen solchen, die einen Tag oder mehr betreffen und solchen, die einen Zeitraum von weniger als einem Tag beschreiben. Für Erstere besteht eine opt-out Möglichkeit des Endkunden, während für Letztere eine explizite Einwilligung desselben benötigt wird. Diese Bestimmungen könnten ein Hinweis darauf sein, dass vor allem die Tageswerte sowie die Werte darunter als personenbezogene Daten angesehen werden. Der Netzbetreiber darf indes sogar Halbstundenwerte verwenden, sofern diese keinen Rückschluss auf den individuellen Endkunden zulassen (aggregierte und/oder anonymisierte Daten). Wiederum lässt dies den Schluss zu, dass solche Daten, sofern sie eben nicht aggregiert bzw. anonymisiert wurden, wohl als personenbezogen zu qualifizieren sind.

6.5.2.2. Umgang mit Smart Meter-Daten

Die Rahmenbedingungen zum Umgang mit Smart Meter-Daten wurden von der Regierung in einem Zusatzdokument (Data Access and Privacy)[161] vom Dezember 2012 zum Smart Metering Implementation Programme festgelegt. Diese Rahmenbedingungen wer-

[160] *Department of Energy and Climate Change*, Smart Metering Implementation Programme- Supporting Dokument 1 of 5, 2011, abrufbar unter: <http://webarchive.nationalarchives.gov.uk/20121217150421/http://www.decc.gov.uk/assets/decc/Consultations/smart-meter-imp-prospectus/1477-data-access-privacy.pdf>.

[161] *Department of Energy and Climate Change,* Smart Metering Implementation Programme – Data access and privacy, 2012, abrufbar unter: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf>.

den vor allem in den Lizenzierungsvoraussetzungen für Anbieter und Netzbetreiber bzw. Gas Transporteure (licence conditions)[162] basierend auf Art. 6 (1) (d) des Elektrizitätsgesetzes (Electricity Act)[163] und Art. 7A (1) des Gasgesetzes (Gas Act)[164], umgesetzt. Die Befugnisse der Data Communication Company (DCC), welche in Grossbritannien die Kommunikation zwischen den intelligenten Messgeräten und den autorisierten Nutzern der Messdaten koordinieren wird, sind in der Data Communication Company Licence (finale Version noch nicht veröffentlicht) sowie im Entwurf zum Smart Energy Code[165] festgelegt. Die technischen Anforderungen an die Datensicherheit sind Gegenstand der Smart Metering Equipment Technical Specifications (SMETS)[166]. Geplant ist ausserdem die Erstellung einer sogenannten "Privacy Charter" unter Mitarbeit der Anbieter, welche die Kunden über die Art und Weise der Verwendung ihrer Daten informieren und die Entwicklung von Standards in diesem Bereich vorantreiben soll.

Energy UK, ein Verband von über 80 Unternehmen in der Energiebranche, hat bereits eigene "Privacy Commitments for Smart Metering"[167] herausgegeben, in denen sich die Firmen zum Datenschutz verpflichten und der Kunde sämtliche Informationen im Zusammenhang mit Smart Meter-Daten erhält. In den Rahmenbedingungen zum Umgang mit Smart Meter-Daten wird zunächst der Zugang des Endkunden zu seinen eigenen Daten thematisiert. Demnach hat der Endverbraucher drei Möglichkeiten, Zugriff auf seine eigenen Daten zu erlangen. Die grösste Rolle spielt dabei das sogenannte "In-Home Display", welches dem Kunden ermöglicht, seine Verbrauchsdaten direkt auf dem Smart Meter einzusehen. Die technischen Voraussetzungen an ein "In-Home Display" sind in den SMETS festgelegt. Des Weiteren soll der Endkunde über weitere Geräte durch eine Verbindung mit seinem Heimnetz (Home Area Network) Zugang zu seinen Daten erhalten. Als dritte Möglichkeit wird die direkte Anfrage beim Anbieter genannt. In diesem Zusammenhang wird zurzeit auch das Angebot einer Homepage, auf welcher die Daten eingesehen werden könnten, geprüft.

Den Anbietern ist es gemäss den Standard Conditions of Electricity Supply Licences und den Standard Conditions of Gas Supply Licences grundsätzlich verboten, sich Konsumentendaten zu beschaffen, welche sich auf eine Zeitperiode von weniger als einem Monat beziehen.[168] Sämtliche Konsumentendaten (inkl. der Daten, welche mehr als einen Monat betreffen) dürfen zudem grundsätzlich nur für die korrekte Verrechnung des Stromverbrauchs sowie zur Compliance mit gesetzlichen Regelungen verwendet werden. Ist die Verwendung für einen anderen Zweck vorgesehen, muss der Endverbraucher sieben Tage vorher darüber informiert werden. Um Daten zu verwenden, die einen Zeitraum von weniger als einem Monat aber nicht weniger als einen Tag betreffen, muss der Anbieter den Endverbraucher über den Zweck der Beschaffung dieser Daten informieren. Der Zweck des "Marketing" wird explizit nicht als legitim anerkannt. Der Endverbraucher hat daraufhin die Möglichkeit, sich innert sieben Kalendertagen gegen die Verwendung seiner Daten auszusprechen. Der Anbieter darf die Daten erst beschaffen bzw. verwenden, sobald der Verbraucher entweder sein ausdrückliches Einverständnis gegeben oder innert sieben Tagen nicht widersprochen hat. Die Verwendung dieser Daten ist ausserdem legitim, wenn sie einem der folgenden Zwecke dienlich ist: Untersuchung im Rahmen eines begründeten Verdachts auf Elektrizitätsdiebstahl, korrekte Verrechnung des

---

162 *Department of Energy and Climate Change* (Anm. 161), S. 61ff.

163 Electricity Act vom 27. Juli 1989, abrufbar unter: <http://www.legislation.gov.uk/ukpga/1989/29/contents>.

164 Gas Act vom 5. August 1965, abrufbar unter: <http://www.legislation.gov.uk/ukpga/1965/36/contents>.

165 *Department of Energy and Climate Change,* Draft to the Smart Energy Code, 2013, abrufbar unter: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/193074/20130424_Stage_1_SEC_Response_and_Consultation_on_Updated_legal_text.pdf>.

166 *Department of Energy and Climate Change,* Draft to the Smart Metering Equipment Technical Specifications, 2013, abrufbar unter: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/68898/smart_meters_equipment_technical_spec_version_2.pdf>.

167 *Energy UK*, Energy UK's Privacy Commitments for Smart Metering, abrufbar unter: http://www.energy-uk.org.uk/publication/finish/37-smart-meter-policies/448-energy-uk-privacy-commitments-for-smart-metering.html.

168 *Department of Energy and Climate Change* (Anm. 161), S. 61ff.

bezogenen Stroms und Information des Endkunden auf dessen Wunsch. Daten, welche sich auf einen Zeitraum von weniger als einem Tag beziehen, dürfen nur verwendet/beschafft werden, wenn der Endverbraucher dem Anbieter sein explizites Einverständnis erteilt. Ein bereits erteiltes Einverständnis darf jederzeit zurückgezogen werden.

Die Befugnisse des Netzbetreibers (Network Operator, Distributor) bzw. des Gas Transporteurs (Gas Transporter) zur Verwendung von Konsumentendaten werden in den Standard Conditions of Electrictiy Distribution Licences bzw. den Standard Conditions of Gas Transporters‘ Licences geregelt.[169] Im Folgenden wird der Einfachheit halber nur auf die Regelung für den Netzbetreiber eingegangen, die Bestimmungen für den Gas Transporteur decken sich jedoch damit. Der Netzbetreiber darf Daten verwenden, welche jeden beliebigen Zeitraum unter einem Monat betreffen, wenn er der zuständigen Behörde (Gas and Electricity Markets Authority) beweist, dass er konkrete Massnahmen zur Anonymisierung dieser Daten trifft. Der Netzbetreiber ist in der Wahl seiner Massnahmen frei, sofern garantiert ist, dass die Daten nicht mit einem spezifischen Endkunden in Verbindung gebracht werden können. Zudem dürfen die Daten auch bei Nichterfüllung dieser Voraussetzungen verwendet werden, wenn der Endkunde sein ausdrückliches Einverständnis dazu gegeben hat. Ein solches Einverständnis kann jederzeit wieder zurückgezogen werden.

Die DCC wird gemäss Entwurf zum Smart Energy Code als "Data Processor" im Sinne des Datenschutzgesetzes angesehen und darf personenbezogene Daten nur verarbeiten, wenn dies mit dem Zweck in der DCC-Lizenz vereinbar ist. Ausserdem muss die DCC Massnahmen treffen, welche den unautorisierten Zugriff auf solche Daten verhindern. Die Verarbeitung der Daten muss innerhalb des Europäischen Wirtschaftsraums erfolgen. Des Weiteren muss die DCC die Nutzer der Daten (Anbieter, Netzbetreiber etc.) bei der Einhaltung der Vorgaben im Bereich Datenschutz unterstützen.

In den Rahmenbedingungen zum Umgang mit Smart Meter-Daten wird zuletzt der Zugang von sogenannten Drittparteien (Third Parties) zu Konsumentendaten thematisiert. Unter die Kategorie der Drittparteien fallen neben nichtlizenzierten Akteuren auch lizenzierte Anbieter, welche ihre Dienstleistungen (bspw. ein Preisangebot) einem Endverbraucher anbieten möchten, der (noch) nicht ihr registrierter Kunde ist. Die Endverbraucher sollen die Möglichkeit erhalten, ihre Daten einer Drittpartei mitzuteilen bzw. über die DCC weiterzuleiten. Die Drittpartei muss in einem solchen Fall der DCC beweisen, dass sie tatsächlich vom Endverbraucher aufgefordert wurde, die betreffenden Daten zu verlangen. Es wird zurzeit noch diskutiert, mittels welchen Instruments diese Verifizierung vonstattengehen soll.

6.5.2.3. Vorgaben zur Netzsicherheit

Die technischen Anforderungen an die Smart Meter sind im Entwurf zu den Smart Metering Equipment Technical Specifications (SMETS) festgelegt. Die Vorgaben bezüglich Datensicherheit sind für Smart Meter für Elektrizität und für Smart Meter für Gas identisch. Generell müssen die Smart Meter so gestaltet werden, dass Fehler oder Störungen am Gerät keine Gefährdung für die persönlichen Konsumentendaten darstellen können. Ein Smart Meter muss zudem in der Lage sein, eine rollenbasierte Zugriffskontrolle auszuüben. Das Gerät autorisiert je nach Rolle (Berechtigung) eines Benutzers andere Aktionen.

Die intelligenten Messgeräte müssen folgende kryptographischen Algorithmen unterstützen: Elliptic Curve DSA, Elliptic Curve DH sowie SHA-256. Beim Ausführen oder Erzeugen eines Befehls, einer Rückmeldung oder einer Warnung muss das Gerät kryptographische Algorithmen zu Zwecken der digitalen Signatur, der Verifizierung einer digi-

[169] *Department of Energy and Climate Change* (Anm. 161), S.79ff.

talen Signatur, des Hashing, der Nachrichtenauthentifizierung sowie der Verschlüsselung bzw. Entschlüsselung anwenden können. Beim Transfer von Personendaten, Konsumdaten und Sicherheitsinformationen muss das Gerät die Fähigkeit haben, jeglichen unautorisierten Zugangsversuch, der die Vertraulichkeit oder die Intaktheit der Daten gefährden könnte, zu bemerken und zu verhindern. Dasselbe gilt für Zugriffsversuche auf Daten, welche auf dem Smart Meter gespeichert sind. Des Weiteren muss der Smart Meter technische Möglichkeiten besitzen, sich gegen Replay-Angriffe zu schützen.

6.5.3. Deutschland

Die deutsche Bundesregierung wird in Umsetzung ihres Energiekonzepts stufenweise für eine intelligente Anbindung von Verbrauchern und Erzeugern an das Energienetz sorgen.[170] Eine Einbaupflicht von intelligenten Messsystemen ist derzeit jedoch noch nicht vorgesehen. § 21c EnWG enthält lediglich eine Pflicht zum Einbau intelligenter Messsysteme ab einem Verbrauch von 6‘000 Kilowattstunden und bei Neubauten oder Renovierungen, soweit dies technisch machbar ist. Bei allen übrigen Gebäuden ist eine Einbaupflicht nach § 21c Abs. 2 EnWG erst vorgesehen, wenn dies technisch machbar und wirtschaftlich vertretbar ist. Eine Kosten-Nutzen-Analyse, die von Ernst & Young im Auftrag des deutschen Bundes durchgeführt und 2013 veröffentlicht worden ist, zeigt, dass derzeit die flächendeckende Einführung von intelligenten Messsystemen in Deutschland weder gesamtwirtschaftlich noch einzelwirtschaftlich vorteilhaft ist.[171] Eine allgemeine Einbaupflicht ist deshalb nicht absehbar. Ohne ein derartiges Obligatorium hängt der Erfolg von Smart Metering unmittelbar von der Akzeptanz der Verbraucher ab. Wie Erfahrungen in Kanada und den Niederlanden belegen, stellt die Gewährleistung eines angemessenen Datenschutzes dabei ein wesentliches Erfolgskriterium dar.[172] Gesetzliche Grundlagen müssen sicherstellen, dass die Betroffenen nicht zu "gläsernen Energieverbrauchern" werden.[173]

6.5.3.1. Qualifikation der Smart Meter-Daten

Die für das Smart Metering relevanten Rechtsgrundlagen machen keine Angaben darüber, wie die erhobenen Daten zu qualifizieren sind. § 21g Abs. 1 EnWG besagt lediglich, "*die Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus dem Messsystem oder mit Hilfe des Messsystems darf ausschließlich durch zum Datenumgang berechtigte Stellen erfolgen und auf Grund dieses Gesetzes nur, soweit dies erforderlich ist […].*" Welche Daten nun aber als personenbezogen zu qualifizieren sind, geht nicht aus den gesetzlichen Grundlagen hervor. Gemäss den Datenschutzbeauftragten des Bundes und der Länder handelt es sich bei allen Daten, die durch einen Smart Meter erfasst werden, um personenbezogene Daten, unabhängig davon, ob es technische Daten sind.[174] Nach dem Bundesdatenschutzgesetz besteht ein Personenbezug bereits dann, wenn die Daten auf eine Person beziehbar sind.[175] Die Sensitivität und damit der Schutzbedarf der personenbezogenen Daten können variieren und sind abhängig davon, inwieweit Rückschlüsse auf das Verhalten und die Lebensgewohnheiten der Letztverbraucher gemacht werden können.[176]

---

170 *Bundesamt für Sicherheit in der Informationstechnik*, Smart Metering Systems, 2013, abrufbar unter: <https://www.bsi.bund.de/DE/Themen/SmartMeter/smartmeter.html>.

171 *Ernst & Young*, Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler, 2013, S. 217.

172 *Der Bundesbeauftragte für den Datenschutz und Informationssicherheit*, Positionspapier zu den Datenschutzanforderungen an Smart Meter, 2011.

173 *Der Bundesbeauftragte für den Datenschutz und Informationssicherheit* (Anm. 172).

174 *Datenschutzkonferenz/Düsseldorfer Kreis*, Orientierungshilfe datenschutzgerechtes Smart Metering, 2012, S. 9.

175 § 3 Abs. 1 BDSG

176 *Datenschutzkonferenz/Düsseldorfer Kreis* (Anm. 174), S 9.

6.5.3.2. Umgang mit Smart Meter-Daten

Das deutsche Datenschutzrecht geht von einem Verbot mit Erlaubnisvorbehalt aus. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit eine Rechtsgrundlage dafür besteht oder der Betroffene eingewilligt hat. Im Zusammenhang mit Smart Metering stellt § 21g EnWG eine Rechtsvorschrift in diesem Sinne dar. Gemäss der genannten Vorschrift ist die Erhebung, Verarbeitung und Nutzung von Daten nur zulässig, soweit es für die in § 21g Abs. 1 EnWG abschliessend aufgeführten Fälle erforderlich ist und darf nur durch die dafür berechtigten Stellen erfolgen. Jegliche darüber hinausgehende Datenverarbeitung bedarf im Einzelfall einer Einwilligung des Letztverbrauchers.[177] Die Einwilligung muss den Anforderungen des Bundesdatenschutzgesetzes genügen, wonach sie nur wirksam wird, wenn sie auf der freien, bestimmten und informierten Entscheidung des Letztverbrauchers beruht.[178] Das Energiewirtschaftsgesetz sieht zudem die Grundsätze der Verhältnismässigkeit und der Zweckbindung vor und verankert ein Koppelungsverbot der generierten Daten, die ständige Information des Letztverbrauchers über die erhobenen Daten, das Einwilligungserfordernis sowie Einwirkungsmöglichkeiten für das Fernmessen und Fernwirken. Daneben sieht das Energiewirtschaftsgesetz die Möglichkeit der Auftragsdatenverarbeitung vor. Dabei wird dem Endverbraucher die Anonymisierung und Pseudonymisierung der Daten zugesichert. Allgemein sind die personenbezogenen Daten nach § 21g Abs. 5 EnWG zu anonymisieren oder zu pseudonymisieren, soweit dies der Verwendungszweck erlaubt und es im Verhältnis zum angestrebten Schutzzweck keinen unverhältnismässigen Aufwand erfordert. Näheres ist nach § 21g Abs. 6 i.V.m. § 21i Abs. 1 Nr. 4 EnWG in einer Rechtsverordnung zu regeln, deren Inkraftsetzung grundsätzlich noch 2013 geplant ist. Die Rechtsverordnung soll unter anderem die in § 21g Abs. 1 EnWG aufgezählten Verwendungszwecke weiter konkretisieren, Höchstfristen für die Speicherung festlegen und die berechtigten Interessen der Unternehmen und der Betroffenen angemessen berücksichtigen.

Basierend auf der Aufzählung in § 21 Abs. 1 EnWG hat die Konferenz der Datenschutzbeauftragten des Bundes und Länder Use Cases entwickelt, welche unter anderem die für den jeweiligen Anwendungsfall erforderlichen Daten, deren Schutzbedarf und die beteiligten Akteure angeben. Diese Use Cases unterscheiden sich von den in der vorliegenden Studie definierten Use Cases. Die Use Cases in Deutschland dienen ausschliesslich der Definition von Voraussetzungen, unter denen die Datenverarbeitung beim Smart Metering datenschutzrechtlich zulässig ist und die auch bei der Konzeption von Geräten, Verfahren und Infrastrukturen zu beachten sind.[179] Zusammenfassend können daraus folgende Empfehlungen abgeleitet werden:[180]

- Die Verarbeitung der Smart Meter-Daten ist nur zulässig, soweit dies für einen der in § 21g Abs. 1 EnWG abschliessend aufgezählten Zwecken notwendig ist.
- Das Ablesen der Daten muss in so grossen Intervallen stattfinden, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten des Letztverbrauchers geschlossen werden können.
- Soweit möglich, sollen die Smart Meter-Daten anonymisiert, pseudonymisiert oder aggregiert übermittelt werden.
- Der Endverbraucher muss die Möglichkeit haben, hoch aufgelöste Daten lokal abzurufen, ohne auf eine externe Datenverarbeitung angewiesen zu sein.
- Die Zahl der in der Datenerhebung, Verbreitung und Nutzung involvierter Akteure soll möglichst klein sein.

177 *Datenschutzkonferenz/Düsseldorfer Kreis* (Anm. 174), S 11.
178 § 4a BDSG.
179 *Datenschutzkonferenz/Düsseldorfer Kreis* (Anm. 174), S 1.
180 *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Entschliessung, 2012.

- Es sind angemessene Löschfristen für die Daten festzulegen, so dass eine Vorratsspeicherung vermieden wird.
- Die Kommunikations- und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar sein. Er muss die Zugriffe auf den Smart Meter erkennen und diese unterbinden können.
- Der Endverbraucher bedarf eines durchsetzbaren Anspruchs auf Löschung, Berichtigung und Widerspruch der erhobenen Daten.
- Der Betroffene muss einen Tarif wählen können, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass sich dies nachteilig auf seine Energieversorgung auswirkt.
- Für den Zugang zu den Smart Metern müssen eindeutige Berechtigungsprofile definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in den technischen Richtlinien des BSI.[181]
- Die Gewährleistung des Datenschutzes muss bereits bei der Konzeption und Gestaltung der technischen Systeme berücksichtigt werden. Der jeweils aktuelle Stand der Technik darf dabei nicht unterschritten werden.

Nachfolgend wird auf einige der erarbeiteten Use Cases ausführlicher eingegangen.

6.5.3.2.1. Vertragsgestaltung (§ 21g Abs. 1 Nr. 1 EnWG)[182]

Für die Begründung, Änderung und Aufhebung von Energielieferungsverträgen ist die Übermittlung verschiedener zum Teil sensibler Daten erforderlich. Dabei sind vor allem Aspekte der technischen Datensicherungen, wie der verschlüsselten Kommunikation nach dem jeweils aktuellen Stand der Technik, relevant.

6.5.3.2.2. Messen (§ 21g Abs. 1 Nr. 2)[183]

Für die Abrechnung der Netzentgelte für die Netznutzung zwischen dem Netznutzer (i.d.R. dem Energielieferanten) und dem Netzbetreiber müssen die Verbrauchsdaten der Letztverbraucher pro Jahr bzw. pro Monat übermittelt werden. Zurzeit erfolgt diese Abrechnung der Netzentgelte pro Zähler. Den Datenschutzbeauftragten des Bundes und der Länder erscheinen jedoch kumulierte Messwerte ausreichend. Sofern die Verbrauchsdaten nur als Jahreswert übermittelt werden, erscheint ihnen der Haushaltsbezug aber dennoch als nicht kritisch. Erst bei einer Übermittlung in kürzeren Zeitintervallen bewerten sie den Haushaltsbezug als kritisch. Sie empfehlen in diesem Fall die Zuordnung der Letztverbraucher zum Energielieferanten über ein Pseudonym.

Zur Abrechnung bezogener und eingespeister Energie im Bilanzierungssystem werden die Verbrauchsdaten der Letztverbraucher pro Zeitintervall zu Bilanzkreissummenzeitreihen aggregiert und vom Verteilnetzbetreiber über den Übertragungsnetzbetreiber an den Bilanzkreisverantwortlichen übermittelt. Zusätzlich werden die nicht aggregierten Daten zu Kontrollzwecken an den Energielieferanten übermittelt. Nach Ansicht der Datenschutzbeauftragten ist dieses Vorgehen aus Sicht des Datenschutzes äusserst problematisch, wenn die Verbrauchsdaten, die meist im 15-Minuten Intervall erhoben werden, einen Haushaltsbezug aufweisen und somit eine Profilbildung ermöglichen. Nach ihren Einschätzungen genügen nicht-haushaltsbeziehbare Messungen an Ortsnetzstationen, um eine bessere Abbildung des tatsächlichen Verbrauchs und der tatsächlichen Einspeisung im Bilanzierungssystem zu erreichen.

---

181 Vgl. *dazu 6.5.3.3 Vorgaben zur Netzsicherheit.*
182 *Datenschutzkonferenz/Düsseldorfer Kreis* (Anm. 174), S. 21ff.
183 *Datenschutzkonferenz/Düsseldorfer Kreis* (Anm. 174), S. 26.

Für das Zu- und Abschalten von unterbrechbaren Verbrauchseinrichtungen wird in 15-Minuten-Intervallen die Differenz zwischen Einspeisung und Verbrauch von Energie ermittelt. Diese feingranulare Datenerfassung ermöglicht gemäss Datenschutzrat Rückschlüsse auf einzelne Geräte und in Verbindung mit anderen Verbrauchsdaten sogar eine Profilbildung. Der Haushaltsbezug erscheint den Datenschutzbeauftragten in diesen Fällen unkritisch, sofern die Daten unmittelbar nach deren Auswertung gelöscht und nicht mit anderen Verbrauchsdaten verbunden und genutzt werden. Nicht klar ist ihnen, weshalb die Erhebung der Ein- und Ausspeismengen im 15-Minuten-Takt erfolgt.

6.5.3.2.3. Beliefern und Abrechnen (§ 21g Abs. 1 Nr. 3)[184]

Für die Abrechnung der vom Letztverbraucher bezogenen Energie müssen dem Energielieferanten die Verbrauchsdaten pro Zeitintervall übermittelt werden. Da die Verbrauchsdaten Rückschlüsse auf die Lebensgewohnheiten der Betroffenen ermöglichen, handelt es sich dabei um hoch sensible Daten. Die Datenschutzbeauftragten raten deshalb, die Energieversorgungsunternehmen zu verpflichten, die erhobenen Daten unmittelbar nach Erstellung der Abrechnungsdaten zu löschen und ein Verbinden mit anderen Verbrauchdaten zu verbieten. Zudem soll der Letztverbraucher darüber informiert werden, wer welche Daten zu welchem Zweck erhält, um dies überprüfen zu können.

Die Erstellung der Abrechnung der Verbrauchsdaten kann auch dezentral im Gateway erfolgen, so dass die Daten in aggregierter Form für die verschiedenen Tarifzonen an den Energielieferanten gesendet werden können. Diese dezentrale Abrechnung im Gateway ist datenschutzfreundlich, da die aggregierte Datenübermittlung keine detaillierten Verbrauchsprofile preisgibt, und ist somit zu bevorzugen.

6.5.3.2.4. Einspeisen und Abrechnen (§ 21g Abs. 1 Nr. 4)[185]

Damit die Einspeisemenge für die Abrechnung des Energielieferanten bereitgestellt werden kann, werden ihm die Abrechnungsdaten durch den Prosumer in aggregierter Form übermittelt. Die Datenschutzbeauftragten des Bundes und der Länder halten eine feingranulare Übertragung der Einspeisemenge durch den Letztverbraucher nicht erforderlich, da die Abrechnung der Einspeisemenge dezentral erfolgen kann. Ein direkter Datenfluss vom Prosumer zum Energielieferant genügt demnach.

6.5.3.2.5. Steuerung von unterbrechbaren Verbrauchseinrichtungen (§ 21g Abs. 1 Nr. 5)[186]

Je nach Netzauslastung kann der Netzbetreiber die Energieaufnahme von unterbrechbaren Verbrauchseinrichtungen wie Elektrospeicherheizung oder Elektrowärmepumpe steuern, sie also ein-und ausschalten bzw. ihre Leistung über die Menge der Energieaufnahme beeinflussen. Anhand der Statusdaten der unterbrechbaren Verbrauchsgeräte des Letztverbrauchers weiss der Netzbetreiber, wie er entsprechend seiner Energiebilanz im Netz die unterbrechbaren Verbrauchsgeräte ansteuern kann. Die Statusdaten ermöglichen insbesondere bei deren Verknüpfung Rückschlüsse auf die Lebensgewohnheiten der Betroffenen. Die Datenschutzbeauftragten des Bundes und der Länder empfehlen deshalb, es zu verbieten, die Statusdaten der einzelnen Geräte zu verknüpfen und die Energielieferanten zu verpflichten, die Statusdaten unmittelbar zu löschen. Dem Letztverbraucher soll ihrer Ansicht nach im Sinne seiner Datenhoheit ein Mitbestimmungsrecht eingeräumt werden. Er soll z.B. über die zeitlichen Übermittlungsintervalle seiner Daten entscheiden oder die Übermittlung der Daten während gewissen Zeiten ganz ausschliessen können. Zudem sind die Statusdaten über verschlüsselte Kommunikationskanäle zu übermitteln.

---

184 *Datenschutzkonferenz/Düsseldorfer Kreis* (Anm. 174), S. 30ff.
185 *Datenschutzkonferenz/Düsseldorfer Kreis* (Anm. 174), S. 32.
186 *Datenschutzkonferenz/Düsseldorfer Kreis* (Anm. 174), S. 34ff.

6.5.3.2.6. Veranschaulichung des Energieverbrauchs (§ 21g Abs. 1 Nr. 6)[187]

Zur Verbrauchsanalyse durch den Endverbraucher werden feingranulare Verbrauchsdaten erfasst. Da der Zweck der Datenauswertung in diesem Fall gerade darin besteht, das Nutzungsverhalten des Letztverbrauchers nachvollziehbar zu machen, handelt es sich dabei gemäss Datenschutzrat um sehr sensible Daten. Gemäss den Datenschutzbeauftragten des Bundes und der Länder kann sich der Endverbraucher mit einer lokalen Schnittstelle von Smart Meter zum Verbraucher ein Bild über seinen Energieverbrauch machen, ohne dass sensible Verbrauchsdaten an Dritte weitergeleitet werden müssen. Ein externer Drittanbieter oder ein Energielieferant ist für die Aufbereitung der Verbrauchsdaten grundsätzlich nicht erforderlich. Wenn eine solche externe Auswertung allerdings auf Grundlage einer Einwilligung trotzdem erfolgen soll, setzt dies nach Ansicht der Datenschutzbeauftragten den Einsatz wirksamer Verschlüsselungstechniken, eine entsprechend vertraglich vereinbarte Zweckbindung sowie die Möglichkeit zur jederzeitigen Kündigung und Löschung der Daten voraus.

6.5.3.2.7. Ermittlung des Netzzustandes (§ 21g Abs. 1 Nr. 7)[188]

Zur Sicherstellung der Energieversorgung und Netzplanung erlaubt es das EnWG, dass Netzzustandsdaten wie Spannung, Frequenz, Strom und Phasenwinkel erhoben werden. Nach Ansicht der Datenschutzbeauftragten des Bundes und der Länder ist allerdings nicht abschliessend geklärt, inwiefern Smart Meter Daten für die Ermittlung des Netzzustandes erforderlich bzw. die Messung in der Ortsnetzstation zu diesem Zweck nicht ausreichen. Je nach Wert der erhobenen Netzzustandsdaten können Massnahmen ergriffen werden, um den Energieverbrauch und die Einspeisung in Einklang zu bringen, so dass Rückschlüsse auf Verbrauchsdaten möglich sind. Abhängig davon, welche Rückschlüsse aufgrund von feingranularen Daten auf sensible Verbrauchsdaten gemacht werden können, kann ein Verbraucherprofil erstellt werden. Gemäss den Datenschutzbeauftragten erfordert die Erhebung der Netzzustandsdaten keinen Haushaltsbezug. Eine Zuordnung der Daten zu einer Ortsnetzstation über ein Pseudonym sollte demnach ausreichend sein.

6.5.3.3. Vorgaben zur Netzsicherheit

§ 21e EnWG sieht vor, dass nur Messsysteme verwendet werden dürfen, welche die Datenschutz-, Datensicherheits- und Interoperabilitätsanforderungen für Smart Metering zum jeweils aktuellen Stand der Technik erfüllen. Dabei wird die Pflicht zur Verwendung von Verschlüsselungsverfahren bei der Nutzung allgemeinzugänglicher Kommunikationsnetze betont.

Um einen einheitlichen technischen Sicherheitsstandard für alle Marktakteure zu gewährleisten, hat das Bundesamt für Sicherheit und Informationstechnik (BSI) eine Bedrohungsanalyse und ausgehend davon ein Schutzprofil für den sicheren und datenschutzfreundlichen Betrieb entwickelt, das die Mindestsicherheitsanforderungen an intelligente Netze festlegt. Zukünftige Smart Meter Gateways müssen auf Basis dieses Schutzprofils geprüft werden und erhalten nach positivem Prüfergebnis ein Zertifikat als verbindlichen Nachweis über die Erfüllung der Schutzziele. Die Sicherheitsanforderungen sind so formuliert worden, dass den Herstellern ausreichend Spielraum bei der technischen Ausgestaltung verbleibt, um Innovationen zu ermöglichen, gleichzeitig aber ein einheitlich hoher Sicherheitsstandard gewährleistet wird.[189] In der weitergehenden technischen Richtlinie des BSI (BSI TR-03109) sind die im Schutzprofil formulierten Sicherheitsanfor-

187 *Datenschutzkonferenz/Düsseldorfer Kreis* (Anm. 174), S. 36.
188 *Datenschutzkonferenz/Düsseldorfer Kreis* (Anm. 174), S. 37f.
189 *Deutsche Energie Agentur*, Datensicherheit und Datenschutz beim Einsatz von Smart Metern, abrufbar unter: <http://www.effiziente-energiesysteme.de/themen/smartmeter/rechtliche-rahmenbedingungen-fuer-den-einsatz-von-stromzaehlern-in-deutschland.html>.

derungen weiter ausgestaltet und darüber hinaus funktionale Anforderungen zur Gewährleistung von Interoperabilität und der technischen Umsetzung der Mindestsicherheitsanforderungen des Schutzprofils entwickelt worden.[190] Zudem regelt die überarbeitete Messsystemverordnung, die noch 2013 in Kraft treten soll, die technische Mindestanforderungen an den Einsatz von Messsystemen im Sinne von § 21d Abs. 1 EnWG.[191]

6.5.4. Niederlande

Um die europäischen Vorgaben im Energiemarkt umzusetzen, lancierte die niederländische Regierung im Jahr 2007 einen ersten Gesetzesentwurf. Die Regierung entschied sich u.a. für eine gesetzlich verpflichtende Einführung von Smart Metern. Man sah sich zu diesem Schritt genötigt, da davon ausgegangen wurde, dass ohne diesen regulativen Eingriff lediglich eine Marktpenetration mit Smart Metern von rund 30% erreicht werden könne. Am 3. Juli 2008 erliess die Zweite Kammer der Generalstaaten das entsprechende Gesetz, welches die flächendeckende Einführung von Smart Metern in den Niederlanden vorsah. Die Weigerung, einen Smart Meter einbauen zu lassen, wurde als "Wirtschaftsstraftat" qualifiziert und mit einer Busse von bis zu 17‘000 Euro oder einer mehrmonatigen Gefängnisstrafe belegt. Infolge heftiger Proteste durch die Öffentlichkeit kippte 2009 die Erste Kammer der Generalstaaten das Gesetz. Im Zentrum der Proteste standen insbesondere datenschutzrechtliche Bedenken. Von Bedeutung war in diesem Zusammenhang auch ein Bericht der Universität Tilburg, welcher festhielt, dass der niederländische Rollout das in Art. 8 ERMK statuierte Recht auf Achtung des Privat- und Familienlebens verletzen würde. Das Vorliegen einer gesetzlichen Grundlage für den Eingriff wurde zwar bejaht (Art. 8 Abs. 2 EMRK). Moniert wurde jedoch, dass die niederländische Regierung nicht klar darlegen konnte, dass der Rollout in *"einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer*" (Art. 8 Abs. 2 EMRK).[192]

Der nun revidierte niederländische Elektrizitäts- und Gas-Akt (in Kraft seit 2012) verpflichtet den Netzbetreiber dazu, Kleinkunden, worunter Haushalte und kleine Unternehmen fallen, einen Smart Meter anzubieten. Dabei haben die Kunden das Recht zu entscheiden, ob sie den Smart Meter einbauen lassen wollen oder nicht. Wird der Einbau des Smart Meters akzeptiert, muss der Verbraucher den Netzwerkbetreiber zur Bearbeitung der Daten autorisieren. Danach wird ein definiertes Mindestmass an Informationen für speziell regulierte Zwecke wie bspw. die Erstellung der Jahresrechnung geliefert. Es wurde also gesetzlich ein Mindestmass an Dienstleistungen definiert, welche die Netzbetreiber dem Kunden erbringen müssen. Alles, was darüber hinausgeht, also bspw. das Erfassen aller Informationen in Echtzeit und damit verbundene Dienstleistungen, werden dem Markt überlassen. Des Weiteren müssen von den Netzbetreibern Massnahmen getroffen werden, dass die vom Smart Meter gesammelten Daten nur für diejenigen Zwecke verwendet werden, in welche der Verbraucher eingewilligt hat. Im neuen Erlass wurden im Standardisierungsprozess also nicht nur kommerzielle und technische Aspekte, sondern auch die Interessen der Konsumenten, wie der Schutz der Privatsphäre, berücksichtigt.[193]

---

190 *Deutsche Energie Agentur* (Anm.189).

191 *Bundesamt für Sicherheit in der Informationstechnik*, Schutzprofil für ein Smart Meter Gateway (BSI-CC-PP-0073), abrufbar unter: <https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html>.

192 *Van Elburg*, SmartRegions: improving energy efficiency prospects of smart metering through collaboration and innovative services, 2011, S. 4ff.

193 *Hierzinger et al.*, European Smart Metering Landscape Report 2012 – update May 2013, 2012, S. 8; vgl. auch: *Hoenkamp/Huitma/De Moor van Vugt*, The Neglected Consumer: The Case of the Smart Meter Rollout in the Netherlands, Renewable Energy Law and Policy Review (4/2011), S. 275ff.

6.6. Exkurs: Datenschutzbestimmungen im Fernmeldegesetz

Das FMG regelt die fernmeldetechnische Übertragung von Informationen (Art. 2 FMG) und enthält in Art. 43ff. FMG und der dazugehörigen Verordnung (Art. 80ff. FDV[194]) Bestimmungen zum Datenschutz, welche gemäss Art. 89 FDV den Bestimmungen des DSG vorgehen. Aufgrund des weiten Anwendungsbereichs des FMG können diese Datenschutzbestimmungen grundsätzlich auch auf die Datenübertragung im Smart Grid Anwendung finden, da bspw. Metering-Daten bei der Fernauslesung fernmeldetechnisch übertragen werden.

Zu beachten sind indes folgende Vorbehalte. Zunächst haben die Bestimmungen nur Geltung für Anbieterinnen und Anbieter von Fernmeldediensten. Ausserdem nimmt Art. 2 FDV gewisse Fälle der Datenübermittlung vom Anwendungsbereich aus. Einige Bestimmungen scheinen auf den ersten Blick für den spezifischen Anwendungsbereich des Smart Grids nicht einschlägig zu sein bzw. es sind zum jetzigen Zeitpunkt kaum Anwendungsfälle denkbar (so bspw. Vorgaben bezüglich der Rufnummer oder Anrufumleitung, Art. 84-86, 88 FDV). Andere Bestimmungen wiederum könnten den Kundinnen und Kunden gewisse, über das DSG hinausgehende, zusätzliche Rechte verleihen bzw. die Pflichten der Fernmeldedienstanbieter auf den Anwendungsbereich des Smart Grids ausweiten. Zu denken ist bspw. an Informations- und Hilfsmittelangebotspflichten bezüglich Dienstesicherheit im Rahmen von Art. 87 FDV oder hinsichtlich der zu treffenden Massnahmen bei unlauterer Massenwerbung (Art. 82f. FDV).

Werden zukünftig für gewisse Dienste im Smart Grid Standortdaten verwendet, müsste Art. 45b FMG ebenfalls beachtet werden.[195] Denkbar ist ebenso, dass gewisse Datenverarbeitungsvorgänge von Art. 45c FMG erfasst sein könnten. Nach dieser Bestimmung dürfen Daten auf fremden Geräten nur dann durch fernmeldetechnische Übertragung bearbeitet werden, wenn dies entweder für die Erbringung der Fernmeldedienste oder ihre Abrechnung erforderlich ist oder die betroffenen Personen über die Bearbeitung und ihren Zweck informiert und darauf hingewiesen werden, dass sie die Bearbeitung ablehnen können.[196] Die Bestimmung wurde zwar bewusst technologieneutral formuliert, allerdings ist ebenfalls klar, dass der Gesetzgeber damit Eingriffe wie die Installation und Nutzung von sog. Cookies, Web-Bugs, Hidden Identifiers oder Spyware erfassen wollte, was den Anwendungsbereich von Art. 45c FMG vorliegend wieder einschränkt.[197]

Man kann sich fragen, ob die Kommunikation zwischen dem Smart Meter und dem Smart Grid dem Fernmeldegeheimnis (Art. 43 FMG) untersteht.[198] Dies ist jedenfalls dann zu verneinen, sofern Informationen innerhalb eines Gebäudes, innerhalb ein und desselben Unternehmens oder innerhalb öffentlich-rechtlicher Körperschaften sowie zwischen ihnen übertragen werden (Art. 2 FDV mit weiteren Ausnahmen). Bei einer Einwilligung der Kunden liegt ein Rechtfertigungstatbestand vor, Art. 43 FMG käme in einem solchen Fall also ebenso wenig zur Anwendung. Würde schliesslich die Bearbeitung der Informationsströme im Smart Grid in einem Bundesgesetz geregelt, hätten diese Bestimmungen als lex specialis Vorrang.

Zusammenfassend kann festgehalten werden, dass die Bestimmungen im FMG den Fernmeldedienstanbietern bei den Informationsströmen im Smart Grid gewisse zusätzliche Pflichten auferlegen könnten, diese scheinen jedoch nur von beschränkter Relevanz zu sein.

---

194 Verordnung vom 9. März 2007 über Fernmeldedienste (FDV), SR 784.101.1.

195 Hierbei geht es nicht um den Standort der Smart Mieter, sondern um andere, zukünftig womöglich kommunizierende Dinge wie bspw. Elektrofahrzeuge.

196 *Isler*, Mobile Medical Apps: Patient Datenschutz, in: digma (3/2013), S. 110-115, S. 113.

197 Vgl. *Jöhri/Rosenthal* (Anm. 18), Art. 45c FMG N. 8

198 So handelt es sich bei IP-Adressen gemäss BGE 136 II 508 E. 3.1um Adressierungselemente im Sinne der Fernmeldegesetzgebung.

6.7. Schlussfolgerung und Lösungsansätze für die Schweiz

Nachfolgend werden die Ausführungen in den Kapiteln 6.2 bis 6.5 in Schlussfolgerungen zusammengefasst und es werden mögliche Lösungsansätze für den Schweizer Gesetzgeber dargestellt.

6.7.1. Gesetzliche Rahmenbedingungen

6.7.1.1. Schlussfolgerungen

Personendaten: Bei einem grossen Teil der in den 12 Use Cases erfassten Datenströme, wie bspw. Abrechnungsdaten, Kundendaten, Meter-Daten inkl. Historie, Netzkonfigurations- oder Netzbauplanungsdaten handelt es sich um Personendaten, bei deren Bearbeitung die datenschutzrechtlichen Vorgaben zu beachten sind. Zu beachten ist dabei, dass sobald ein Datensatz geschützte Personendaten enthält, die datenschutzrechtlichen Anforderungen für den ganzen Datensatz Anwendung finden.

Rechtszersplitterung: In der Schweiz besteht im Bereich des Datenschutzes eine Parallelität von Bundesrecht und kantonalem Recht. Nebst dem bundesrechtlichen Datenschutzgesetz, welches unter Privaten und gegenüber Bundesbehörden gilt, haben auch Kantone eigene Datenschutzgesetze, die mit Bezug auf kantonale Behörden zur Anwendung kommen. Da sehr viele Netzbetreiber zur kantonalen Verwaltung im weiteren Sinne zählen (Kantonswerke), würden auf solche Netzbetreiber kantonale Gesetze zur Anwendung kommen. Die sich daraus ergebende Rechtszersplitterung im Datenschutz kann im Anwendungsbereich des Smart Grid sowohl auf Seiten der Netzbetreiber aber insbesondere auch auf Seiten der Konsumenten zu Rechtsunsicherheit führen und eine einheitliche Regelung im Zusammenhang mit Meter-Daten verunmöglichen. Solche Rechtsunsicherheiten hindern Investitionen in Smart Grid und können einer optimalen Nutzung des Potenzials im Wege stehen.

Bundeskompetenz: Nach der hier vertretenen Auffassung hat der Bund gestützt auf Art. 89 Abs. 3 und Art. 91 der Bundesverfassung die Kompetenz, den Betrieb eines Smart Grids unter Einsatz von Smart Metering Geräten umfassend zu regeln. Diese Kompetenz umfasst auch die Frage, wie, von wem und unter welchen Voraussetzungen Meter-Daten genutzt bzw. bearbeitet werden können und welche Rechte den davon betroffenen Personen zukommen.

Rechtsunsicherheiten in der Anwendung des DSG: Aber selbst die direkte Anwendbarkeit eines Datenschutzgesetzes (z.B. jenes des Bundes) führt bereits bei den hier untersuchten 12 Use Cases zu Rechtsunsicherheiten. Namentlich enthält die Datenschutzgesetzgebung in der Regel keine sektorspezifischen, sondern allgemeine Regeln, deren Anwendung in einem konkreten Fall u.U. erhebliche Interpretationsspielräume offen lässt. So ist es z.B. für den Einzelnen schwierig zu beurteilen, wann ein überwiegend privates oder öffentliches Interesse im Sinne von Art. 13 Abs. 1 DSG für die Bearbeitung von Personendaten vorliegt.

Stromversorgungsrechtliche Regelung: Der Bund hat bereits Regelungen für die Bearbeitung von Messdaten der Endverbraucher erlassen. In Art. 10 Abs. 2 StromVG wird statuiert, dass wirtschaftlich sensible Informationen, die aus dem Betrieb der Elektrizitätsnetze gewonnen werden, von den Elektrizitätsversorgungsunternehmen unter Vorbehalt der gesetzlichen Offenlegungspflichten vertraulich behandelt und nicht für andere Tätigkeitsbereiche genutzt werden dürfen (sog. informationelles Unbundling). Der Zugang zu Messdaten wird in Art. 8 StromVV geregelt; dies mit einer für die vorliegend diskutierten 12 Use Cases zu engen Zweckumschreibung: Die Informationen dürfen namentlich nur insoweit weitergegeben werden, als sie für den Netzbetrieb, das Bilanzmanagement, die Energielieferung, die Anlastung der Kosten, die Berechnung der Netznutzungsentgelte

und die Abrechnungsprozesse im Zusammenhang mit dem Energiegesetz notwendig sind. Anwendungen wie z.B. Use Case 3 (Gebäudeautomatisierung) sind von der Regelung in Art. 8 StromVV nicht erfasst. Zudem genügen in den meisten in Art. 8 StromVV umschriebenen Fällen aggregierte Daten ohne Personenbezug (Bilanzmanagement) oder Daten, welche ein- oder zweimal jährlich erhoben werden (Abrechnungen), so dass die datenschutzrechtlichen Fragen im heutigen gesetzlichen Rahmen eine untergeordnete Rolle spielen.

Big Data: Die Problematik von Big Data ist in der heutigen Datenschutzgesetzgebung ungelöst. Hier dürfte es schwierig sein, eine allgemeine Regelung unter Berücksichtigung der zukünftigen Technologieentwicklungen und der Verfügbarkeit von Daten im Internet (z.B. GIS-Daten, Social Networks, Wasserverbrauch etc.) zu finden.

6.7.1.2. Lösungsansätze

Nach der vorliegend vertretenen Rechtsauffassung besteht mit Bezug auf Smart Grid und Smart Meter Handlungsbedarf des Gesetzgebers. Es gilt vorliegend, die Rechtsunsicherheiten, welche derzeit in Datenschutzfragen im Zusammenhang mit Smart Grid-Anwendungen bestehen, zu beseitigen oder zumindest zu reduzieren. Folgende Lösungsansätze sind denkbar:

Anwendbarkeit des eidgenössischen Datenschutzgesetzes: Ein Lösungsansatz würde darin bestehen, das Datenschutzgesetz des Bundes für anwendbar zu erklären. Dies würde die erwähnte Rechtszersplitterung beheben. Allerdings würden die Unsicherheiten in der Rechtsanwendung bestehen bleiben. Ausserdem würden die bestehenden Unbundlingvorschriften einen breiten Einsatz von Meter-Daten verunmöglichen.

Sektorspezifische gesetzliche Regelung: Dieser Lösungsansatz würde ebenfalls das Problem der Rechtszersplitterung lösen. Durch eine detailliertere Regelung könnten jedoch spezifische Regeln geschaffen werden, die die Rechtsanwendung erleichtern und eine einheitliche Praxis erlauben. Ausserdem könnte auf Gesetzesebene der Konflikt mit den Unbundlingvorschriften gelöst werden und die Problematik der Big Data gezielt angegangen werden. Hier ist jedoch zu beachten, dass je detaillierter die Vorschriften sind, desto eher laufen sie Gefahr, dass sie zukünftige innovative Businessmodelle und technischen Entwicklungen behindern. Bei diesem Lösungsansatz gilt es daher, eine Balance zwischen Rechtssicherheit in der Rechtsanwendung und Flexibilität mit Bezug auf heute noch nicht bekanntes Entwicklungspotenzial zu finden. Zudem ist die Frage des Verhältnisses der sektorspezifischen Regelung zum bundesrechtlichen Datenschutzgesetz zu beantworten (z.B. ergänzende Anwendung des DSG als Ganzes oder Anwendung der spezifischen DSG-Bestimmungen). Die ergänzende Anwendung des DSG würde allenfalls einer detaillierten sektorspezifischen Regelung die notwendige Flexibilität verleihen sowie die Regelung bestimmter Aspekte erleichtern (z.B. Rolle des Eidgenössischen Datenschutzbeauftragten, Informations- und Auskunftsrechte der Betroffenen etc.).

Selbstregulierung: Eine ausschliessliche Selbstregulierung ist aufgrund der geschilderten Rechtslage (Anwendbarkeit der Datenschutz- und Stromversorgungsgesetzgebung) kaum zielführend. Einheitliche Standards der involvierten Branchen können jedoch sinnvolle Ergänzungen zur staatlichen Regulierung darstellen. Der Gesetzgeber ist hier gehalten zu entscheiden, ob für spezifische Themen Branchenstandards für verbindlich erklärt werden können. Mit Bezug auf die Datenschutzthematik bietet sich dies insbesondere im Bereich der Datensicherheit und den entsprechenden technischen Normen an.

Zentrale Datenverwaltung: In Grossbritannien übernimmt die Data Communication Company (DCC) die Koordination zwischen den intelligenten Messgeräten und den zuvor von dieser lizenzierten Nutzern der Messdaten. Die DCC darf personenbezogene Daten nur verarbeiten, wenn dies mit dem Zweck in der DCC-Lizenz vereinbar ist. Sie muss

Massnahmen für die Datensicherheit treffen und die Nutzer bei der Einhaltung der Vorgaben im Bereich Datenschutz unterstützen. Eine solche zentrale Stelle für die Datenbearbeitung stellt eine einheitliche Praxis sicher und erhöht die Rechtssicherheit sowohl auf der Seite der betroffenen Personen als auch auf der Seite der Datennutzer. Allerdings ist ein solches System schwerfällig und stellt sicherheitstechnisch ein "Klumpenrisiko" dar. Die Auswahl und die Aufgaben und Befugnisse einer solchen zentralen Stelle müssten darüber hinaus auf Gesetzesebene (Gesetz im formellen Sinne) geregelt werden.

6.7.2. Rollout und Datenschutz

6.7.2.1. Schlussfolgerung

Datenschutzthemen politisch und rechtlich von grosser Bedeutung: Die datenschutzrechtlichen Fragen bzw. der Grad ihrer Berücksichtigung können im Zusammenhang mit der Einführung von Smart Meters bzw. Smart Grid entscheidend sein für den Erfolg oder Misserfolg des Rollouts von Smart Meters und damit der Einführung des Smart Grids. Dies hat sie bspw. deutlich in Niederlande gezeigt, wo ein flächendeckendes, verpflichtendes Rollout aus Gründen des Datenschutzes gescheitert ist.

6.7.2.2. Lösungsansätze

Flächendeckendes und verpflichtendes Rollout: Insbesondere bei einem flächendeckenden und verpflichtenden Rollout dürfen die datenschutzrechtlichen Themen nicht zu kurz kommen. Das flächendeckende und verpflichtende Rollout von Smart Meters ist in den Niederlanden daran gescheitert, dass im Standardisierungsprozess vor allem kommerzielle und technische Aspekte berücksichtigt worden sind. Die Interessen der Konsumenten, wie der Schutz der Privatsphäre, sind jedoch weitgehend vernachlässigt worden, worauf der Rollout in der Gesellschaft auf grossen Widerstand gestossen ist. Dies äusserte sich z.B. in der Weigerung vieler Bürger, einen Smart Meter einbauen zu lassen. Dieser Widerstand hat zu einer Gesetzesrevision geführt, welche den verpflichtenden Rollout von Smart Metern wieder aufhob.

Marktgetriebener Rollout (Opt-in): Der Botschaft zum ersten Massnahmenpaket der Energiestrategie 2050 ist zu entnehmen, dass es grundsätzlich auch denkbar wäre, den Rollout dem Markt zu überlassen.[199] Zu denken wären etwa an sog. opt-in Modelle. Solche freiwillige Rollouts sind aus datenschutzrechtlicher Sicht weniger kritisch, da die Endverbraucher in die Installation von Smart Meters ausdrücklich einwilligen. Nach Treu und Glauben kann davon ausgegangen, dass sie mit dem Wunsch, Smart Meter installieren zu lassen, auch in die damit zusammenhängende Bearbeitung von Daten einwilligen. Allerdings ist hier zu beachten, dass der Netzbetreiber bzw. ein Drittanbieter die Daten nur zu dem Zweck bearbeiten darf, zu welchem der Endverbraucher unter Berücksichtigung der Umstände auch zugestimmt hat. Die darüber hinausgehende Bearbeitung von Daten bedarf auch hier eines Rechtfertigungsgrundes (überwiegendes privates oder öffentliches Interesse, gesetzliche Vorschrift).

Opt-out-Modelle: Einen Mittelweg stellen sogenannte opt-out-Modelle dar. Demnach ist der Netzbetreiber zur flächendeckenden Installation von Smart Meters verpflichtet, die Endkunden könnten jedoch die Installation ablehnen. In solchen Fällen muss der Netzbetreiber ein herkömmliches Messgerät installieren. Diesen Weg haben z.B. Österreich und Grossbritannien gewählt. Insbesondere Österreich hat die Möglichkeit des Optingouts im Gesetz verankert, nachdem Proteste von verschiedenen Seiten (u.a. Mietervereinigung und Datenschutzrat) erfolgt sind. Dieses Modell erfordert eine differenzierte Regelung des Zwecks und der Berechtigung an Meter-Daten sowie der Voraussetzungen für

[199] *Bundesrat* (Anm.76), S. 157.

darüber hinausgehende Nutzung (z.B. ausdrückliche Einwilligung der Endkunden für bestimmte Verwendungen und/oder Granularitäten).

Bei der Wahl des Rollout-Modells sollten somit neben wirtschaftlichen und energiepolitischen auch datenschutzrechtliche Überlegungen eine wichtige Rolle spielen. Den dadurch entstehenden Interdependenzen ist dabei genügend Beachtung zu schenken. So wird bspw. zu berücksichtigen sein, dass auf Kundenseite der Anreiz einer Partizipation (bspw. durch ein opt-in) sehr wahrscheinlich im vergrösserten und verbesserten Dienstleistungsangebot liegen wird. Das Dienstleistungsangebot selbst wird indes davon abhängig sein, wie viele Kundinnen und Kunden am Rollout teilnehmen werden.

7. Beurteilung Datensicherheit und Datenschutz

7.1. Abrechnungsdaten

Verwendet in den Use Cases: 1

Beteiligte Rollen: Verteilnetzbetreiber, Energielieferant

7.1.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit sind die Abrechnungsdaten unkritisch.

Datensicherheit aus Gründen des Datenschutzes:

Aus Datenschutzgründen ist die Vertraulichkeit und die Integrität der Abrechnungsdaten kritisch, da diese nicht anonymisiert werden.

7.1.2. Datenschutzrechtliche Qualifikation der Daten

Bei Abrechnungsdaten handelt es sich um Daten für die Kundenrechnungsstellung wie Namen, Adressen, Angaben zur Bankverbindung usw. Sie stellen Informationen dar, welche eine Person bestimmen oder zumindest bestimmbar machen. Es handelt sich bei solchen Angaben um Personendaten gemäss Art. 3 lit. a DSG.

7.2. Abrufsignale

Verwendet in den Use Cases: 4

Beteiligte Rollen: Übertragungsnetzbetreiber, Verteilnetzbetreiber, SDV, Datenmanager, Erzeuger, Prosumer

7.2.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Die Abrufsignale sind bezüglich Integrität und Verfügbarkeit für die Versorgungssicherheit kritisch, da diese genau für diesen Zweck verwendet werden und falsche oder nicht vorhandene Daten im kritischen Zeitpunkt das Netz instabil machen können. Bezüglich der Vertraulichkeit wird davon ausgegangen, dass diese Daten unkritisch sind.

Datensicherheit aus Gründen des Datenschutzes:

Die Abrufsignale sind tendenziell nicht kritisch aus Sicht des Datenschutzes, da aus diesen Daten keine absoluten Nutzungsdaten eruiert werden können.

7.2.2. Datenschutzrechtliche Qualifikation der Daten

Die SDL Steuersignale werden heute zentral vom ÜNB übermittelt (Sekundärregelleistung, Tertiärregelleistung) oder direkt lokal eingestellt. Das Signal beinhaltet die Leistung, die im Kraftwerkt hoch-/runterzufahren ist. Damit das DSG anwendbar auf diesen Daten-

typ ist, müssten aus der hoch- bzw. runterzufahrenden Leistung Rückschlüsse auf bestimmte bzw. bestimmbare natürliche oder juristische Personen gezogen werden können. Dies ist grundsätzlich nicht auszuschliessen und wird von der konkreten Ausgestaltung des Use Cases abhängig sein. Die derzeitigen Unsicherheiten über die Ausgestaltung dieses Use Cases erlauben somit vorliegend keine abschliessende Qualifikation der Daten.

7.3. Angebote SDL

Verwendet in den Use Cases: 4

Beteiligte Rollen: Übertragungsnetzbetreiber, Verteilnetzbetreiber, SDV

7.3.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Die Vertraulichkeit und Integrität der SDL Angebote ist für die Versorgungssicherheit tendenziell kritisch, da falsche Daten in kritischen Situationen zu falschen Abrufsignalen führen könnten.

Datensicherheit aus Gründen des Datenschutzes:

Die SDL Angebote sind tendenziell kritisch aus Sicht der Vertraulichkeit und der Integrität, da aus diesen Angeboten Rückschlüsse auf den zukünftigen Bedarf gemacht werden könnten (erhöhtes Angebot aufgrund von Abwesenheiten / Ferien der Bewohner).

7.3.2. Datenschutzrechtliche Qualifikation der Daten

Der SDL-Verantwortliche (SDV) unterbreitet dem ÜNB die SDL-Angebote (evtl. als Aggregator für virtuelle Kraftwerke) und hält die zugeschlagenen SDL-Scheiben zwecks Leistungsvorhaltung fest. Die Rolle des SDV wird häufig durch den Handel wahrgenommen. Heute beinhalten die Angebote und Zuschläge eine Leistungsscheiben- und Preiskomponente (bspw. wie viel MW zu welchem Preis). Die Angebote stellen somit geschäftssensible Daten dar, die der SDV dem ÜNB übergibt. Es handelt sich somit um personenbezogene Daten.

7.4. Anreizsignale

Verwendet in den Use Cases: 2

Beteiligte Rollen: Energielieferant, Verteilnetzbetreiber, Prosumer, Datenmanager

7.4.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit ist die Verfügbarkeit der Anreizsignale als unkritisch einzustufen, da diese lediglich einen Anreiz darstellen und keine direkte Steuerung.

Die Integrität der Anreizsignale kann tendenziell als kritisch eingestuft werden, da in der Masse mit falschen Werten ein kritischer Zustand hervorgerufen werden könnte.

Datensicherheit aus Gründen des Datenschutzes:

Die Anreizsignale werden bezüglich des Datenschutzes als nicht kritisch eingestuft, da diese keine personenbezogenen Daten sind. Allenfalls könnten die Daten auf personenbezogenen Daten basieren, was zu einer erneuten Überprüfung der Datensicherheit führen würde.

7.4.2. Datenschutzrechtliche Qualifikation der Daten

Informationen und Signale werden den Kunden und Nutzern zur Verfügung gestellt, um Anreize zu schaffen, das Netz und die Energie optimal (im Verhältnis zum aktuellen Zustand) zu nutzen. Dies kann manuell oder automatisiert beim Kunden durchgeführt werden. Inhalt und Form der Daten ist noch nicht bestimmt. Fallweise könnte es sich um Verbrauchsstatistiken, Vergleichsdaten mit dem Verbrauchsdurchschnitt der Nachbarn etc. handeln. Solche Daten wären wahrscheinlich als personenbezogene Daten zu qualifizieren.

7.5. Aufbereitete Verbrauchsdaten

Verwendet in den Use Cases: 3

Beteiligte Rollen: Prosumer, Datenmanager, Dienstleister Gebäudeautomation

7.5.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Die Verbrauchsdaten sind für die Versorgungssicherheit bezüglich Vertraulichkeit, Integrität und Verfügbarkeit unkritisch.

Datensicherheit aus Gründen des Datenschutzes:

Für den Datenschutz können die aufbereiteten Verbrauchsdaten kritisch sein bezüglich Vertraulichkeit und Integrität. Die Kritikalität ist abhängig von der Art der Aufbereitung der Daten und den daraus entstehenden Möglichkeiten personenbezogene Rückschlüsse zu ziehen.

7.5.2. Datenschutzrechtliche Qualifikation der Daten

Visualisierte bzw. einfach verständlich aufbereitete Verbrauchsdaten des Smart Meters bzw. von einzelnen Verbrauchsgeräten stellen potentielle personenbezogene Daten dar. Insbesondere die Daten von einzelnen Verbrauchsgeräten können, falls sie bspw. nur von einer bestimmten Person verwendet werden (etwa ein Dialysegerät für Zuhause), (besonders schützenswerte) personenbezogene Daten darstellen.

7.6. Bedrohungszustand

Verwendet in den Use Cases: 6

Beteiligte Rollen: Übertragungsnetzbetreiber, Verteilnetzbetreiber

7.6.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit sind die Vertraulichkeit, die Integrität und die Verfügbarkeit des Bedrohungszustands als kritisch einzustufen. Insbesondere bei einem potentiellen Angriff müssen die Daten korrekt und vollständig zur Verfügung stehen, um allfällige Massnahmen zu ergreifen.

Datensicherheit aus Gründen des Datenschutzes:

Die Relevanz aus Sicht Datenschutz lässt sich zu diesem Zeitpunkt noch nicht abschliessend beurteilen. Aus der heutigen Sicht wird angenommen, dass die Daten des Bedrohungszustandes keine personenbezogene Daten beinhalten und daher würden keine Datensicherheitsanforderungen aufgrund des Datenschutzes anfallen.

7.6.2. Datenschutzrechtliche Qualifikation der Daten

Unter Bedrohungszustand werden die Resultate der Risikoanalyse verstanden. Für die Bestimmung der Personenbezogenheit der Daten fehlen die notwendigen Informationen. Die derzeitigen Unsicherheiten über die Ausgestaltung dieses Use Cases erlauben vorliegend keine abschliessende Qualifikation der Daten.

7.7. Betriebsmittelzustand

Verwendet in den Use Cases: 7, 8, 9, 11, 12

Beteiligte Rollen: Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.7.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit könnte der Betriebsmittelzustand beim Verteilnetzbetreiber und beim Übertragungsnetzbetreiber tendenziell kritisch sein bezüglich Vertraulichkeit, Integrität und Verfügbarkeit. Schwachstellen in den Betriebsmitteln könnten durch Fremde genutzt werden, um die Versorgungssicherheit zu mindern.

Datensicherheit aus Gründen des Datenschutzes:

Aus Sicht des Datenschutzes kann davon ausgegangen werden, dass diese Daten Rückschlüsse auf die Persönlichkeit im Sinne eines Unternehmens zulassen.

7.7.2. Datenschutzrechtliche Qualifikation der Daten

Use Case 7, 8, 9

Die Zustandsdaten der Betriebsmittel werden jeweils innerhalb des Netzgebietes überwacht, um Fehler und den Netzzustand zu erkennen. Es handelt sich hier um Daten zu jedem Betriebsmittel und in welchem Zustand dieses ist wie Alter, Reparaturen etc. Bei den Daten zu den Betriebsmitteln könnte es sich allenfalls um personenbezogene Daten handeln, eine genaue Qualifikation setzt aber auch hier weitere Informationen voraus. Die derzeitigen Unsicherheiten über die konkrete Ausgestaltung dieses Use Cases erlauben vorliegend keine abschliessende Qualifikation der Daten.

Use Case 11

Die Zustandsgrössen von Betriebsmitteln können als Archivdaten aus einer Datenbank oder als Mess- und Steuerdaten der Betriebsmittel selbst zur Verfügung gestellt werden. Wie bereits zuvor erwähnt, können Daten zu den Betriebsmitteln allenfalls personenbezogene Daten darstellen, da aber auch hier das Format noch offen ist, müssen die weiteren Entwicklungen abgewartet werden, bevor der Datenfluss genauer qualifiziert werden kann.

Use Case 12

Um den Betriebsmittelzustand zu überwachen, werden Daten aus einer Datenbank, welche bei Ersatz und Wartung von Komponenten aktualisiert werden muss, verwendet. Hierbei könnten unter Umständen personenbezogene Daten von Unternehmen vorliegen. Die Datenbank könnte zudem eine Datensammlung i.S.v. Art. 3 lit. g DSG. darstellen. Es ist wiederum darauf zu verweisen, dass aufgrund der derzeitigen Offenheit des Formats eine abschliessende Qualifikation der Personenbezogenheit der Daten nicht möglich ist.

7.8. Daten Versorgungsqualität

Verwendet in den Use Cases: 8, 11

Beteiligte Rollen: Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.8.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Aus Sicht der Versorgungssicherheit sind die Daten zur Versorgungsqualität kritisch in der Vertraulichkeit, Integrität und Verfügbarkeit. Einerseits könnten durch Fremde die Versorgungssicherheit beeinträchtigt werden, wenn diese die Daten einsehen und evtl. ändern könnten. Andererseits ist die Verfügbarkeit der Daten für den laufenden Betrieb notwendig, um schnell auf Instabilitäten zu reagieren

Datensicherheit aus Gründen des Datenschutzes:

Aus Sicht des Datenschutzes sind die Daten zur Versorgungsqualität personenbezogene Daten im Sinne eines Unternehmens. Da die Daten voraussichtlich nur innerhalb eines Unternehmens zur Verfügung stehen, besteht kein zusätzlicher Datensicherheitsbedarf.

7.8.2. Datenschutzrechtliche Qualifikation der Daten

Die Versorgungsqualität ist die Kombination von Messwerten (aktuell oder aus dem Archiv), welche den Standards und deren Bandbreite sowie den Archivwerten gegenübergestellt werden. Das Kombinieren von Personendaten stellt eine Bearbeitung i.S.d. DSG dar, die derzeitigen Unsicherheiten über die Ausgestaltung der Use Cases erlauben indes vorliegend keine abschliessende Qualifikation der Daten.

7.9. Fehlerinformationen

Verwendet in den Use Cases: 6, 7, 9

Beteiligte Rollen: Erzeuger, Prosumer, Datenmanager, Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.9.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Je nach Use Case können die Fehlerinformationen für die Versorgungssicherheit bezüglich der Vertraulichkeit, der Integrität und der Verfügbarkeit kritisch eingestuft werden. So sollten bei einem Bedrohungszustand (Use Case 6) oder bei grossflächigen Fehlern / Ausfälle (Use Case 7) die Fehlerinformationen korrekt und verfügbar sein. Zusätzlich ist sollte in einem Bedrohungszustand die Vertraulichkeit gegenüber fremden gewährleistet sein, um das Netz zusätzlich vor Angriffen zu schützen.

Datensicherheit aus Gründen des Datenschutzes:

Die Relevanz der Fehlerinformationen aus Sicht Datenschutz ist bei den Daten von den Prosumern gegeben. Bei diesen Daten sollte die Vertraulichkeit und Integrität als kritisch eingestuft werden.

7.9.2. Datenschutzrechtliche Qualifikation der Daten

Die Fehlerinformationen müssen auch Informationen zu Daten enthalten, damit ein allfälliger Schwachpunkt erkennt werden kann. Für die Bestimmung der Personenbezogenheit der Daten fehlen die notwendigen Informationen. Die derzeitigen Unsicherheiten über die konkrete Ausgestaltung dieses Use Cases erlauben vorliegend keine abschliessende Qualifikation der Daten.

7.10. Flexibilisierungsoptionen Ein-/ Ausspeisung

Verwendet in den Use Cases: 10, 12

Beteiligte Rollen: Erzeuger, Prosumer, Datenmanager, Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.10.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Die Flexibilisierungsoptionen sind für die Versorgungssicherheit tendenziell bezüglich deren Integrität kritisch, da falsche Daten (wenn z.B. grossflächig manipuliert) falsche Regelungen auslösen könnten und das Netz in einen Instabilen Zustand bringen könnte.

Datensicherheit aus Gründen des Datenschutzes:

Die Flexibilisierungsoptionen sind aus Datenschutzsicht tendenziell kritisch, falls sie Rückschlüsse auf Personen zulassen. Insbesondere beim Prosumer ist denkbar, dass die Flexibilisierungsoptionen Rückschlüsse auf An- / Abwesenheiten und Grössenordnungen des Stromverbrauchs zulassen (z.B. mehr Flexibilität bei Abwesenheit oder mit einem Elektroauto / grossen Batterien).

7.10.2. Datenschutzrechtliche Qualifikation der Daten

Aus den gesammelten und aufbereiteten Daten können zeitlich flexible Energieflüsse (Ein- und Ausspeisepunkte) auf Grund des Netzzustandes optimiert werden. Die Optionen sollen Profile darstellen, wie die Lastflüsse gestaltet werden können. Auch hier handelt es sich um ein neues Format, die Ausgestaltung bzw. das Format der Daten ist also zurzeit noch offen, weshalb keine datenschutzrechtliche Qualifizierung vorgenommen werden kann.

7.11. Historische Onlinedaten

Verwendet in den Use Cases: 11, 12

Beteiligte Rollen: Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.11.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Die historischen Onlinedaten sind aus Versorgungssicherheitsgründen kritisch bezüglich Integrität, da diese für Berechnungen verwendet werden, welche die Versorgungssicherheit betreffen.

Datensicherheit aus Gründen des Datenschutzes:

Da die historischen Onlinedaten voraussichtlich nicht zwischen den Rollen ausgetauscht werden, sind diese für den Datenschutz unkritisch.

7.11.2. Datenschutzrechtliche Qualifikation der Daten

Use Case 11

Die Historie der Onlinedaten der Ein- und Ausspeisung wird innerhalb des Netzgebietes genutzt, um den Einsatz der Betriebsmittel zu planen. Eine abschliessende Qualifikation der Personenbezogenheit der Daten ist vorliegend aufgrund der noch offenen Ausgestaltung der Use Cases nicht möglich.

Use Case 12

Die Historie der Messdaten der Ein- und Ausspeisung wird innerhalb des Netzgebietes und aggregiert von anderen Netzgebieten genutzt, um die Flexibilität zu Berechnen. Bei der Frage, ob es sich bei den aggregierten Daten um personenbezogene Daten handelt, ist von Bedeutung, in welchem Grad die Daten anonymisiert worden sind (K-Anonymität), bzw. ob noch Rückschlüsse auf die einzelnen Datensätze bzw. Personen (eventuell in Verbindung mit anderen Datenbanken) gezogen werden können. Zu beachten gilt hier, dass das Anonymisieren von personenbezogenen Daten als Bearbeitung i.S.d. DSG verstanden wird.

7.12. Instandhaltungs-Massnahmen

Verwendet in den Use Cases: 9, 11

Beteiligte Rollen: Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.12.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Die geplanten Instandhaltungs-Massnahmen sind tendenziell lediglich aus Sicht der Integrität kritisch, da falsche Daten zu falschen Annahmen und Berechnungen führen könnten, welche zu falschen Massnahmen und geringerer Versorgungssicherheit führen könnten.

Datensicherheit aus Gründen des Datenschutzes:

Die Instandhaltungs-Massnahmen können gegebenenfalls zwischen den Rollen Verteilnetzbetreiber und Übertragungsnetzbetreiber ausgetauscht werden. In diesem Fall würden die Daten unter dem Datenschutzgesetz im Sinne der Unternehmensdaten fallen und müssten zusätzlich geschützt werden.

7.12.2. Datenschutzrechtliche Qualifikation der Daten

Historische Instandhaltungs-Massnahmen

Die historischen Daten werden innerhalb des Netzgebietes genutzt. Das Format dieser Daten ist zurzeit noch völlig offen, für die Bestimmung der Personenbezogenheit der Daten müssen somit die künftigen Entwicklungen abgewartet werden.

Geplante Instandhaltungs-Massnahmen

Die geplanten Instandhaltungsdaten werden sowohl innerhalb des Netzgebietes als auch netzgebietsübergreifend übermittelt. Das Format dieser Daten ist zurzeit noch völlig offen, für die Bestimmung der Personenbezogenheit der Daten müssen somit die künftigen Entwicklungen abgewartet werden.

7.13. Konfigurationsdaten

Verwendet in den Use Cases: 1

Beteiligte Rollen: Prosumer

7.13.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Die Konfigurationsdaten der Prosumer sind für die Versorgungssicherheit unkritisch.

Datensicherheit aus Gründen des Datenschutzes:

Aus Datenschutzgründen sind die Vertraulichkeit und die Integrität der Konfigurationsdaten möglicherweise kritisch, weil sie Rückschlüsse auf personenbezogene Daten zulassen könnten.

7.13.2. Datenschutzrechtliche Qualifikation der Daten

Konfigurationsdaten stellen Passwörter, Verschlüsselungscodes etc. dar. Diese Daten sind insbesondere im Zusammenhang mit Art. 7 DSG von Bedeutung. Gemäss Art. 7 Abs. 1 DSG müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Auch die Konfigurationsdaten des Smart Meters müssen somit entsprechend vor Missbrauch geschützt werden.

7.14. Kundendaten

Verwendet in den Use Cases: 1

Beteiligte Rollen: Datenmanager, Verteilnetzbetreiber, Energielieferant, Weitere Marktpartner

7.14.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit sind die Kundendaten unkritisch.

Datensicherheit aus Gründen des Datenschutzes:

Aus Datenschutzgründen sind die Vertraulichkeit und die Integrität der Kundendaten kritisch, weil es sich um personenbezogene Daten handelt.

7.14.2. Datenschutzrechtliche Qualifikation der Daten

Hierbei handelt es sich insbesondere um Angaben zu einer Person, Vertragsdaten, Messpunkte etc. Diese Daten scheinen zumindest die Bestimmbarkeit einer Person zu ermöglichen, in bestimmten Fällen können Personen auch direkt bestimmt werden. Es handelt sich dabei in der Regel um Personendaten gemäss Art. 3 lit. a DSG.

7.15. Marktinformationen

Verwendet in den Use Cases: 2

Beteiligte Rollen: Energielieferant, Datenmanager, Prosumer

7.15.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit ist die Verfügbarkeit aller Daten als unkritisch einzustufen.

Die Integrität der Marktinformationen ist tendenziell als kritisch einzustufen, da in der Masse (grossflächig) mit falschen Werten ein kritischer Netzzustand hervorgerufen werden könnte. Die Verfügbarkeit und Vertraulichkeit der Marktdaten im hier beschriebenen Sinn ist unkritisch bezüglich der Versorgungssicherheit.

Datensicherheit aus Gründen des Datenschutzes:

Die Marktinformationen werden bezüglich des Datenschutzes als nicht kritisch eingestuft, da diese keine personenbezogenen Daten sind.

7.15.2. Datenschutzrechtliche Qualifikation der Daten

Marktinformationen sind Informationen zu Preisen und Marktentwicklungen, welche dem Kunden zur Verfügung gestellt werden. Es ist zurzeit noch offen, welche Daten der Dienstleistungserbringer definieren bzw. erbringen will. Handelt es sich um öffentlich zugängliche Informationen wie Preise oder Marktentwicklungen, ist davon auszugehen, dass die Bearbeitung dieser Daten, auch wenn sie personenbezogen sind, aus dem datenschutzrechtlichen Blickwinkel unproblematisch ist.

7.16. Messwerte Endgeräte

Verwendet in den Use Cases: 3

Beteiligte Rollen: Prosumer, Datenmanager, Dienstleister Gebäudeautomation

7.16.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Aus Sicht der Versorgungssicherheit kann die Integrität der Messwerte der Endgeräte kritisch sein, insbesondere wenn aufgrund deren an eine grössere Anzahl von Gebäudeautomationen gleichzeitig falsche Steuersignale gesendet werden.

Die Verfügbarkeit und Vertraulichkeit dieser Daten ist für die Versorgungssicherheit unkritisch.

Datensicherheit aus Gründen des Datenschutzes:

Für den Datenschutz sind die Messwerte der Endgeräte als kritisch einzustufen, hinsichtlich deren Vertraulichkeit und Integrität, da Rückschlüsse auf personenbezogene Daten möglich sind.

7.16.2. Datenschutzrechtliche Qualifikation der Daten

Es handelt sich hier um aktuelle und historische Messdaten von Endgeräten des Prosumers, für beliebige zukünftige Anwendungszwecke im Smart-Home. Es ist davon auszugehen, dass gewisse Endgeräte nur von bestimmten Personen verwendet werden (bspw. ein Beatmungsgerät). Daher ist es wahrscheinlich, dass es sich bei diesen Daten auch um besonders schützenswerte Personendaten oder Persönlichkeitsprofile handeln könnte. Dies deshalb, weil ein persönlichkeitsbezogener Datensatz genügt, damit die gesamte Datensammlung als personenbezogen qualifiziert wird.

7.17. Meteringdaten

Verwendet in den Use Cases: 1, 2, 3, 5, 8

Beteiligte Rollen: Prosumer, Datenmanager, Verteilnetzbetreiber, Energielieferant, Weitere Marktpartner, Dienstleister Gebäudeautomation, Erzeuger

7.17.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit sind die Meteringdaten unkritisch, sofern es sich um reine Messwerte zu Abrechnungszwecken und statistische Zwecke handelt und sie nicht zur direkten Berechnung von Netzzuständen und Schaltungen / Steuerungen führen. Bei der Berechnung von Prognosewerte aus den Meteringdaten ist es wichtig diese zu verifizieren und plausibilisieren, damit keine unerwünschten Netzzustände entstehen.

Datensicherheit aus Gründen des Datenschutzes:

Aus Datenschutzgründen ist die Vertraulichkeit und die Integrität der personenbezogenen Meteringdaten kritisch, d.h. ausser diese werden aggregiert und anonymisiert. Für weiterführende Arbeiten soll der in der Branche verwendete 15-Minuten Wert angestrebt werden. Dieser ist unter Umständen noch nicht genügend aggregiert (An- und Abwesenheiten).

7.17.2. Datenschutzrechtliche Qualifikation der Daten

Zu prüfen ist, ob es sich bei den Meteringdaten und historischen Meteringdaten um personenbezogene Daten handelt oder nicht. Hierzu muss geklärt werden, welche Informationen durch Auslesung der Smart Meter-Daten in welcher Granularität gewonnen werden können.

Einige Beispiele sollen die Möglichkeiten aufzeigen: Gemäss verschiedener Autoren besteht die Möglichkeit, insbesondere Tagesabläufe wiederzugeben (inklusive wann jemand im Haus bzw. wann das Haus leer ist, wann die Hausbewohner am Schlafen sind usw.), ob das Haus mit einer Alarmanlage ausgerüstet ist, ob teure elektronische Geräte wie Plasmafernseher oder Waschmaschinen verwendet werden oder ob gewisse medizinische Geräte im Einsatz stehen.[200] Auch können gemäss verschiedenen Literaturstellen Aussagen darüber getroffen werden, wie viele Personen sich zu einer gewissen Zeit in einem Gebäude befinden und ob dies mehr Personen als üblich sind.[201] Detaillierte Aussagen scheinen bei Einpersonenhaushalten möglich zu sein. Aufgrund des Energieverbrauchs können spezifische Aktivitäten und Handlungsmuster beobachtet werden, etwa wann und ob diese Person duscht, u.U. ob sie sich rasiert oder die elektronische Zahnbürste benutzt, ob die Person selbst kocht oder eine Mikrowelle verwendet, wann sie den Kühlschrank benützt, ja selbst Aussagen zu Fahrrouten (vorausgesetzt, ein Elektrofahrzeug wird verwendet) scheinen möglich zu sein.[202] Da das DSG nicht nur private, sondern auch Daten von juristischen Personen schützt, sind diesbezüglich weitere personenbezogene Daten, wie Angaben zu Herstellungs- und Produktionsverfahren sowie weitere Betriebs- und Geschäftsgeheimnisse, denkbar.[203] Das US-Department of Energy (US-DoE) geht indes in einem Bericht vom Oktober 2010 davon aus, dass "*the current state of the art, in terms of the granularity of data collected by utilities using advanced metering, cannot yet identify individual appliances and devices in the home in detail*".[204] Die Aussage wird jedoch insofern relativiert, indem anschliessend festgehalten wird, "*but this will certainly be within the capabilities of subsequent generations of Smart Grid technologies*."[205]

Unter der Voraussetzung, dass solch detaillierte Informationen in der Zukunft möglich sein werden, handelt es sich dabei um Angaben, welche unter dem DSG erfasste Tatsachenfeststellungen darstellen können.[206] Schwieriger zu beurteilen ist, ob sich diese Angaben auf eine bestimmte oder bestimmbare Person beziehen. Denn das Smart-Meter-Gerät misst grundsätzlich nur den Energieverbrauch eines Haushaltes (bei Privatpersonen) bzw. eines Gebäudes oder einer Anlage (bei Unternehmen). Experten bezweifeln daher, dass derzeit und in naher Zukunft Meteringdaten detaillierte Aussagen über das individuelle Verhalten zulassen.[207] Andere wissenschaftliche Untersuchen zeigen relativ deutlich, dass nur sehr wenige Informationen aus Messwerten mittlerer Zeitdauer (mehrere Minuten) gewonnen werden können.[208] Da in einem Haushalt mitunter eine Vielzahl

---

200 *U.S. Department of Energy*, Data Access and Privacy Issues Related to Smart Grid Technologies, 2010, S. 2.

201 *U.S. Department of Commerce* (Anm. 42), S. 11.

202 Vgl. *Quinn*, Smart Metering & Privacy: Existing Law and Competing Policies: A Report for the Colorado Public Utilities Commission, 2009, S. 3, 9; *Kohlen*, Belkin-Sensor analysiert Stromverbrauch von Elektrogeräten, 2013, abrufbar unter: <http://www.itespresso.de/2013/08/12/belkin-sensor-analysiert-stromverbrauch-von-geraten/>.

203 Vgl. *U.S. Department of Commerce* (Anm. 42), S. 18; vgl. auch *Verband Schweizerischer Elektrizitätsunternehmen*, Branchenempfehlung Strommarkt Schweiz, Metering Code Schweiz, 2012, S. 34, abrufbar unter: <http://www.strom.ch/uploads/media/MC-CH_2012_D_01.pdf>.

204 *U.S. Department of Energy* (Anm. 200), S. 9.

205 *U.S. Department of Energy* (Anm. 200), S. 9.

206 Vgl. *Belser* (Anm. 18), Art. 3 N. 5.

207 In der Begleitgruppe des BFE zu diesem Bericht (Sitzung vom 30. Oktober 2013 in Ittingen) wurde darauf hingewiesen, dass es weder heute noch in naher Zukunft möglich sein wird, mit Hilfe von Meteringdaten detaillierte Informationen über die betroffenen Personen zu gewinnen.

208 *Christian Beckel, Leyna Sadamori, Silvia Santini (ETH Zurich and TU Darmstadt)*, Automatic Socio-Economic Classification of Households Using Electricity Consumption Data, 2013; *Wilhelm Kleiminger, Christian Beckel, Thorsten Staake, Silvia Santini*, Occupancy Detection from Electricity Consumption Data, 2014

von Personen lebt, stellt sich die Frage, ob die Daten einer bestimmten bzw. bestimmbaren Person zuordenbar sind. Die Frage ist bei einem Einpersonenhaushalt wohl zu bejahen. Auch bei einem Zweipersonenhaushalt ist davon auszugehen, dass aufgrund der jeweils individuellen Verhaltens- und Handlungsmuster die Identifikation einer Person durch die Kombination der gewonnen Daten möglich scheint.[209] Bei grossen Wohngemeinschaften (bspw. ein Studentenwohnheim mit regelmässig wechselnden Mietern) wird jedoch der Aufwand zur Identifizierung sehr wahrscheinlich derart gross sein, dass nach heutigem Stand der Technik und der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird; die Bestimmbarkeit einzelner Personen ist deshalb dort zu verneinen.[210]

Aufgrund der Rechtsprechung des Bundesgerichts könnte die Zuordnung jedoch grundsätzlich vernachlässigt werden. Bezüglich einer Sammlung von IP-Adressen und der daraus möglichen Bestimmbarkeit von einzelnen Personen hielt das Bundesgericht nämlich fest, dass in vielen Fällen die dahinter stehende Person nicht ausfindig gemacht werden könne, insbesondere dann, wenn verschiedene Personen zu einem Computer oder einem Netzwerk Zugang hätten. Dem Gericht erschien es aber als ausreichend, dass die Bestimmbarkeit in Bezug auf einen Teil der von der Beschwerdegegnerin gespeicherten Informationen gegeben ist und qualifizierte deshalb die von der Beschwerdegegnerin bearbeiteten IP-Adressen als Personendaten i.S.v. Art. 3 lit. a DSG.[211] Der Entscheid wurde in BGE 138 II 346 E. 6.1 bestätigt, wo das Bundesgericht ausführte, dass "*[…] die Bestimmbarkeit zu bejahen [ist], wenn sie sich zumindest auf einen Teil der gespeicherten Informationen bezieht.*" Dieser Rechtsprechung folgend ist davon auszugehen, dass eine Sammlung mit Meteringdaten, unter der Bedingung, dass die oben beschriebenen Informationen tatsächlich ermittelbar sind, wohl insgesamt als personenbezogene Datensammlung zu qualifizieren ist.

Die Meteringdaten können in Meteringdaten (mit periodischer Übertragung) und historische Daten unterteilt werden. Dabei ist zu beachten, je regelmässiger und detaillierter Daten übertragen werden, desto eher können nicht nur personenbezogene Daten, sondern auch besonders schützenswerte Personendaten und Persönlichkeitsprofile gemäss Art. 3 lit. c und d DSG vorliegen. Dasselbe gilt hinsichtlich historischer Daten, je länger der Zeitraum der Speicherung und je grösser die Menge an gesammelten Daten, desto eher werden besonders schützenswerte Personendaten und Persönlichkeitsprofile generiert.

7.18. Monitoringdaten

Verwendet in den Use Cases: 4

Beteiligte Rollen: Übertragungsnetzbetreiber, SDV, Datenmanager

7.18.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Die Integrität der Monitoringdaten ist für die Versorgungssicherheit tendenziell kritisch, da falsche Daten in kritischen Situationen zu falschen Abrufsignalen führen könnten. Die Vertraulichkeit und Verfügbarkeit sind etwas weniger kritisch für die Versorgungssicherheit.

[209] Vgl. *Belser* (Anm. 18), Art. 3 N. 6.
[210] Vgl. BGE 138 II 346, E. 6.1; BVGer A-7040/2009 vom 30. März 2011, E. 7.2.
[211] BGE 136 II 508, E. 3.5 und. E. 3.8.

Datensicherheit aus Gründen des Datenschutzes:

Die Monitoringdaten sind aus Sicht des Datenschutzes unkritisch, da es sich nicht um personenbezogene Daten handelt.

7.18.2. Datenschutzrechtliche Qualifikation der Daten

Die Vorhaltung der SDL bei den teilnehmenden Anlagen soll vom SDV und dem Übertragungsnetzbetreiber laufend überwacht werden. Die hierfür benötigten Daten enthalten die aktuell abrufbare Leistung und je nach Regelleistung (primär, sekundär, tertiär) Angaben zum Arbeitspunkt und zur momentanen Leistung der teilnehmenden Erzeugungseinheit (bspw. einer Turbine). Die Überwachung solcher u.U. geschäftssensibler Unternehmensdaten durch den SDV und den Übertragungsnetzbetreiber stellt eine Bearbeitung von personenbezogenen Daten gemäss DSG dar.

7.19. Netzauslastung

Verwendet in den Use Cases: 5, 7, 8, 9, 10, 11, 12

Beteiligte Rollen: Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.19.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit sind die Daten der Netzauslastung bezüglich Vertraulichkeit, Integrität und Verfügbarkeit kritisch. Da diese durch Fremde missbraucht werden könnten und die Netzstabilität beeinträchtigen könnten.

Datensicherheit aus Gründen des Datenschutzes:

Aus Datenschutzgründen ist die Netzauslastung nicht kritisch, da diese Daten nicht zwischen den Rollen ausgetauscht werden.

7.19.2. Datenschutzrechtliche Qualifikation der Daten

Use Case 5, 10, 11, 12

Die Zustandsdaten der Netzauslastung werden jeweils innerhalb der Netzgebiete überwacht, um regionale Flexibilitäten zu erkennen. Das Format ist hier noch offen, eine abschliessende Qualifikation der Personenbezogenheit der Daten ist somit noch nicht möglich. Normalerweise handelt es sich um rein interne Netzbetreiberdaten, es werden also keine Daten von anderen Personen bearbeitet. Das DSG gelangt, falls die Daten nur intern verwendet werden, nicht zur Anwendung.[212]

Use Case 7, 8

Die aktuelle Netzauslastung wird innerhalb des Netzgebietes und an den Schnittstellen zu anderen Netzgebieten überwacht. Eine abschliessende Qualifikation der Daten ist auch hier aufgrund der derzeitigen Unsicherheiten über die Ausgestaltung der einzelnen Use Cases nicht möglich.

[212] Anwendung findet das DSG nur, soweit Daten von anderen natürlichen oder juristischen Personen bearbeitet werden. Nicht in den Anwendungsbereich des DSG fällt somit, wer nur Personendaten über sich selbst bearbeitet, *Jöhri/Rosenthal* (Anm. 18), Art. 2 N. 13.

Use Case 9, 10, 11, 12

Die aktuellen und historischen Daten werden innerhalb des Netzgebietes genutzt. Durch die historischen Netzauslastungen können ausserordentliche Situationen und Statistiken ausgewertet werden. Durch die Kombination von historischen Daten mit aktuellen Daten erhöht sich die Wahrscheinlichkeit, dass die Netzauslastungsdaten personenbezogene Daten der Verteilnetzbetreiber darstellen, da diese Daten einen solchen Betreiber unter Umständen bestimmen bzw. bestimmbar machen. Ebenfalls eine Rolle spielt, insbesondere bei den historischen Daten, ob diese aggregiert bzw. anonymisiert werden. Eine abschliessende Qualifikation der Personenbezogenheit der Daten ist aufgrund der noch offenen Ausgestaltung der Use Cases nicht möglich. Sollten diese Daten nur intern genutzt werden, würde dies die Anwendbarkeit des DSG ausschliessen.

7.20. Netzbauplanung

Verwendet in den Use Cases: 11, 12

Beteiligte Rollen: Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.20.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Die Daten der Netzbauplanung sind aus Versorgungssicherheitsgründen möglicherweise kritisch bezüglich deren Integrität, da falsche Daten zu falschen Berechnungen und Massnahmen führen könnten

Datensicherheit aus Gründen des Datenschutzes:

Aus Datenschutzgründen sind die Daten der Netzbauplanung kritisch. Das Sammeln und Aufbereiten dieser Daten durch Dritte kann eine Bearbeitung von personenbezogenen Daten im Sinne der Unternehmensdaten darstellen.

7.20.2. Datenschutzrechtliche Qualifikation der Daten

Aus den gesammelten und aufbereiteten Daten können die Dimensionierung der Betriebsmittel berechnet und die Netztopologie optimiert werden. Diese Daten stellen aus Sicht der Unternehmen geschäftssensible Daten (wie bspw. Vorhabensplanungen für den Netzausbau) dar. Das Sammeln und Aufbereiten dieser Daten durch Dritte stellt somit eine Bearbeitung von personenbezogenen Daten dar.

7.21. Netzkonfiguration

Verwendet in den Use Cases: 5, 6, 7, 8, 9, 10, 11, 12

Beteiligte Rollen: Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.21.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit sind die Daten der Netzkonfiguration bezüglich Vertraulichkeit, Integrität und Verfügbarkeit kritisch, da diese durch Fremde missbraucht werden könnten und die Netzstabilität beeinträchtigen könnten.

Datensicherheit aus Gründen des Datenschutzes:

Aus Datenschutzgründen ist die Netzkonfiguration nicht kritisch, da diese Daten nicht zwischen den Rollen ausgetauscht werden.

7.21.2. Datenschutzrechtliche Qualifikation der Daten

Dies sind Daten zur aktuellen Konfiguration des Netzes und seiner Betriebsmittel. Sie beinhalten die gesamte Netztopologie, d.h. sämtliche Betriebsmittel mit ihren Konfigurationen. Diese Daten sind geschäftssensibel. Normalerweise stellen auch diese Daten rein interne Netzbetreiberdaten dar. Werden die Daten nicht nur intern vom Netzbetreiber verwendet, gelangt das DSG zur Anwendung.

7.22. Onlinedaten Ein- / Ausspeisung

Verwendet in den Use Cases: 4, 5, 7, 8, 9

Beteiligte Rollen: Verteilnetzbetreiber, Übertragungsnetzbetreiber, SDV

7.22.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit sind die Onlinedaten unkritisch bezüglich der Vertraulichkeit. Bezüglich der Verfügbarkeit und Integrität sind die Onlinedaten tendenziell weniger kritisch für die Versorgungssicherheit.

Datensicherheit aus Gründen des Datenschutzes:

Die Onlinedaten Ein-/Ausspeisung sind tendenziell unkritisch aus Sicht des Datenschutzes, da sie nicht unter den Rollen ausgetauscht werden.

7.22.2. Datenschutzrechtliche Qualifikation der Daten

Use Case 4,5, 9

Die aktuelle Last und Erzeugung muss bekannt sein, um die vorgehaltene Leistung zu überwachen (Onlinedaten). Der Übertragungsnetzbetreiber (ÜNB) bzw. die Swissgrid überwacht dabei das Randintegral der Regelzone, der Systemdienstleitungs-Anbieter (SDL-Anbieter) die Kapazitäten "seiner" Anlagen (evtl. in einem Pool) sowie der Verteilnetzbetreiber (VNB) sein Netz (zwecks Notübersteuerung der SDL-Kraftwerke). Diese Messdaten sind im Wesentlichen Leistungsangaben (Einspeisung/Ausspeisung) entlang der Zeit. Hier können insbesondere die Kapazitäten der Anlagen der SDL-Anbieter und die Netzdaten der VNB personenbezogene Daten darstellen.

Use Case 7

Die aktuelle Last und Erzeugung muss bekannt sein, um Fehler zu beheben. Diese Daten werden innerhalb des Netzgebietes und wahrscheinlich aggregiert zwischen den Netzgebieten übermittelt. Bei der Frage, ob es sich bei den aggregierten Daten um personenbezogene Daten handelt, ist von Bedeutung, zu welchem Grad die Daten anonymisiert worden sind (K-Anonymität), bzw. ob noch Rückschlüsse auf die einzelnen Datensätze resp. Personen (eventuell in Verbindung mit anderen Datenbanken) gezogen werden können.

Use Case 8, 9

Die Einspeiseleistung und Spannung an den Einspeisepunkten wird. innerhalb des Netzgebietes und sehr wahrscheinlich aggregiert netzgebietübergreifend überwacht. Vorliegend ist aufgrund der derzeitigen Unsicherheiten über die Ausgestaltung der einzelnen Use Cases keine abschliessende Qualifikation der Personenbezogenheit der Daten möglich ist.

7.23. Prognosedaten

Verwendet in den Use Cases: 1, 10, 11, 12

Beteiligte Rollen: Verteilnetzbetreiber, Übertragungsnetzbetreiber, Energielieferant

7.23.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit sind die Prognosedaten tendenziell unkritisch, da ohnehin mit einer gewissen Unschärfe gerechnet werden muss und durch die heute angenommene Regelmässigkeit auch veraltete Daten für den stabilen Betrieb in der Regel ausreichen.

Datensicherheit aus Gründen des Datenschutzes:

Die Prognosedaten für Netz und Energie sind in den meisten Fällen aggregiert und nicht personenbezogen und werden daher in diesen Fällen für die Datensicherheit als unkritisch eingestuft.

7.23.2. Datenschutzrechtliche Qualifikation der Daten

Prognosedaten Energie

Use Case 1

Bei den Prognosedaten Energie handelt es sich um Daten für Energiebeschaffung und Preisberechnungen. Es gibt sowohl personenbezogene Prognosedaten (der Lieferant prognostiziert einen einzelnen (Gross-)Kunden), als auch aggregierte Prognosen über alle oder Gruppen von Kleinkunden. Bei den Daten der einzelnen Kunden handelt es sich grundsätzlich um personenbezogene Daten. Bei der Frage, ob es sich bei den aggregierten Daten um personenbezogene Daten handelt, ist allgemein von Bedeutung, zu welchem Grad die Daten anonymisiert worden sind (K-Anonymität), bzw. ob noch Rückschlüsse auf die einzelnen Personen (eventuell in Verbindung mit anderen Datenbanken) gezogen werden können.

Prognosedaten Netz

Use Case 1

Hierbei handelt es sich um Daten für die Netznutzungskalkulation und Verlustbeschaffung. Zu beachten ist, dass auch die Daten der Verteilnetzbetreiber vom DSG erfasst sind, wenn sie personenbezogen sind, auch wenn Sie hier nicht im Fokus stehen. Im Netz sind es üblicherweise aggregierte Prognosen (über den gesamten Netzbereich zusammen), was dazu führt, dass die Daten keiner bestimmten bzw. bestimmbaren Person zugeordnet werden können.

Prognosedaten Ein-/ Ausspeisung

Use Case 10, 11

Aus Archiv- und Messdaten (aus dem Verteilnetz) und Meterdaten können Einspeiseprognosen erstellt werden. Neu könnten auch Prosumer Daten dazu beitragen (vorprogrammierte Geräte), d.h. die Prognosen können (auch) auf den Metering-Daten der Prosumer basieren. Die Resultate (Prognosedaten) würden in einem solchen Fall jedoch aggregiert werden. Die Daten der Prosumer stellen grundsätzlich Personendaten i.S.d. DSG dar; das Aggregieren dieser Daten ist als Bearbeitung zu qualifizieren. Bei der Verwendung der bereits aggregierten und dadurch anonymisierten Daten handelt es sich indes nicht um eine Bearbeitung von Personendaten i.S.d. DSG.

Use Case 12

Die Prognosen über die Last und Erzeugung können die Berechnung der Flexibilität unterstützen. Es ist notwendig, die Bilanz über das gesamte Netz zu kennen. Die Daten können dabei aggregiert sein. Bei der Frage, ob es sich bei den aggregierten Daten um personenbezogene Daten handelt, ist auch hier von Bedeutung, zu welchem Grad die Daten anonymisiert worden. Zu beachten gilt hier, dass das Anonymisieren von personenbezogenen Daten als Bearbeitung i.S.d. DSG verstanden wird. Siehe hierzu ebenfalls oben: Use Case 10 – Reduktion Netzverluste, Ein-/Ausspeiseprognosen.

7.24. Regionale Netzauslastung (Echtzeit)

Verwendet in den Use Cases: 5

Beteiligte Rollen: Verteilnetzbetreiber

7.24.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit sind die Daten der regionalen Netzauslastung bezüglich Vertraulichkeit und Integrität kritisch, da diese durch Fremde missbraucht werden können und die Netzstabilität dadurch beeinträchtigt werden könnte. Die Verfügbarkeit ist tendenziell unkritisch bezüglich der Versorgungssicherheit, da diese Daten voraussichtlich für regionale Steuerungen verwendet werden, um die Netzstabilität zu erhöhen. Die Grundversorgung wird voraussichtlich analog zu heute auch ohne diese Daten funktionieren.

Datensicherheit aus Gründen des Datenschutzes:

Die regionale Netzauslastung ist tendenziell unkritisch aus Sicht des Datenschutzes, da sie nicht unter den Rollen ausgetauscht werden.

7.24.2. Datenschutzrechtliche Qualifikation der Daten

Die Zustandsdaten der Netzauslastung werden jeweils innerhalb der Netzgebiete überwacht, um regionale Flexibilitäten zu erkennen. Das Format ist hier noch offen, eine abschliessende Qualifikation der Personenbezogenheit der Daten ist somit noch nicht möglich. Normalerweise handelt es sich um rein interne Netzbetreiberdaten, es werden also keine Daten von anderen Personen bearbeitet. Das DSG gelangt, falls die Daten nur intern verwendet werden, nicht zur Anwendung.[213]

[213] Anwendung findet das DSG nur, soweit Daten von anderen natürlichen oder juristischen Personen bearbeitet werden. Nicht in den Anwendungsbereich des DSG fällt somit, wer nur Personendaten über sich selbst bearbeitet, *Jöhri/Rosenthal* (Anm. 5), Art. 2 N. 13.

7.25. Regionale Netzkonfiguration

Verwendet in den Use Cases: 5

Beteiligte Rollen: Verteilnetzbetreiber

7.25.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit sind die Daten der regionalen Netzkonfiguration bezüglich Vertraulichkeit und Integrität kritisch, da diese durch Fremde missbraucht werden können und die Netzstabilität dadurch beeinträchtigt werden könnte. Die Verfügbarkeit ist tendenziell unkritisch bezüglich der Versorgungssicherheit.

Datensicherheit aus Gründen des Datenschutzes:

Die regionale Netzkonfiguration ist tendenziell unkritisch aus Sicht des Datenschutzes, da sie nicht unter den Rollen ausgetauscht werden.

7.25.2. Datenschutzrechtliche Qualifikation der Daten

Dies sind Daten zur aktuellen Konfiguration des Netzes und seiner Betriebsmittel. Sie beinhalten die gesamte Netztopologie, d.h. sämtliche Betriebsmittel mit ihren Konfigurationen. Diese Daten sind geschäftssensibel. Normalerweise stellen auch diese Daten rein interne Netzbetreiberdaten dar. Werden die Daten nicht nur intern vom Netzbetreiber verwendet, gelangt das DSG zur Anwendung.

7.26. Schaltinformationen

Verwendet in den Use Cases: 7

Beteiligte Rollen: Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.26.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Die Schaltinformationen sind für die Versorgungssicherheit bezüglich deren Integrität und Verfügbarkeit tendenziell kritisch. Falsche oder fehlende Informationen könnten Schaltungen auslösen, welche die Versorgungssicherheit gefährden.

Datensicherheit aus Gründen des Datenschutzes:

Die Schaltinformationen sind tendenziell kritisch aus Sicht des Datenschutzes, da sie unter den Rollen ausgetauscht werden und es sich um personenbezogene Daten im Sinne der Unternehmensdaten handelt.

7.26.2. Datenschutzrechtliche Qualifikation der Daten

Die Schaltinformationen werden innerhalb des Netzgebietes überwacht. Für die Bestimmung der Personenbezogenheit der Daten sind die vorhanden Informationen ungenügend.

7.27. Schaltsignal

Verwendet in den Use Cases: 4, 7, 8, 10, 12

Beteiligte Rollen: Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.27.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit sind die Schaltsignale unkritisch bezüglich der Vertraulichkeit. Für die Versorgungssicherheit sind sie bezüglich deren Integrität und Verfügbarkeit kritisch. Falsche oder fehlende Daten könnten die für die Netzstabilität notwendigen Schaltungen beeinträchtigen und so die Versorgungssicherheit gefährden.

Datensicherheit aus Gründen des Datenschutzes:

Die Schaltsignale sind tendenziell unkritisch aus Sicht des Datenschutzes, da sie nicht unter den Rollen ausgetauscht werden.

7.27.2. Datenschutzrechtliche Qualifikation der Daten

Use Case 4, 7, 8, 10, 12

Schaltsignale des VNB zur Übersteuerung der SDL-Vorhaltung und –Abrufsignale; es sind dies im Wesentlichen An- und Ausschaltungen. Diese Schaltsignale scheinen auf den ersten Blick aus datenschutzrechtlicher Perspektive unbedenklich.

Use Case 7, 8, 10, 12

Nach der Berechnung von Netzrekonfigurationen werden die Schaltsignale an die Betriebsmittel gesendet. Schaltsignale sind auf den ersten Blick aus datenschutzrechticher Perspektive unbedenklich. Eine genauere Qualifikation ist aufgrund der Unsicherheiten bezüglich der konkreten Ausgestaltung der Use Cases nicht möglich. Für die Qualifikation siehe oben: Use Case 4 – Systemdienstleistungen, Schaltsignale.

7.28. Schutzmassnahmen

Verwendet in den Use Cases: 6

Beteiligte Rollen: Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.28.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit sind die Vertraulichkeit und die Integrität der Schutzmassnahmen als kritisch einzustufen, da diese im Falle eines Angriffs durch Fremde nicht eingesehen und nicht manipuliert werden dürfen.

Datensicherheit aus Gründen des Datenschutzes:

Da die Schutzmassnahmen gegebenenfalls zwischen den Rollen ausgetauscht werden, könnten diese aus Sicht des Datenschutzes kritisch sein. Es kommt darauf an inwiefern aus den Daten Rückschlüsse auf personenbezogene Daten (in diesem Fall Unternehmensdaten) gemacht werden können.

7.28.2. Datenschutzrechtliche Qualifikation der Daten

Dies ist eine Liste der aktuellen und anzugehenden Schutzmassnahmen. Auch hier ist anzumerken, dass für die Bestimmung der Personenbezogenheit der Daten nur ungenügende Informationen vorliegen. Die derzeitigen Unsicherheiten über die konkrete Ausgestaltung dieses Use Cases erlauben vorliegend keine abschliessende Qualifikation der Daten.

7.29. Steuersignale Ein- / Ausspeisung

Verwendet in den Use Cases: 5, 8, 10, 12

Beteiligte Rollen: Prosumer, Datenmanager, Erzeuger, Verteilnetzbetreiber, Übertragungsnetzbetreiber

7.29.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Die Integrität der Steuersignale der Ein- und Ausspeisungen kann für die Versorgungssicherheit als kritisch eingestuft werden, da bei einer breiten Verteilung falscher Werte die Netzstabilität gefährdet werden kann. Die Verfügbarkeit und Vertraulichkeit ist tendenziell weniger kritisch für die Versorgungssicherheit.

Datensicherheit aus Gründen des Datenschutzes:

Da die Steuersignale zwischen den Rollen ausgetauscht werden, muss berücksichtigt werden, inwiefern Rückschlüsse auf personenbezogene Daten (auch Unternehmensdaten) gemacht werden könnten. Aufgrund der heutigen Annahmen sind diese Daten tendenziell unkritisch bezüglich des Datenschutzes.

7.29.2. Datenschutzrechtliche Qualifikation der Daten

Die Steuersignale für die Einspeisung gehen an alle steuerbaren Erzeuger, einerseits innerhalb des Netzgebietes und aggregiert zu anderen Netzgebieten. Die Gesamtkapazität der Blindleistungseinspeisung muss abgeschätzt werden oder bekannt sein. Diese Signale gehen vom Netzbetreiber zum Prosumer und zum Erzeuger. Im Wesentlichen handelt es sich um An- und Ausschaltungen bzw. Erhöhung oder Senkung der Kapazitäten. Diese Schaltsignale scheinen auf den ersten Blick aus datenschutzrechticher Perspektive unbedenklich. Indes ist es denkbar, dass aus der Summe dieser Signale der Bedarf des Netzbetreibers hergeleitet werden könnte und somit diese Datenströme ebenfalls vom DSG erfasst wären.

7.30. Steuersignale Endgeräte

Verwendet in den Use Cases: 3

Beteiligte Rollen: Prosumer, Datenmanager, Dienstleister Gebäudeautomation

7.30.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Aus Sicht der Versorgungssicherheit kann die Integrität der Steuersignale der Endgeräte kritisch sein, insbesondere wenn an eine grössere Anzahl von Gebäudeautomationen gleichzeitig falsche Steuersignale gesendet werden.

Die Verfügbarkeit und Vertraulichkeit dieser Daten ist für die Versorgungssicherheit unkritisch.

Datensicherheit aus Gründen des Datenschutzes:

Für den Datenschutz sind die Steuersignale tendenziell als kritisch einzustufen, da möglicherweise daraus konkrete Daten zu den vorhandenen Endgeräten herausgelesen werden könnten. Bei diesen Daten würde es sich um personenbezogene und daher geschützte Daten handeln, insbesondere dann, wenn das entsprechende Gerät nur von einer bestimmten Person verwendet wird.

7.30.2. Datenschutzrechtliche Qualifikation der Daten

Steuersignale dienen der Ansteuerung der Endgeräte des Prosumers für beliebige zukünftige Anwendungszwecke im Smart-Home. Diese Signale gehen vom Dienstleistungserbringer zum Prosumer. Im Wesentlichen handelt es sich um An- und Ausschaltungen der Endgeräte. Das Ansteuern spezifischer Geräte generiert personenbezogene Daten, soweit die Nutzung dieser Geräte selbst personenbezogen ist.

7.31. Systemzustandsdaten

Verwendet in den Use Cases: 2

Beteiligte Rollen: Verteilnetzbetreiber, Prosumer, Datenmanager

7.31.1. Datensicherheitsbedarf

Datensicherheit aus Gründen der Versorgungssicherheit:

Für die Versorgungssicherheit ist die Verfügbarkeit und Integrität der Systemzustandsdaten als kritisch einzustufen. Mit falschen oder fehlenden Systemzustandsdaten könnten Schaltungen ausgelöst werden, welche die Netzstabilität beeinträchtigen und so die Versorgungssicherheit gefährden.

Datensicherheit aus Gründen des Datenschutzes:

Die Systemzustandsdaten sind aus Datenschutzsicht kritisch einzustufen, da diese Rückschlüsse auf geschützte personenbezogene Daten und Unternehmensdaten zulassen und unter den Rollen ausgetauscht werden.

7.31.2. Datenschutzrechtliche Qualifikation der Daten

Systemzustandsdaten sind Daten über den Netzzustand, so dass der Verbraucher aktiv und zugunsten des Netzsystems agieren kann. Die Idee ist hier, dass diese Daten Anreizsignale an den Prosumer darstellen sollen. Inhalt und Form dieser Daten sind zurzeit jedoch noch offen. Ein Sammeln solcher Daten könnte Aufschluss über die generelle Versorgungsqualität des Netzes geben, womit Personendaten der Netzbetreiber vorliegen können.

8. ICT-Architektur und Datensicherheit

Im folgenden Kapitel wird die aus den Use Cases resultierende ICT-Architektur vorgestellt. In einem ersten Schritt zeigt die gemäss der Smart Grid Coordination Group [6] empfohlene Referenzarchitektur das Gesamtbild der sich ergebenden ICT-Architektur im Smart Grid. Anschliessend werden sämtliche Rollen, Komponenten und Datenflüsse der Use Cases zu einem übergreifenden Gesamtbild der Datenflussarchitektur zusammengestellt, aufgrund welcher der Datensicherheitsbedarf den einzelnen Elementen zugewiesen werden kann.

8.1. Referenzarchitektur Smart Grid

Parallel zu den Use Cases wurde eine Referenzarchitektur entwickelt. Diese besteht aus vertikalen Domänen und horizontalen Ebenen:

- Die Domänen Zentrale Produktion, Handel & Vertrieb, Übertragung, Verteilung / dezentrale Erzeugung, Prosumer stellen die Wertschöpfungskette der Energieversorgung dar.
- Die Ebenen Komponenten, Kommunikation, Information, Funktionen und Aktionsfelder wurden auf Basis der Smart Grid Referenzarchitektur [6] (siehe Kapitel 3) gewählt. Die Referenzarchitektur wurde auf europäischer Ebene von CEN / CENELEC / ETSI erarbeitet und soll helfen Use Cases zu identifizieren. Des Weiteren soll sie helfen bei der Identifizierung von Standardisierungsbedarf.

Die Referenzarchitektur wurde in allen Ebenen durch die aus Berichten und Studien bekannten Elemente ergänzt. In der obersten Ebene der Aktionsfelder wurden die folgenden vier Ziel-Kategorien für die Smart Grid Funktionalitäten identifiziert und die zugehörigen Funktionen jeweils zugeordnet. Aufgrund der vielschichtigen Funktionen gibt es bei der Zuordnung zu den Aktionsfeldern eine gewisse Unschärfe. In einigen Fällen kann die Funktion auch anderen Aktionsfeldern dienen:

- Netzbetrieb: Fehlererkennung und Netzrekonfiguration, Instandhaltung, Steuerung Wirk- und Blindleistung, Reduktion Netzverluste
- Netzsicherheit: Systemdienstleistungen, Regionale Flexibilitäten, Schutzerhalt Netzsystem und Daten
- Netzplanung: Betriebsmitteleinsatzplanung, Zeitliche Flexibilisierung Ein-/ Ausspeisung
- Weitere Dienstleistungen: Datenmanagement, Demand Side Response, Gebäudeautomatisierung

Aus der Funktionsebene wurden die Use Cases entwickelt und beschrieben. Die Objekte der Informations-, Kommunikations- und Komponentenebene werden in mehreren Use Cases verwendet und sind daher weder den einzelnen Funktionen und Aktionsfeldern noch den Domänen direkt zugeordnet.

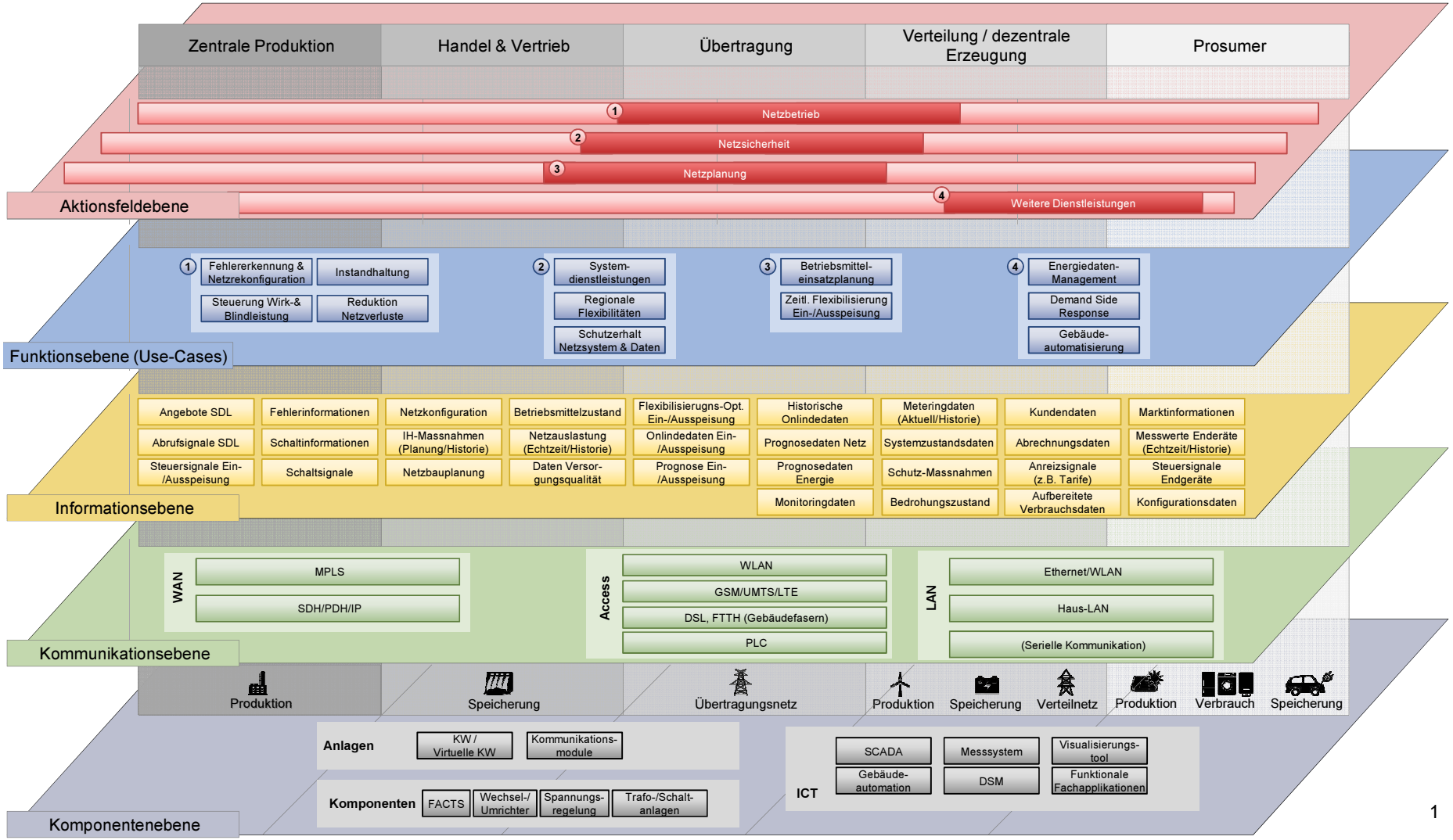


Abbildung 14: ICT Architektur – Referenzarchitektur

8.2. Gesamtbild der Use Cases

8.2.1. Gesamtarchitektur

In vielen Use Cases wurden für unterschiedliche Verwendungszwecke dieselben Datenobjekte oder Datenflüsse sowie Komponenten und Rollen verwendet. In einem Gesamtbild, das alle identifizierten Use Cases in einem Bild zusammen darstellt, kann die gesamte Menge der Datenobjekte und Datenflüsse, sowie deren Einbettung in die Komponenten und Rollen erfasst werden. In der folgenden Abbildung ist diese Gesamtsicht aufgezeigt.

Für die Übersichtlichkeit wurden die Kommunikationsverbindungen farblich unterschieden:

MPLS, SDH / PDH

WLAN, GSM, UMTS, LTE, DSL, FTTH, PLC

WLAN, Ethernet

Die weiteren Elemente des Gesamtbildes sind analog zu den einzelnen Use Cases abgebildet. Pro Rolle sind alle darin vorkommenden Komponenten und die zugehörigen Datenobjekte aufgeführt. Zwischen den Rollen sind mit gelben Pfeilen die Datenflüsse dargestellt.

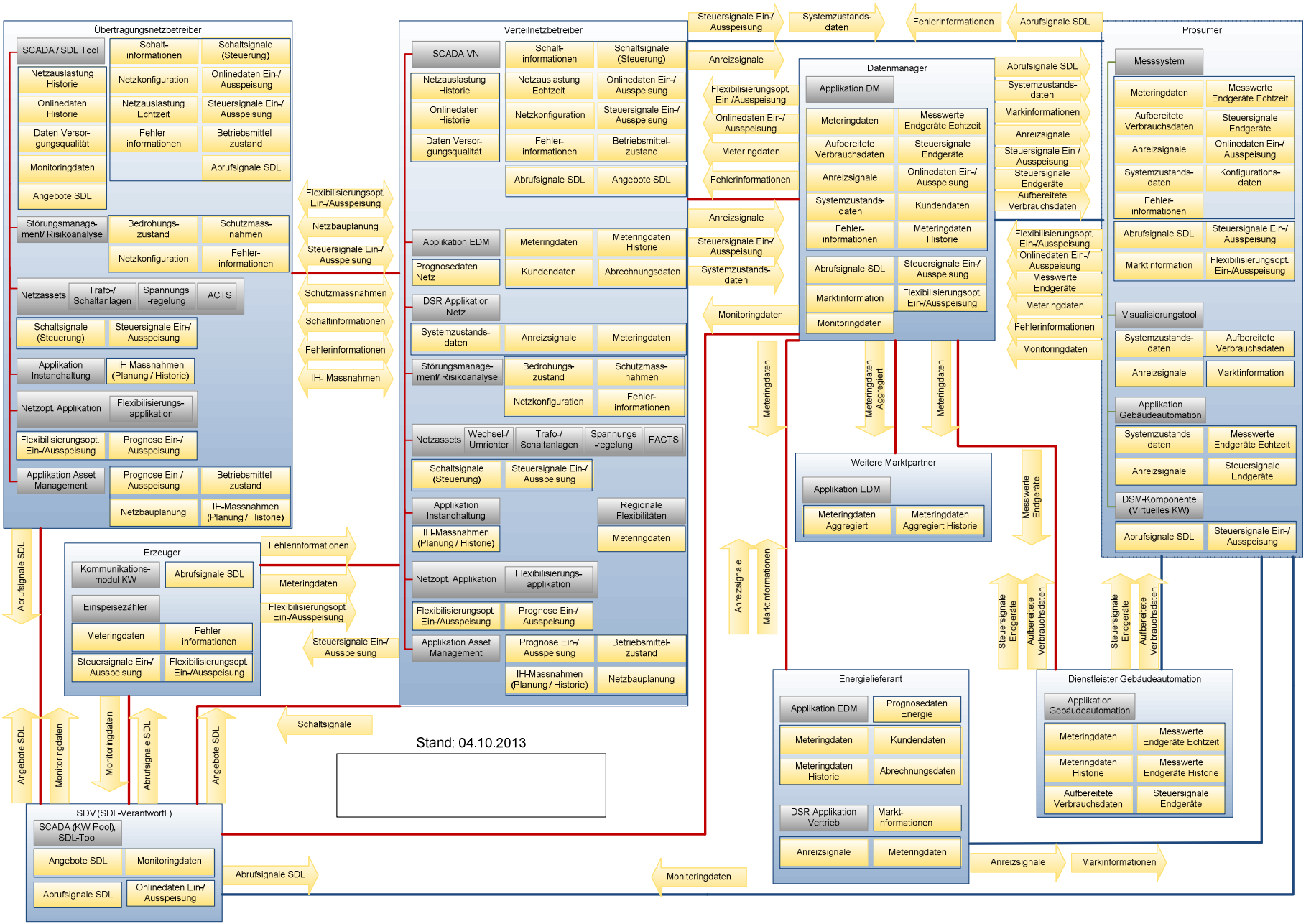
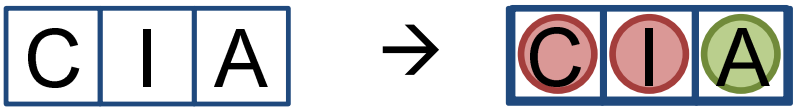


Abbildung 15: ICT Architektur – Gesamtbild der Use Cases

8.2.2. Datensicherheitsbedarf

In der Gesamtdarstellung in Abbildung 17 wird der Datensicherheitsbedarf dargestellt. Dabei wird die Beurteilung nach „CIA“ – Vertraulichkeit, Integrität, Verfügbarkeit (gemäss Kapitel 4.4.1) vorgenommen:



Rot = kritisch, grün = unkritisch, orange = tendenziell kritisch

Die Datenobjekte wurden entsprechend ihrer diesbezüglichen Bewertung innerhalb der jeweils betroffenen Komponenten gruppiert. Die Einteilung erfolgt auf Grund der exakten Bewertungen und deren Begründungen in Kapitel 1. Durch die noch unklare Ausgestaltung der Daten ergibt sich bei der Bewertung eine gewisse Unschärfe. So muss beispielsweise bei der konkreten Ausarbeitung die Periodizität und Granularität der Daten für die Endbeurteilung mit einbezogen werden. Bei Daten, welche kritisch („rot“) bewertet wurden, wurde für diese Studie angenommen, dass deren Ausprägung entsprechend detailliert ausfallen könnte. In Abbildung 16 ist ein Ausschnitt mit der Rolle Prosumer und der Komponente Messsystem dargestellt. Das Messsystem enthält einerseits Datenobjekte, welche beim Prosumer gemessen werden und allenfalls personenbezogene Rückschlüsse zulassen könnten (Messwerte, Konfigurationsdaten, Verbrauchsdaten, Zustandsdaten, etc.). Diese Daten wurden gruppiert und mit kritischer Vertraulichkeit und Integrität beurteilt; Letzteres, da auch manipulierte Daten die Persönlichkeitsrechte verletzen können. Die Verfügbarkeit dieser Daten ist weder aus Sicht Versorgungssicherheit noch aus Sicht Datenschutz relevant. Andererseits werden im Messsystem auch Datenobjekte vorgehalten, welche keine persönlichen Informationen beinhalten, wie Marktinformationen und Flexibilisierungsoptionen. Diese Informationen sind weder vertraulich noch kritisch bezüglich der Verfügbarkeit. Sie sind jedoch für die Versorgungssicherheit tendenziell kritisch aus Integritätssicht, da diesbezügliche Manipulationen in der Masse durchaus einen Einfluss auf die Netzstabilität haben könnten. .

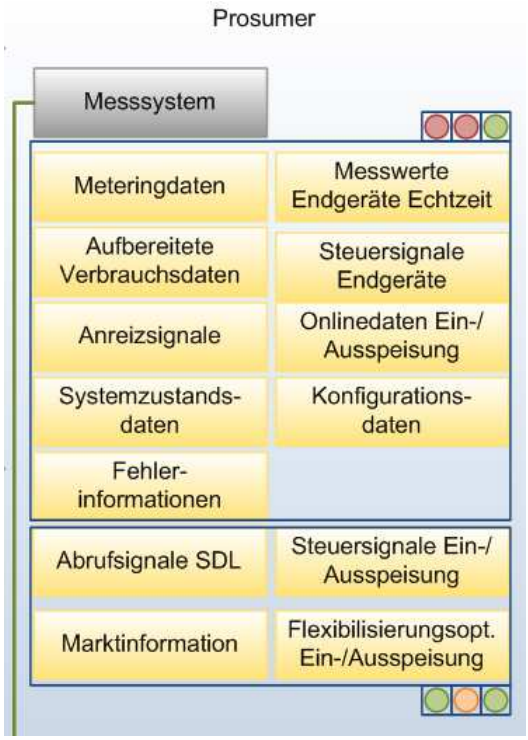


Abbildung 16: Beispiel der CIA-Bewertung der Datensicherheit

Nicht separat bewertet wurde hier das vierte Kriterium aus Kapitel 4.4.1, die Nachvollziehbarkeit, da sich diese direkt aus den ersten drei Kriterien ergibt. Sofern ein Datenobjekt aus Sicht der Vertraulichkeit, der Integrität oder der Verfügbarkeit kritisch ist, wird automatisch die Nachvollziehbarkeit des Datenobjektes als kritisch eingestuft.

Die Darstellung auf der folgenden Seite fasst die gesamte Datenflussarchitektur mit dem Smart Grid Datensicherheitsbedarf zusammen:

In der Gesamtansicht wird ersichtlich, dass die Daten im Prosumerumfeld insbesondere bezüglich der Vertraulichkeit und Integrität kritisch sind. Die Verfügbarkeit dieser Daten ist generell weniger kritisch.

Bei den Daten in den anderen Rollen kann vielfach unterschieden werden zwischen Daten, die vom Prosumer empfangen werden und daher demselben Muster unterliegen (Vertraulichkeit und Integrität kritisch) und Daten im Umfeld der Steuerung und Regelung des Netzes und der Lastflüsse, mit einer hohen Kritikalität bei der Verfügbarkeit und der Integrität.

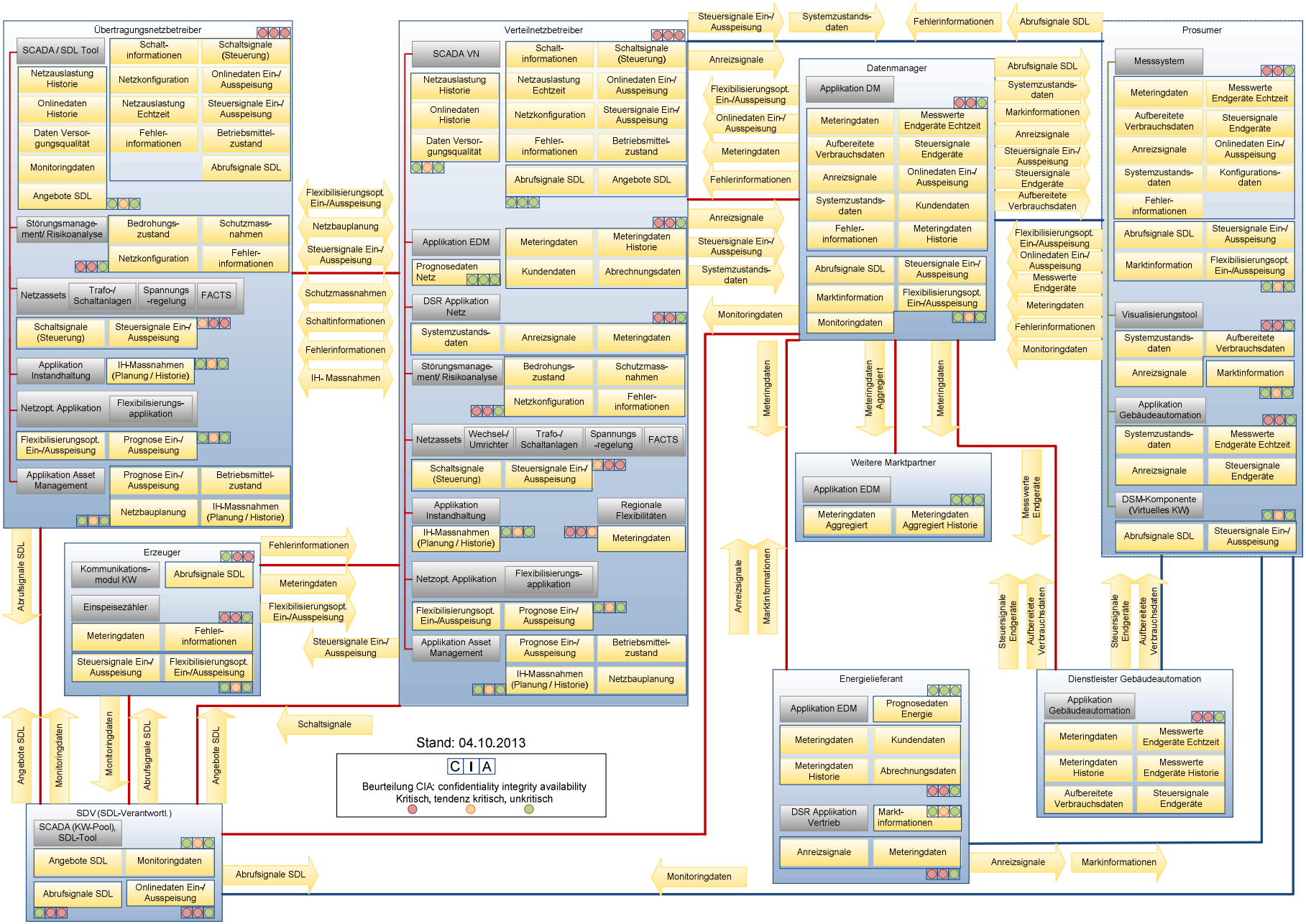


Abbildung 17: ICT Architektur – Datensicherheitsbedarf

9. Standardisierungsbedarf

9.1. Strukturierung anhand der ICT Architektur

Basierend auf der Bewertung des Datensicherheits- und Datenschutzbedarfs lässt sich der Bedarf an zukünftigen diesbezüglichen Standards und Richtlinien sowie deren geeignete Strukturierung ableiten. Dazu wurde das Gesamtbild in vier Sektoren unterteilt, die inhaltlich gruppiert werden können und in die Struktur bestehender Standards und Richtlinien sowohl in der Schweiz als auch dem internationalen Umfeld passen.

Dies ergibt die folgenden Standardisierungskategorien:

- Datensicherheitstandards für Messsysteme: Hiermit sind Standards und Richtlinien gemeint, welche den sicheren Betrieb der Messsysteme und den Umgang mit den dort vorgehaltenen Daten aus Datensicherheitssicht regeln. Die Messsysteme beinhalten alle Systeme beim Endkunden, welche den allenfalls angeschlossenen (unabhängig vom Kommunikationsweg) Netz- und Marktpartnern gemessene Daten für deren Weiterverwendung (primär Abrechnung und Prognose) zur Verfügung stellen. Je nach zukünftigem Verwendungszweck aus den Use-Cases in Kapitel 5, können die Messsysteme auch eine Gateway-Funktion zur Übermittlung weiterer Datenobjekte ausüben.
- Datensicherheitstandards für die Anbindung der Gebäudegeräte: Hiermit sind Standards und Richtlinien gemeint, welche die Schnittstellen zwischen der Gebäudeautomation und der dort mit dem Stromnetz angebundenen Geräte mit dem Stromnetz aus Datensicherheitssicht regeln.
- Datensicherheitstandards für den Umgang mit Prosumer Daten: Hiermit sind Standards und Richtlinien gemeint, welche den Umgang mit den Prosumer Daten bei den Netz- und Marktpartnern in Abhängigkeit von der Ausprägung der aufgenommenen Daten regeln, d.h. bei denjenigen Rollen aus den Use-Cases in Kapitel 5, welche Prosumer Daten verwalten und diese in Systemen ausserhalb der Verfügung des betroffenen Prosumers vorhalten.
- Datensicherheitstandards für Netzmanagement Daten: Hiermit sind Standards und Richtlinien gemeint, welche den Umgang mit den Daten zur Netzführung aus Datensicherheitssicht regeln. Dazu gehören die Automatisierungen und Optimierungen des Netzbetriebs, der Netzregelung, sowie des Asset Managements.

Die folgende Abbildung grenzt diese Standardisierungskategorien im Rahmen der Gesamtarchitektur ab:

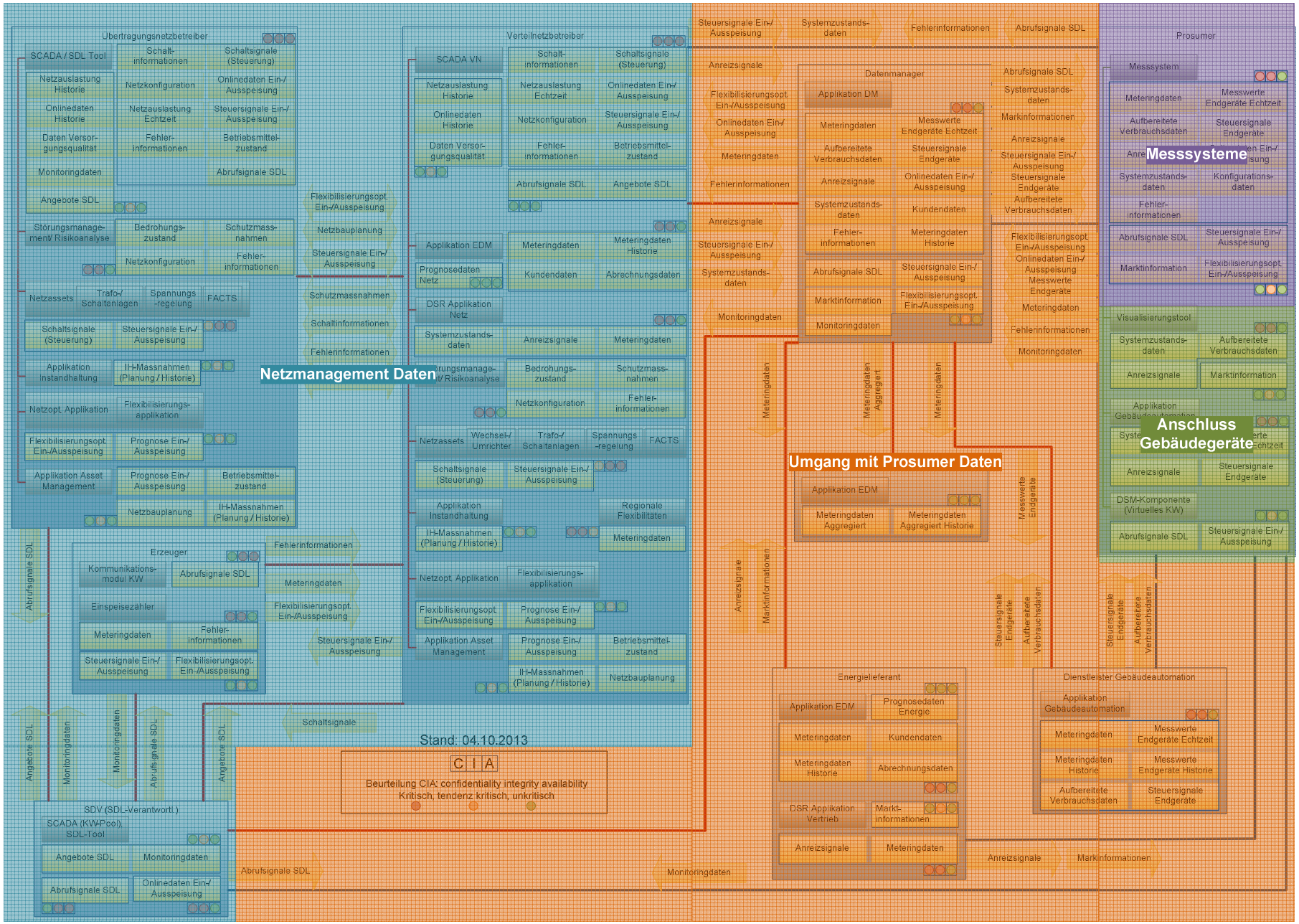


Abbildung 18: ICT Architektur – Standardisierungskategorien

9.2. Anforderungen

Im Rahmen der EU-weiten Aktivitäten bezüglich Datensicherheits- und Datenschutzbedarf wurden von der ENISA[214] Anforderungen und Massnahmen zum Umgang mit der Informationssicherheit im Smart Grid definiert [3]. Je nach Bewertung der Datensicherheit und des Datenschutzes sind unterschiedliche Standards zu erstellen, welche die entsprechenden Anforderungen konkretisieren. Diese Anforderungen eignen sich als Grundlage sowohl zur Analyse, Definition und Umsetzung sicherheitstechnischer Anforderungen im Unternehmen, als auch zur Betrachtung und Diskussion branchenweiter Best-Practices und zukünftiger Richtlinien. Die dort formulierten Anforderungen werden deshalb an dieser Stelle als Hilfestellung für zukünftige hiesige Präzisierungen und Adaptionen aufgeführt. Sie sind im Rahmen dieser Studie jedoch rein informativer Natur und stellen keine Mindestanforderungen im Sinne zukünftiger Richtlinien dar. Die Auflistung soll als Hilfestellung dienen, um die Themen umfassend beurteilen zu können.

Die Anforderungen und Massnahmen aus dem ENISA-Dokument werden nachfolgend auf die bisher definierten Sicherheitskriterien Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit bezogen und dementsprechend unterteilt. Des Weiteren werden übergeordnete Anforderungen aus betrieblicher und technischer Sicht aufgeführt. So werden je nach der in dieser Studie identifizierten Kritikalität dieser Sicherheitskriterien unterschiedliche Anforderungen gemäss der ENISA Massnahmen an ein datenverarbeitendes System und dessen Objekte gestellt. Zusätzlich werden auch übergreifend geltende betriebliche und technische Anforderungen gestellt, welche hier der Vollständigkeit halber aufgeführt werden.

Die Anforderungen werden aufgrund ihrer datensicherheitsbezogenen Relevanz priorisiert, wie folgt:

- **Kernanforderungen (in der Liste fett dargestellt)**: Dies sind Anforderungen, welche bezüglich der Datensicherheit eine hohe Priorität aufweisen.
- Sekundäranforderungen: Dies sind Anforderungen, welche bezüglich der Datensicherheit eine niedrigere Priorität aufweisen.

Die nachfolgend aufgeführte Nummerierung der Anforderungen entspricht der originalen Referenzierung im ENISA-Dokument.

Die folgenden *übergeordneten betrieblichen Anforderungen* sollten für alle Standardisierungskategorien (Abbildung 18) berücksichtigt werden. Sie beinhalten grundlegende betriebliche oder organisatorische Sicherheitsanforderungen für Unternehmen, die kritisches Daten verwenden. Die Verwendung kann dabei zur Analyse, Bearbeitung oder auch zu einem anderen Zweck erfolgen. Die folgende Tabelle beschreibt grundlegende Sicherheitsanforderungen, welche in jedem System mit kritischen Daten analysiert und gegebenenfalls umgesetzt werden sollten.

[214] ENISA ist die Europäische Agentur für Netz- und Informationssicherheit, welche für die europäischen Mitgliedsstaaten und Industrie zentrale Themen der Informationssicherheit und deren Herausforderungen bearbeitet.

Security Measure	Description
Kernanforderungen	
SM 1.2 Organisation of information security	The provider should establish and maintain an appropriate structure of security roles and responsibilities.
SM 3.1 Security requirements analysis and specification	The provider should identify and define beforehand the necessary security requirements for smart grid components and systems during the design and procurement.
SM 3.2 Inventory of smart grid components/systems	The provider should establish and maintain an inventory that represents the components and smart grid information systems
SM 4.1 Personnel screening	The provider should perform appropriate background checks on personnel (employees, contractors, and third-party users) if required for their duties and responsibilities
SM 4.3 Security and awareness program	The provider should establish and maintain a security awareness program across the organisation.
SM 4.4 Security training and certification of personnel	The provider should establish and maintain security training and personnel certification programmes, taking into account its needs based on their roles and responsibilities.
Sekundäranforderungen	
SM 1.1 Information security policy	The provider should establish and maintain an appropriate information security policy
SM 1.3 Information security procedures	The provider should establish and maintain an appropriate set of security procedures that supports the implementation of the security policy
SM 1.4 Risk management framework	The provider should establish and maintain an appropriate risk management framework for risk assessment and risk treatment activities across the organisation which will take into account the complex operational environment.
SM 1.5 Risk assessment	The provider should establish and perform risk assessment activities to identify and evaluate the risk across the organisation at regular intervals.

SM 1.6 Risk treatment plan	The provider should establish and maintain an appropriate risk treatment plan in order to manage the risk across the organisation
SM 2.1 Third party agreements	The provider should establish and maintain appropriate third party agreements to preserve the integrity, confidentiality and availability of the information at the same level as the internal services when dealing with customers and third parties
SM 3.5 Software/firmware upgrade of smart grid components/systems	The provider should establish and maintain activities for software/firmware upgrade on the components and smart grid information systems.

Die folgenden *übergeordneten technischen Anforderungen* sollen für alle Standardisierungskategorien berücksichtigt werden. Sie beinhalten grundlegende Sicherheitsanforderungen, welche in jedem System mit kritischen Daten analysiert und gegebenenfalls umgesetzt werden sollten.

Security Measure	**Description**
Kernanforderungen	
SM 5.1 Incident response capabilities	The provider should establish and maintain capabilities to respond against cyber security incidents
SM 8.1 Physical security	The provider should establish and maintain the appropriate physical security of the smart grid facilities/components/systems.
SM 8.3 Physical security on third party premises	The provider should protect equipment located outside of the organisations' own grounds or premises in areas that are the responsibility of other utilities against physical and environmental threats
SM 9.6 Media handling	The provider should establish and maintain secure procedures for the access, storage, distribution, transport, sanitization, destruction and disposal of the media assets.
Sekundäranforderungen	
SM 5.2 Vulnerability assessment	The provider should establish and maintain vulnerability assessment activities on the smart grid information systems

SM 5.3 Vulnerability management	The provider should establish and maintain an appropriate vulnerability management plan in order to manage vulnerabilities on smart grid information systems
SM 5.4 Contact with authorities and security interest groups	The provider should establish and maintain contacts with authorities and security interest groups to be aware of vulnerabilities and threats

Die Anforderungen zu „CIA“ – *Vertraulichkeit, Integrität* und *Verfügbarkeit* – sind wie folgt:

Vertraulichkeit:

Security Measure	**Description**
Kernanforderungen	
SM 9.2 Account management	The provider should establish and maintain system/groups/user accounts on smart grid information systems
SM 9.3 Logical access control	The provider should enforce logical access to authorised entities on smart grid information systems and security perimeters
SM 9.1 Data security	The provider should implement security requirements in order to protect the information on smart grid information systems
SM 9.4 Secure remote access	The provider should establish and maintain secure remote access where applicable to smart grid information systems.
SM 10.1 Secure network segregation	The provider should establish and maintain a segregated network for the smart grid information system.
SM 10.2 Secure network communications	The provider should establish and maintain secure communications across the segregated network
Sekundäranforderung	
SM 3.6 Disposal of smart grid components/systems	The provider should establish and maintain activities for the secure disposal of smart grid components and smart grid information systems

Integrität:

Security Measure	**Description**
Kernanforderungen	

SM 3.3 Secure configuration management of smart grid components/systems	The provider should ensure that the base security configuration of a smart grid's components/systems is identified, set and maintained for every instance of that component/system.
SM 3.4 Maintenance of smart grid components/systems	The provider should establish and maintain activities for performing routine and preventive/corrective maintenance on the components and smart grid information systems.
SM 9.5 Information security on information systems	The provider should establish and maintain appropriate information security capabilities on information systems, to provide protection against malware, viruses and other common threats
Keine Sekundäranforderungen	

Verfügbarkeit:

Security Measure	Description
Kernanforderungen	
SM 7.1 Continuity of operations capabilities	The provider should establish and maintain capabilities to ensure essential functions after disruption events on smart grid Information systems
SM 7.2 Essential communication services	The provider should establish, maintain and test essential/emergency communication services in case of major disasters
Keine Sekundäranforderungen	

Sie werden in den folgenden Kapiteln hinsichtlich der Standardisierungskategorien gemäss Abbildung 18 spezifisch beschrieben.

Da die Anforderungen zur *Nachvollziehbarkeit* für alle Datenobjekte gilt, welche betreffend „CIA" kritisch sind, müssen sie für alle Standardisierungskategorien berücksichtigt werden. Die in [3] aufgeführten Anforderungen an die Nachvollziehbarkeit sind:

Security Measure	Description
Kernanforderungen	
SM 3.7 Security testing of smart grid components/systems	Security testing activities on the smart grid components/systems should be performed in order to verify its security

SM 4.2 Personnel changes	The provider should establish and maintain an appropriate process for managing changes in personnel (employees, contractors, third-party users) or changes in their roles and responsibilities
SM 6.1 Auditing capabilities	The provider should establish and maintain auditing capabilities on the smart grid Information systems and components.
SM 6.2 Monitoring of smart grid information systems	The provider should establish and maintain monitoring activities on the smart grid Information systems and components.
SM 6.3 Protection of audit information	The provider should protect the audit information generated
SM 8.2 Logging and monitoring physical access	The provider should establish and maintain capabilities for logging and monitoring the physical access to the smart grid facilities/components taking into account the criticality of the facility.
Sekundäranforderung	
SM 2.2 Monitoring third parties services and validating solutions against predefined acceptance criteria	The provider should establish and maintain mechanisms in order to monitor the compliance of contractual obligations of information and services and validate solutions against predefined acceptance criteria

9.3. Standardisierungskategorie Messsysteme

9.3.1. Definition

Die Messsysteme haben das Ziel, den Netz- bzw. Marktpartnern Datenobjekte zur Ein- und Ausspeisung zu deren Weiterverwendungszwecke (primär Abrechnungs- und Prognosezwecke) zur Verfügung zu stellen. Je nach Einsatzszenario fungiert das Messsystem auch als Gateway zur Weiterleitung diverser weiterer Datenobjekte. Abhängig von Granularität und Umfang der Daten sowie deren Speicherung bestehen unterschiedliche Risiken und Gefahren, insbesondere für den Datenschutz.

9.3.2. Schutzbedarf

In Abbildung 18 ist der Datenumfang dieser Standardisierungskategorie dargestellt. Für die Beurteilung des Schutzbedarfs, wird die höchste Kritikalität pro Sicherheitskriterium (C, I, A) herangezogen. Die prosumerbezogenen Daten sind bezüglich der Vertraulichkeit und Integrität kritisch, gleichzeitig wurde die Verfügbarkeit für alle Datenobjekte als unkritisch beurteilt.

Aus dieser Beurteilung können die Anforderungen an die Datensicherheit gestellt werden. Die Beurteilung der Kritikalität alleine bestimmt noch nicht, ob die Anforderungen erfüllt

werden müssen. Bei weniger kritischen Daten wird die Umsetzung der Anforderung geringer ausfallen als bei höherer Kritikalität.

9.3.3. Anforderungen

Um die Datensicherheit zu gewährleisten, werden für eine Standardisierung in dieser Kategorie die folgenden Anforderungen empfohlen. Für die Festlegung der konkreten und angemessenen Massnahmen ist jeweils eine fallbezogene Risikoanalyse (Eintrittswahrscheinlichkeit und Auswirkungsgrad) durchzuführen. Diese Risikobetrachtung sollte bei der Festlegung der Standards und Richtlinien (siehe Kapitel 10) erfolgen. Zusätzlich zu den im Folgenden aufgelisteten Anforderungen müssen in jedem Fall die *übergeordneten betrieblichen Anforderungen*, die *übergeordneten technischen Anforderungen* und die Anforderungen zur *Nachvollziehbarkeit* berücksichtigt werden (siehe Kap. 9.2).

Vertraulichkeit

- Entsorgung von Komponenten / Systemen: Die physischen Messsysteme und die darin enthaltenen Datenobjekte müssen nach Betriebsende so (auch physisch) entsorgt werden, dass der Schutz der Datenobjekte auch danach erhalten bleibt. Es soll nicht möglich sein aus entsorgten / obsoleten Komponenten / Systemen kritische Daten auszulesen.
- Accountmanagement: Die für den Zugriff auf die Messsysteme berechtigten Systeme, Gruppen und User Accounts sind zu definieren, deren Zugriff zu regeln sowie dem Prosumer bekannt zu sein.
- Zugriffsschutz: Der logische Zugriff auf die Datenobjekte soll nur autorisierten Personen ermöglicht werden (z.B. mittels Passwort).
- Geschützter Fernzugriff: Da das Messsystem von Fern ausgelesen werden soll, unterliegt dieser Fernzugriff auch den Datensicherheitsbestimmungen. Das bedeutet, dass die dafür verwendete Kommunikation denselben Anforderungen untersteht wie die restliche Kommunikation. Als Beispiel könnte hier die Verschlüsselung der Kommunikation vorgeschrieben werden (z.B. via VPN).
- Netzwerktrennung: Um die Vertraulichkeit der Prosumer Daten zu schützen, kann gegebenenfalls ein getrenntes Netzwerk eingerichtet werden, je nach erfolgter Risikoabschätzung. Es ist unwahrscheinlich, dass für die Smart Meter ein separates physisches Netzwerk eingesetzt wird. An anderen Stellen ist es denkbar, dass die Netzwerke aus Sicherheitsgründen getrennt werden (wie es heute beispielsweise schon bei den Leitsystemen grossteils der Fall ist)
- Sichere Kommunikation: Die Kommunikation der Prosumer Daten über das gewählte Netzwerk muss die Vertraulichkeit sicherstellen.

Integrität

- Konfigurationsmanagement: Die grundlegenden Sicherheitskonfigurationen müssen bestimmt und gepflegt werden.
- Wartung der Komponenten / Systeme: Für die Messsysteme sollten klare Vorgaben zur präventiven und korrektiven Wartung und Pflege bestehen.
- Informationssicherheit (Schutz gegen Angriffe von aussen): Die Messsysteme sollten ausreichend vor Angriffen von aussen (Viren, Malware etc.) geschützt werden.

9.3.4. Bestehende Standards, Gesetze und Richtlinien

Die folgende Auflistung ist nicht abschliessend und sollte bei der Ausarbeitung weiterer Standards zwingend ergänzt werden.

Allgemeine Standards, Gesetze und Richtlinien:

- ISO/IEC 27002:Internationaler Standard „IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management“
- Bundesgesetz über den Datenschutz (DSG): Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.
- Fernmeldegesetz (FMG): Unter anderem für die Sicherstellung des störungsfreien, die Persönlichkeits- und Immaterialgüterrechte achtenden Fernmeldeverkehrs.

Smart Grid spezifische Standards, Gesetze und Richtlinien (EU oder andere Länder):

- NISTIR 7628: US Richtlinien für die Datensicherheit im Smart Grid “Guidelines for Smart Grid Cyber Security”
- ISO/IEC TR 27019: „Leitlinien zum Informationssicherheitsmanagement auf Basis ISO/IEC 27002 für die Telekommunikation für die Energiewirtschaft“

9.4. Standardisierungskategorie Anbindung Gebäudegeräte

9.4.1. Definition

Intelligente Gebäudegeräte oder Gebäudeautomationen werden vermehrt bei den Prosumern eingesetzt werden. Mit Informationen und Steuerungsmöglichkeiten dieser Geräte, können gezielte Dienstleistungen durch beliebige zukünftige Dienstleister zur Verfügung gestellt werden. Die diesbezüglichen Datenobjekte sind vor allem aus Datenschutzgründen zu schützen.

9.4.2. Schutzbedarf

In Abbildung 18 ist der Datenumfang dieser Standardisierungskategorie dargestellt. Für die Beurteilung des Schutzbedarfs, wird die höchste Kritikalität pro Sicherheitskriterium (C, I, A) betrachtet. Analog zur Standardisierungskategorie Messsysteme sind die prosumerbezogenen Datenobjekte bezüglich der Vertraulichkeit und Integrität kritisch. Gleichzeitig wurde die Verfügbarkeit für alle Datenobjekte als unkritisch beurteilt.

Aus dieser Beurteilung können die Anforderungen an die Datensicherheit gestellt werden.

9.4.3. Anforderungen

Um die Datensicherheit zu gewährleisten, werden die folgenden Anforderungen empfohlen. Für die Festlegung der konkreten und angemessenen Massnahmen ist jeweils eine fallbezogene Risikoanalyse (Eintrittswahrscheinlichkeit und Auswirkungsgrad) durchzuführen. Diese Risikobetrachtung sollte bei der Festlegung der Standards und Richtlinien (siehe Kapitel 10) erfolgen. Zusätzlich zu den im Folgenden aufgelisteten Anforderungen müssen in jedem Fall die *übergeordneten betrieblichen Anforderungen*, die *übergeordneten technischen Anforderungen* und die Anforderungen zur *Nachvollziehbarkeit* berücksichtigt werden (siehe Kap. 9.2).

Vertraulichkeit

- Entsorgung von Komponenten / Systemen: Die angebundenen Geräte und die darin enthaltenen Datenobjekte müssen nach Betriebsende so entsorgt werden, dass der Schutz der Datenobjekte auch danach erhalten bleibt. Dies betrifft auch Geräte, welche nicht in den Dienstleistungen einbezogen sind, aber die entsprechenden Datenobjekte zur Verfügung stellen können. Zum Beispiel könnten zukünftige Geräte die Daten aufnehmen und zur Verfügung stellen, auch wenn der Prosumer diese nicht nutzt.
- Accountmanagement: Die für den Zugriff auf die Gebäudegeräte berechtigten Systeme, Gruppen und User Accounts sind zu definieren, deren Zugriff zu regeln sowie dem Prosumer bekannt zu sein.
- Zugriffsschutz: Der logische Zugriff auf die Datenobjekte soll nur autorisierten Personen ermöglicht werden (z.B. mittels Passwort).
- Geschützter Fernzugriff: Da die Datenobjekte in den Gebäudegeräten von Fern ausgelesen werden und von Fern Steuersignale empfangen werden, unterliegt dieser Fernzugriff den Datensicherheitsbestimmungen, sowohl aus Datenschutzgründen als auch aus Versorgungssicherheitsgründen.
- Netzwerktrennung: Um die Vertraulichkeit der Prosumer Daten zu schützen, kann gegebenenfalls ein getrenntes Netzwerk eingerichtet werden, je nach erfolgter Risikoabschätzung.
- Sichere Kommunikation: Die Kommunikation der Prosumer Daten über das gewählte Netzwerk muss die Vertraulichkeit sicherstellen.

Integrität

- Konfigurationsmanagement: Die grundlegenden Sicherheitskonfigurationen der Geräte und deren Anbindung müssen bestimmt und gepflegt werden.
- Wartung der Komponenten / Systeme: Für die Gebäudegeräte sowie für deren Anbindung sollten klare Vorgaben zur präventiven und korrektiven Wartung und Pflege bestehen.
- Informationssicherheit (Schutz gegen Angriffe von aussen): Die Gebäudegeräte sowie deren Anbindungen sollten vor Angriffen von aussen (Viren, Malware etc.) geschützt werden.

9.4.4. Bestehende Standards, Gesetze und Richtlinien

Allgemeine Standards, Gesetze und Richtlinien:

- ISO/IEC 27002:Internationaler Standard „IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management“
- ISO/IEC 60870: Internationaler Standard für die Netztechnik „Fernwirkeinrichtungen und -systeme“
- ISO/IEC 14908 (Gebäudeautomation): Internationaler Standard mit den Teilen Kommunikationsprotokoll, Power Line Übertragungstechnologie, Übertragung über Zweidrahtleitung in freier Topologie, Übertragung über IP
- Bundesgesetz über den Datenschutz (DSG): Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.
- Fernmeldegesetz (FMG): Unter anderem für die Sicherstellung des störungsfreien, die Persönlichkeits- und Immaterialgüterrechte achtenden Fernmeldeverkehrs.

SG-Standards, Gesetze und Richtlinien (EU oder andere Länder):

- DIN EN 50438 – Deutschland: Anforderungen für den Anschluss von Klein-Generatoren an das öffentliche Niederspannungsnetz
- IEEE 1547: Internationaler Standard für die Verbindung verteilter Erzeuger in Stromnetzen
- NISTIR 7628: US Richtlinien für die Datensicherheit im Smart Grid “Guidelines for Smart Grid Cyber Security”

9.5. Standardisierungskategorie Prosumer Daten

9.5.1. Definition

Abgesehen vom Prosumer, werden die Daten des Prosumers im Smart Grid an weitere Rollen verteilt, bearbeitet und gespeichert. Unabhängig von der Quelle dieser Datenobjekte (Messsystem, Gebäudeautomation etc.) müssen Standards und Richtlinien den Umgang mit diesen Datenobjekten regeln. Diese Regelungen sollten die Umsetzung der Datenschutzbestimmungen in diesem Umfeld unterstützen. Dazu gehören unter anderem Vorgaben zu Speicherung, Verwendung und Weitergabe der Datenobjekte.

9.5.2. Schutzbedarf

Für die Beurteilung des Schutzbedarfs in dieser Standardisierungskategorie, wird die höchste Kritikalität pro Sicherheitskriterium (C, I, A) betrachtet. Analog zur Standardisierungskategorien Messsysteme und Anbindung Gebäudegeräte sind die prosumerbezogenen Datenobjekte bezüglich der Vertraulichkeit und Integrität kritisch. Gleichzeitig wurde die Verfügbarkeit für alle Datenobjekte als unkritisch beurteilt.

Aus dieser Beurteilung können die Anforderungen an die Datensicherheit gestellt werden.

9.5.3. Anforderungen

Um die Datensicherheit zu gewährleisten, werden die folgenden Anforderungen empfohlen. Für die Festlegung der konkreten und angemessenen Massnahmen ist jeweils eine fallbezogene Risikoanalyse (Eintrittswahrscheinlichkeit und Auswirkungsgrad) durchzuführen. Diese Risikobetrachtung sollte bei der Festlegung der Standards und Richtlinien (siehe Kapitel 10) erfolgen. Zusätzlich zu den im Folgenden aufgelisteten Anforderungen müssen in jedem Fall die *übergeordneten betrieblichen Anforderungen*, die *übergeordneten technischen Anforderungen* und die Anforderungen zur *Nachvollziehbarkeit* berücksichtigt werden (siehe Kap. 9.2).

Vertraulichkeit

- Entsorgung von Komponenten / Systemen: Überall wo Prosumer Daten verwendet werden, muss die Entsorgung so erfolgen, dass der Schutz der Datenobjekte auch nach Betriebsende erhalten bleibt.
- Accountmanagement: Alle Systeme mit Prosumer Daten sollten Regelungen bezüglich Zugriffe auf und durch die Systeme, Gruppen und User Accounts aufweisen, und diesen müssen dem Prosumer bekannt sein.
- Zugriffsschutz: Der logische Zugriff auf die Datenobjekte soll nur autorisierten Personen ermöglicht werden (z.B. mittels Passwort).

- Geschützter Fernzugriff: Für den Fernzugriff auf Prosumer Daten gelten dieselben Anforderungen an die Datensicherheit, wie für den Direktzugriff.
- Netzwerktrennung: Um die Vertraulichkeit der Prosumer Daten zu schützen, kann gegebenenfalls ein getrenntes Netzwerk eingerichtet werden, je nach erfolgter Risikoabschätzung sichere Kommunikation: Die Kommunikation der Prosumer Daten über das gewählte Netzwerk muss die Vertraulichkeit sicherstellen.
- Sichere Kommunikation: Die Kommunikation der Prosumer Daten über das gewählte Netzwerk muss die Vertraulichkeit sicherstellen.

Integrität

- Konfigurationsmanagement: Die grundlegenden Sicherheitskonfigurationen der Systeme mit Prosumer Daten müssen bestimmt und gepflegt werden.
- Wartung der Komponenten / Systeme: Für alle Systeme mit Prosumer Daten sollten klare Vorgaben zur präventiven und korrektiven Wartung und Pflege bestehen.
- Informationssicherheit (Schutz gegen Angriffe von aussen): Die Systeme mit Prosumer Daten sollen vor Angriffen von aussen (Viren, Malware etc.) geschützt werden.

9.5.4. Bestehende Standards, Gesetze und Richtlinien

Die folgende Auflistung ist nicht abschliessend und sollte bei der Ausarbeitung weiterer Standards zwingend ergänzt werden.

Allgemeine Standards, Gesetze und Richtlinien:

- Bundesgesetz über den Datenschutz (DSG): Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.
- Fernmeldegesetz (FMG): Unter anderem für die Sicherstellung des störungsfreien, die Persönlichkeits- und Immaterialgüterrechte achtenden Fernmeldeverkehrs.

9.6. Standardisierungskategorie Netzmanagement Daten

9.6.1. Definition

Die Standardisierungskategorie Netzmanagement Daten betrifft alle bei den Rollen Verteilnetzbetreiber, Übertragungsnetzbetreiber, Erzeuger und SDV anfallenden Datenobjekte zur Netzführung. Die bestehenden Standards und Richtlinien sollen, wo möglich, weiterverwendet werden. Die Anforderungen erhalten zunehmende Relevanz aufgrund der zukünftig erhöhten Datenkommunikation und den entsprechenden Auswirkungen auf die Kommunikations- und Dateninfrastruktur.

9.6.2. Schutzbedarf

Für die Beurteilung des Schutzbedarfs in dieser Standardisierungskategorie, wird die höchste Kritikalität pro Sicherheitskriterium (C, I, A) betrachtet. Die Datenobjekte sind mindestens teilweise bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit kritisch. Dies ist bei den SCADA Datenobjekten sowie den Schalt- und Steuersignalen vor allem aus Versorgungssicherheitsgründen der Fall. Es sind aber auch Bereiche mit Datenschutz-Kritikalität vorhanden, wo Prosumer Daten verwendet werden.

Aus dieser Beurteilung können die Anforderungen an die Datensicherheit gestellt werden.

9.6.3. Anforderungen

Um die Datensicherheit zu gewährleisten, werden die folgenden Anforderungen empfohlen. Für die Festlegung der konkreten und angemessenen Massnahmen ist jeweils eine fallbezogene Risikoanalyse (Eintrittswahrscheinlichkeit und Auswirkungsgrad) durchzuführen. Diese Risikobetrachtung sollte bei der Festlegung der Standards und Richtlinien (siehe Kapitel 10) erfolgen. Zusätzlich zu den im Folgenden aufgelisteten Anforderungen müssen in jedem Fall die *übergeordneten betrieblichen Anforderungen*, die *übergeordneten technischen Anforderungen* und die Anforderungen zur *Nachvollziehbarkeit* berücksichtigt werden (siehe Kap. 9.2).

Vertraulichkeit

- Entsorgung von Komponenten / Systemen: Der Schutz der Datenobjekte muss auch nach der Entsorgung erhalten bleibt.
- Accountmanagement: Alle Systeme mit kritischen Datenobjekten müssen Regelungen bezüglich Zugriffe auf und durch Systeme, Gruppen und User Accounts definieren und einhalten.
- Zugriffsschutz: Der logische Zugriff auf die kritischen Datenobjekte soll nur autorisierten Personen ermöglicht werden (z.B. mittels Passwort).
- Geschützter Fernzugriff: Für den Fernzugriff auf die kritischen Datenobjekte gelten dieselben Anforderungen an die Datensicherheit, wie für den Direktzugriff.
- Netzwerktrennung: Um die Vertraulichkeit der Datenobjekte zu schützen, kann gegebenenfalls ein getrenntes Netzwerk eingerichtet werden, je nach erfolgter Risikoabschätzung. Grösstenteils bestehen heute bereits getrennte Netzwerke.
- Sichere Kommunikation: Die Kommunikation der kritischen Datenobjekte über das gewählte Netzwerk muss die Vertraulichkeit sicherstellen.

Integrität

- Konfigurationsmanagement: Die grundlegenden Sicherheitskonfigurationen der Systeme mit kritischen Datenobjekten müssen bestimmt und gepflegt werden.
- Wartung der Komponenten / Systeme: Für alle Systeme mit kritischen Datenobjekten sollen klare Vorgaben zur präventiven und korrektiven Wartung und Pflege bestehen.
- Informationssicherheit (Schutz gegen Angriffe von aussen): Die Systeme mit kritischen Datenobjekten sollen vor Angriffen von aussen (Viren, Malware etc.) geschützt werden.

Verfügbarkeit

- Unterbrechungsfreier Betrieb: Bei einem Unterbruch sollen die kritischen Funktionen zur Erhaltung der Versorgungssicherheit aufrecht erhalten bleiben.
- Kommunikationssysteme für Ereignisfälle: Es sollen Kommunikationssysteme in Betrieb, gewartet und getestet sein, welche im Ereignisfall den Wiederaufbau der Versorgungssicherheit unterstützen.

9.6.4. Bestehende Standards, Gesetze und Richtlinien

Allgemeine Standards, Gesetze und Richtlinien:

- ISO/IEC 27002:Internationaler Standard „IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management“

SG-Standards, Gesetze und Richtlinien (EU oder andere Länder)

- IEC 62351 (Informationssicherheit für den Netzbetrieb und die Erzeugung ; wird zur Zeit im EU Mandat M490 weiter ausgearbeitet, für die neuen Herausforderungen im Smart Grid Umfeld)
- IEC 61850: Allgemeines Übertragungsprotokoll für die Schutz- und Leittechnik in elektrischen Schaltanlagen der Mittel- und Hochspannungstechnik (Stationsautomatisierung)

Weitere gebräuchliche Richtlinien:

- Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme, BDEW Bundesverband der Energie und Wasserwirtschaft e.V., Deutschland

10. Standardisierungs-Roadmap

Zur Erarbeitung künftig geltender Standards und Richtlinien in der Schweiz erscheint es als zwingend, die Aktivitäten im internationalen Umfeld und die bestehenden Standards und Richtlinien im In- und Ausland bei der Planung zu berücksichtigen. In der EU ist insbesondere das Mandat M/490 [1] zu erwähnen, welches einen direkten Einfluss auf die Standards und Richtlinien bezüglich Datensicherheit und Datenschutz im Smart Grid haben wird:

- Der weiterführende Bericht des EU Mandats M/490 „Extension and harmonization of Smart Energy Securtiy Solutions“ soll bis Mitte 2014 publiziert werden[215]. Ein „stable Draft“ sollte bereits Ende 2013 fertiggestellt werden.

Derzeit finden Aktivitäten zur Erarbeitung technischer Mindestanforderungen intelligenter Messsystem beim Endverbraucher auf Basis einer Delegationsnorm an den Bundesrat gemäss dem Gesetzesentwurf zum 1. Massnahmenpaket der ES2050 statt. Eine Standardisierung im Bereich Messsysteme ist daher als prioritär zu betrachten. Der Bereich Messsysteme wird ebenfalls auf europäischer Ebene prioritär behandelt. Derzeit laufen Arbeiten im Bereich Standardisierung für intelligente Messsysteme auf europäischer Ebene im Rahmen des EU Mandats M/441. Es ist daher zu erwarten, dass die Standardisierung in diesem Bereich, welche insbesondere von den Herstellern getrieben werden sollte, in näherer Zukunft grosse Fortschritte machen wird. Internationale Standards sind als massgebend zu verstehen, da eine für die Schweiz spezifische Standardisierung kaum als sinnvoll zu erachten ist. Sie kann zu hohen Mehrkosten und einer Inkompatibilität mit den internationalen Märkten führen. Zur Gewährleistung der Datensicherheit und des Datenschutzes sind jedoch insbesondere weitere Erkenntnisse europäischer Standardisierungsgremien, wie die des M/490, hinzu zu ziehen.

Die Erkenntnisse des Mandats sind ab Mitte 2014 zu erwarten. Sie können daher, vorausgesetzt der entsprechenden Ausgestaltung der gesetzlichen Mindestanforderungen, eine Hilfestellung zur sinnvollen Umsetzung der Datensicherheit und des Datenschutzes bei der Einführung intelligenter Messsysteme durch die Energiebranche bieten.

Bei den weiteren Standardisierungskategorien sollten in einem ersten Schritt jeweils die Anwendungsfälle genauer ausgearbeitet werden und darauf basierend die exakten Datensicherheitsanforderungen abgeleitet und ausgestaltet, sowie die Standards und Richtlinien entsprechend erstellt werden. Auch hier sind die internationalen Arbeiten jedoch massgebend. Sie sind, sofern verfügbar und anwendbar, auf die Schweizer Verhältnisse zu adaptieren.

Die nachfolgende Zeitschiene zeigt einen möglichen groben Fahrplan für die Schweiz auf:

[215] Ref. DTR/SmartM2M-00021 / http://webapp.etsi.org/workProgram/Report_Schedule.asp?WKI_ID=39876

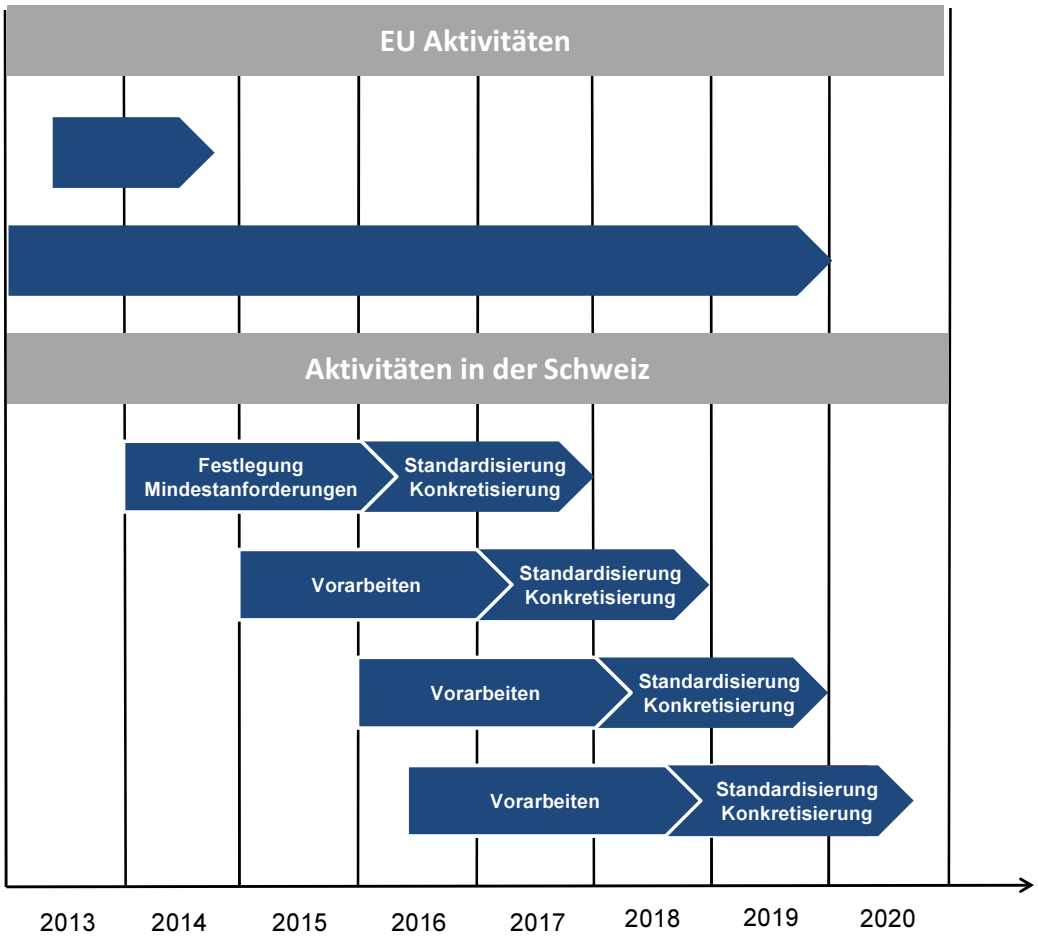


Abbildung 19: Standardisierungs-Roadmap Smart Grid Schweiz

Arbeiten zur Integration von gegebenenfalls internationalen Standards und Schweizerischen Richtlinien sollte je nach Phase und Stand der Arbeiten die folgenden Akteure einbeziehen:

- Bundesbehörden mit Bezug zu den Smart Grid Technologien
- Datenschutz Interessensgruppen
- Regulator
- Übertragungsnetzbetreiber
- Strombranche
- Telekommunikationsbranche
- Industrielle- und Hersteller-Vertreter

Dies stipuliert auch die nationale Strategie zum Schutz vor Cyber Risiken (NCS) [10]. Hier ist die Kritikalität des Stromsystems bereits erkannt worden. Je nach Standardisierungskategorie und zukünftige Entwicklung sind die einzubeziehenden Akteure entsprechend anzupassen und die Liste gegebenenfalls zu erweitern.

30. Juni 2014

AWK Group AG
Leutschenbachstrasse 45
CH-8050 Zürich

VISCHER AG
Schützengasse 1
CH-8021 Zürich

Forschungsstelle für
Informationsrecht (FIR-HSG)
Universität St.Gallen
Guisanstrasse 36

* * * *