Bericht «Data Policy in der Energiebranche»

Juni 2018

Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Hintere Bahnhofstrasse 10, Postfach, 5001 Aarau, Telefon +41 62 825 25 25, Fax +41 62 825 25 26, info@strom.ch, www.strom.ch

Impressum und Kontakt

Herausgeber
Verband Schweizerischer Elektrizitätsunternehmen VSE
Hintere Bahnhofstrasse 10, Postfach
CH-5001 Aarau
Telefon +41 62 825 25 25
Fax +41 62 825 25 26
info@strom.ch
www.strom.ch

Arbeitsgruppe «Data Policy» und Funktionen

Vorname Name	Firma	Funktion
Patrick Baumgartner	CKW	Teilnehmer
Meinrad Engeler	EWZ	Teilnehmer
Gunnar Greiter	SYSDEX	Teilnehmer
Patrick Hauser	AEW	Teilnehmer
Stéphane Henry	Romande Energie	Vorsitz
Schmuel Holles	AWK Group	Beratung & Redaktion
Christoph Joerg	BKW	Teilnehmer
Tobias Keel	AWK Group	Beratung & Redaktion
Wolfgang Korosec	SGSW	Teilnehmer
Georg Meier	AXPO	Teilnehmer
Lyse Pachoud-Haenni	Romande Energie	Teilnehmer
Susanne Weidmann	VSE	Fachsekretariat
Jörg Weyermann	SWiBi	Teilnehmer

Beratung und Umsetzung (für Ausgabe 2017)
AWK Group

Chronologie

Datum	Kurzbeschreibung
Juni 2017	Kickoff Sitzung
Dezember 2017	Vorstellung im Vorstand
Juni 2018	Abschluss überarbeiteter Bericht

Das Dokument wurde unter Einbezug und Mithilfe des VSE und von Branchenvertretern erarbeitet.

Der VSE-Vorstand hat das Dokument am 06.12.2017 zur Kenntnis genommen. Für die Ausgabe 2018 wurden vereinzelte Präzisierungen und Aktualisierungen am Dokument vorgenommen.

Ausgabe 2018

Data Policy in der Energiebranche

Inhalt

Management Summary

Mit fortschreitender Digitalisierung stehen zunehmend geschäftsrelevante Daten und deren zielführende, Mehrwert generierende Verarbeitung im Zentrum der unternehmerischen Aktivitäten. Technische Innovationen sowie eine noch nie dagewesene Fülle an Datenbeständen liefern die Grundlage für ein breites Spektrum möglicher Geschäftsfeldentwicklungen - angefangen bei ergänzenden Ansätzen bis hin zu disruptiven Geschäftsmodellen in den unterschiedlichsten Branchen. Auch in der Energiebranche wird die Informationsverarbeitung definitiv zu einem strategischen Erfolgsfaktor.

Zur Sicherstellung eines geordneten und rechtskonformen, branchenweiten Umgangs mit Daten gilt es, für das Zusammenspiel der Marktteilnehmer eine zweckdienliche **Data Policy** zu erstellen. Diese soll die Grundsätze für relevante Fragestellungen zu Daten-Nutzung, Datenschutz, Datensicherheit sowie Daten-Governance umfassen. Die Data Policy bildet ein gesamtheitliches Framework für den Datenaustausch zwischen Marktteilnehmern bzw. Rollen in der Energielandschaft. Das vorliegende Dokument «Data Policy in der Energiebranche» ist eine erste Version eines solchen Frameworks. Neben einer grundlegenden Strukturierung des Themas soll damit ein Gesamtverständnis für den Umgang mit relevanten Daten aufzeigt und die Einordnung bzw. Einbettung von weiteren Arbeiten am Thema ermöglicht werden.

Um eine solche Data Policy zu erarbeiten, wurden zuerst die **gültigen Rahmenbedingungen** analysiert. Dabei sind rechtliche Grundlagen der Schweiz wie auch der EU zu berücksichtigen. Um die relevanten Anwendungsfälle, Akteure und deren Rollen zu beschreiben, wurden die Auswirkungen von grundlegenden, zukunftsweisenden Trends untersucht. Dazu zählen Liberalisierungen, Dezentralisierung und Fragmentierung, neue Geschäftsmodelle und Dienstleistungen sowie Trends aus energiefremden Branchen.

Auf dieser Basis wurde ein **«Datenmodell» der zukünftigen Energiebranche** entwickelt, welches das für die Data Policy relevante Datenumfeld, die beteiligten Rollen und Stakeholder sowie die geschäftsrelevanten Interaktionen - unter Berücksichtigung der genannten Trends - aufzeigt. Dieses Datenmodell gliedert sich in die drei Bereiche Prosumer, Netzbetrieb und Marktpartner.

Auf Grundlage dieses Datenmodells wurden die Grundsätze zum Umgang mit Daten hinsichtlich **Daten-Nutzung** beschrieben. Dazu wurden die verwendeten Datenobjekte pro Rolle eruiert und die Nutzungsrechte an diesen Datenobjekten definiert. Um die Ansprüche der beteiligten Rollen an den einzelnen Daten-Objekten genauer zu beschreiben, wurde auch deren Verwendungszweck definiert.

Im Abschnitt **Daten-Compliance** werden die durch die identifizierten Rollen zu berücksichtigenden Gegebenheiten und die zu treffenden Massnahmen **bezüglich Datenschutz und Datensicherheit** beschrieben. In einem ersten Schritt wurde eine Übersicht über die zu berücksichtigenden Aspekte erstellt. Aus Perspektive des Datenschutzes zu unterscheiden sind insbesondere personenbezogene und nicht-personenbezogene Daten. Im Hinblick auf die Datensicherheit stehen Anforderungen an die Erfüllung des erforderlichen Schutzbedarfs der Datenobjekte im Vordergrund.

Die **Daten-Governance** schliesslich legt Mechanismen zur Steuerung, Umsetzung sowie nachhaltigen Weiterentwicklung und Pflege der Data Policy fest - sowohl unternehmensintern als auch branchenübergreifend. Inhaltlich werden hierfür die erforderlichen Ziele, Aufgaben, Rollen und Prozesse zur Sicherstellung der Daten-Governance identifiziert.

Für die **Weiterentwicklung und Umsetzung der Data Policy** durch den VSE sind weiterführende Arbeiten notwendig, für die eine Roadmap erstellt wurde. Ein Teil dieser Arbeiten ist bereits am Laufen, ein Teil wird neu lanciert. Im VSE-Bulletin 5/2018 wurde eine erste Publikation zum Thema «Eine Data Policy für die Energiebranche» veröffentlicht.

Management Summary

Du fait de la digitalisation croissante, de plus en plus de données importantes pour les activités commerciales, ainsi que leur traitement efficace et générateur de valeur ajoutée se retrouvent au centre des activités des entreprises. Les innovations techniques et un volume de données encore jamais atteint servent de base à un large éventail d'évolutions commerciales possibles pouvant aller de solutions complémentaires jusqu'à des modèles d'affaires disruptifs dans les branches les plus variées. Dans le secteur énergétique aussi, le traitement des informations devient réellement un facteur stratégique de réussite.

Afin de garantir un traitement des données bien réglé, conforme à la loi et à l'échelle de la branche, il s'agit d'établir une **politique des données (ou «data policy»)** utile pour l'interaction entre les acteurs du marché. Cette politique doit décrire les principes relatifs aux problématiques importantes telles que l'utilisation des données, leur protection et leur sécurité, ainsi que la gouvernance les régissant. La politique des données constitue un cadre global pour l'échange de données entre les acteurs du marché ou les rôles dans le paysage énergétique. Le présent document «Politique des données dans le secteur énergétique» («Data Policy in der Energiebranche») est la première version d'un cadre de ce type. Il entend présenter non seulement une structuration de fond de ce thème, mais aussi une compréhension globale de la manière dont on doit traiter les données importantes et des possibilités de classifier ou d'intégrer de futurs travaux sur ce thème.

Pour établir une telle *data policy*, les **conditions-cadres en vigueur** ont tout d'abord été analysées. Il faut tenir compte des fondements juridiques de la Suisse ainsi que de l'UE. Afin de décrire les cas d'applications pertinents, les acteurs et leurs rôles, on a étudié les répercussions des tendances de fond et porteuses d'avenir, dont font partie les libéralisations, la décentralisation et la fragmentation, les nouveaux modèles d'affaires et prestations de services ainsi que les tendances des secteurs autres que celui de l'énergie.

Sur cette base, on a développé un **«modèle de données» du secteur énergétique du futur**, qui présente l'environnement de données important pour la *data policy*, les rôles et parties prenantes concernés ainsi que les interactions importantes pour les affaires, en tenant compte des tendances précitées. Ce modèle de données se décompose en trois domaines: prosumers, exploitation du réseau et partenaires de marché.

En fonction de ce modèle de données, les principes du traitement des données du point de vue de l'**utilisation des données** ont été décrits. Pour cela, on a identifié les objets de données utilisés pour chaque rôle et défini les droits d'utilisation de ces objets de données. Pour décrire plus précisément les exigences des rôles concernés envers chaque objet de données, leur usage a également été défini.

La partie sur la **conformité à la politique des données (ou «data compliance»)** décrit les éléments à prendre en compte par les rôles identifiés et les mesures à prendre **concernant la protection et la sécurité de données**. Dans un premier temps, on a établi une vue d'ensemble des aspects dont il faut tenir compte. Du point de vue de la protection des données, il faut distinguer en particulier les données personnelles et les données non personnelles. En ce qui concerne la sécurité des données, il s'agit surtout d'exigences quant à la satisfaction des besoins de protection requis des objets de données.

La **gouvernance des données (ou «data governance»)**, enfin, fixe les mécanismes autorisant le pilotage, la mise en œuvre, le développement à long terme et l'actualisation de réglementations d'une politique de données, aussi bien au sein d'une entreprise que pour tout un secteur. Pour ce faire, on détermine les objectifs, tâches, rôles et processus nécessaires à la garantie de la gouvernance des données.

Des travaux supplémentaires sont nécessaires à la **poursuite du développement et à la mise en œuvre de la politique des données** par l'AES; une feuille de route a été établie à cet effet. Une partie de ces travaux est déjà en cours de réalisation tandis que l'autre partie démarre seulement. Un premier article sur le thème de la «data policy» («Une politique des données pour le secteur énergétique») a été publié dans le Bulletin de l'AES 5/2018.

1. Ausgangslage, Betrachtungsbereich und Ziele

Mit fortschreitender Digitalisierung stehen zunehmend geschäftsrelevante Daten und deren zielführende Verarbeitung im Zentrum der unternehmerischen Aktivitäten. Technische Innovationen sowie eine noch nie dagewesene Fülle an Datenbeständen ermöglichen ergänzende Ansätze bis hin zu disruptiven Geschäftsmodellen in den unterschiedlichsten Branchen. Nicht zuletzt in der Energiebranche wird die Informationsverarbeitung zu einem strategischen Erfolgsfaktor. Die zunehmende Dezentralisierung der Wertschöpfungsstrukturen sowie der Eintritt neuer Marktteilnehmer wird dabei die informatorische Komplexität laufend erhöhen.

Zur Sicherstellung eines geordneten branchenweiten Umgangs mit Daten gilt es, für das Zusammenspiel der Marktteilnehmer eine diesbezügliche Data Policy zu erstellen. Diese soll die Grundsätze hinsichtlich der relevanten Fragestellungen zu Daten-Nutzung, Datenschutz, Datensicherheit sowie Daten-Governance definieren. Die Data Policy bildet dabei ein gesamtheitliches Framework für den Datenaustausch zwischen Marktteilnehmern bzw. Rollen in der Energielandschaft.

Die Arbeitsgruppe «Data Policy» (nachfolgend AG Data Policy) befasst sich entsprechend mit der Fragestellung, welchen Grundsätzen der Zugang zu Daten, der Umgang mit Daten und die Sicherheit von Daten genügen müssen. Dabei steht die Strukturierung des Themenfeldes Data Policy, die Definition des für die Data Policy relevanten Datenumfelds, die Identifikation des Regelungsbedarfs sowie die Entwicklung geeigneter Massnahmen im Fokus. Als Ergebnis werden Branchenempfehlungen zur Verfügung gestellt sowie Positionen und Werkzeuge definiert. Abbildung 1 zeigt die für die Erarbeitung dieser Data Policy verwendete Strukturierung des Themenfeldes «Data Policy Energiebranche».

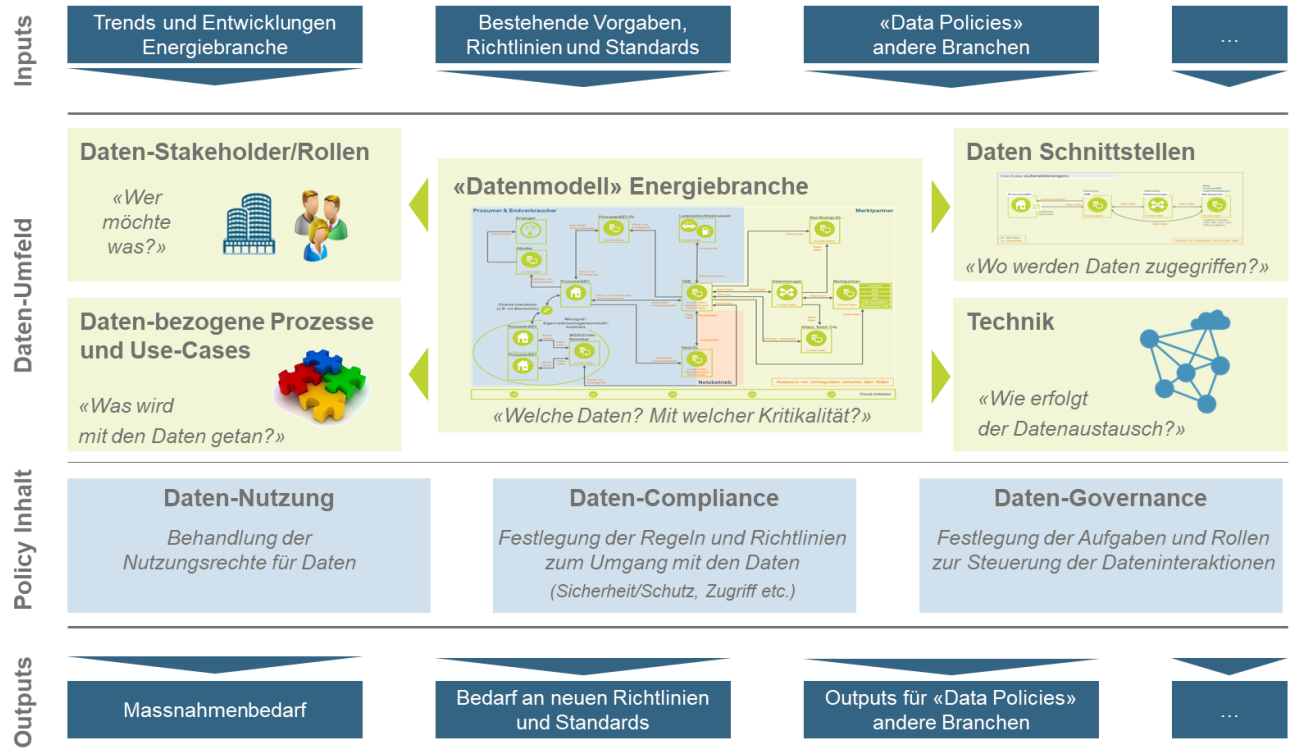

Abbildung 1: Strukturierung Data Policy Energiebranche

Untersucht werden die Fragestellungen, wer welche Daten und Informationen nutzen darf, Art und Zweck der Bearbeitung, sowie welche Sicherheitsmassnahmen entsprechend vorzusehen sind.

Die Data Policy konzentriert sich auf Daten mit klarem Energiebezug. Nicht Bestandteil der Data Policy sind Daten für den Betrieb einer Organisation, ohne direkten Bezug zur Energiebranche wie bspw. Mitarbeiterdaten oder Daten der Buchführung. Die berücksichtigten Daten müssen in einem bereits umgesetzten resp. innerhalb von ca. fünf Jahren realistisch umsetzbaren Anwendungsfall verwendet und zwischen den Marktteilnehmern ausgetauscht werden.

Die Data Policy beinhaltet die folgenden Themenschwerpunkte:

- Identifikation der branchenrelevanten Daten: In geeigneter Detaillierung wird ein «Datenmodell» der zukünftigen Energiebranche zur Verfügung gestellt, welches das für die Data Policy relevante Datenumfeld, die beteiligten Rollen und Stakeholder sowie die geschäftsrelevanten Interaktionen und Trends aufzeigt.

- Definition der Data Policy Regelungen: Auf der Grundlage des Datenmodells werden die Regelungen zum Umgang mit den Daten, hinsichtlich Nutzung, Governance und Compliance (Datenschutz und -Sicherheit) in der Energiebranche beschrieben.

- Planung der Umsetzung der Data Policy: Für die Data Policy wird deren Umsetzung und die weiteren Arbeiten geplant und auf einer Roadmap ausgerollt.

Das vorliegende Dokument «Data Policy in der Energiebranche» ist eine erste Version eines umfassenden Rahmenwerks im Hinblick auf den Umgang mit Daten, welche in den definierten bzw. untersuchten Betrachtungsbereich der Data Policy fallen.

Neben der Strukturierung des Themas soll ein Gesamtverständnis für den Umgang mit entsprechenden Daten aufzeigt und die Einordnung bzw. Einbettung von themennahen Arbeiten ermöglicht werden. Die Data Policy wird laufend weiterentwickelt und konkretisiert werden.

2. Rahmenbedingungen

In diesem Kapitel erfolgt eine einleitende Beschreibung wesentlicher und relevanter Vorgaben für die Data Policy. Sie beinhaltet die Auflistung der zentralen und anzuwendenden Regularien der Schweiz und der Europäischen Union (EU). Zudem wird auf die einzubeziehenden Branchenempfehlungen des VSE hingewiesen. In der AG Data Policy erfolgt eine fortlaufende Ergänzung sowie deren exakte Beschreibung von zukünftig relevanten Artikeln und gesetzgeberischer Trends.

2.1 Rechtliche Rahmenbedingungen Schweiz und EU

Die folgende Abbildung illustriert die relevanten Gesetze und Entwicklungen, welche direkt auf die Data Policy einwirken:

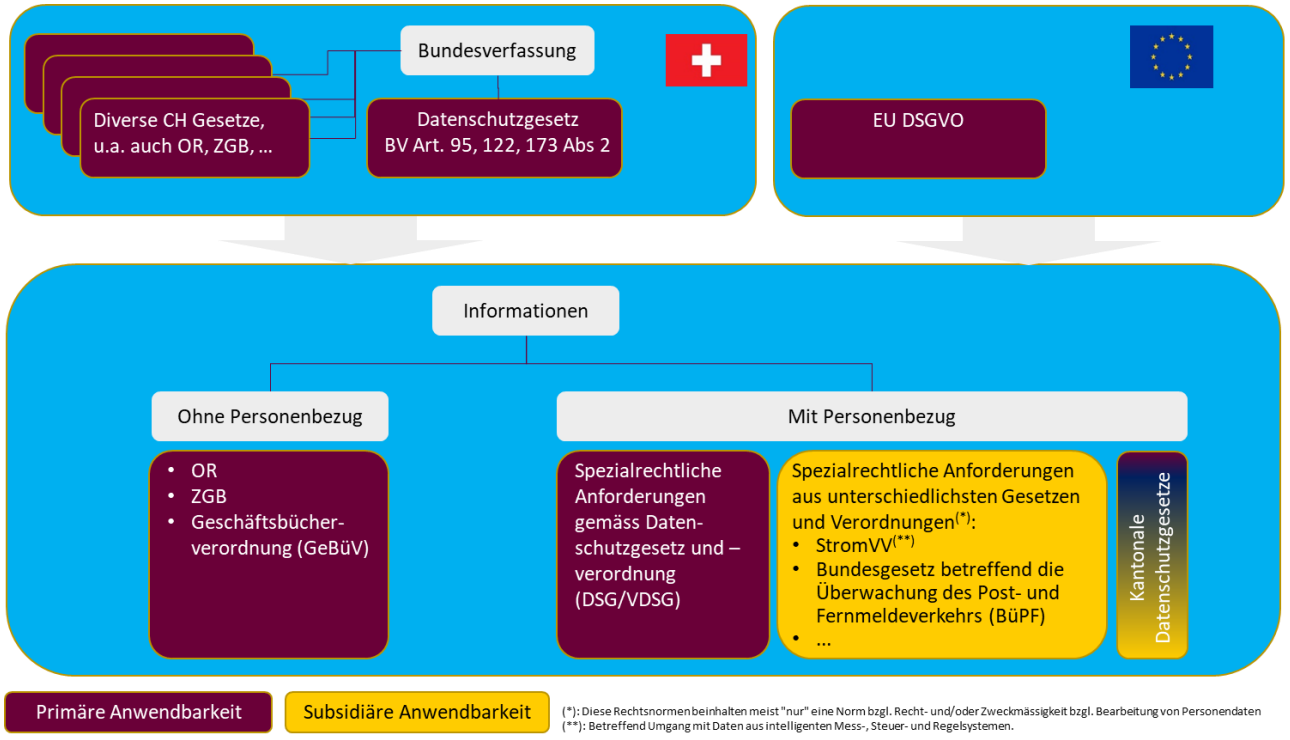

Abbildung 2: Gesetze und Normen im Umfeld der Data Policy

Im Fokus stehen dabei die den Datenschutz betreffenden politischen und gesetzlichen Entwicklungen. Dabei sind sowohl die schweizerische Gesetzgebung, als auch die EU-Normen zu berücksichtigen, sofern ein Unternehmen diesen unterliegt. Obige Abbildung fasst die Gesetzeslage zusammen, wobei vor allem die Gesetze und Normen *mit Personenbezug* als Input zu berücksichtigen sind, d.h.:

- Das Datenschutzgesetz und die Datenschutzverordnung (Schweiz)
- Die Datenschutzgrundverordnung DSGVO (EU)

Das schweizerische Datenschutzgesetz wird aktuell überarbeitet um die Konformität gegenüber der EU zu erhalten. Die Revision des Datenschutzgesetztes wird voraussichtlich in zwei Schritten vorgenommen, wobei der erste Schritt Anpassungen im Hinblick auf das europäische Recht umfassen dürfte.[1] Eine Übersicht der wichtigsten zu erwartenden Änderungen aus der Revision ist im Anhang zu finden.

[1] «Revision des Datenschutzrechtes in zwei Etappen», Medienmitteilung des Bundes vom 12. Januar 2018.

2.2 Mitgeltende Dokumente

Die nachfolgenden Branchenempfehlungen und Positionspapiere des VSE sind als Input für die Data Policy von direkter Bedeutung.

Publizierte Dokumente:

- ***ICT-Continuity***: Die «Umsetzungsempfehlung zur Gewährleistung der ständigen Disponibilität der Informatik- und Kommunikationstechnologie zwecks Sicherstellung der Versorgung» umfasst konkrete Handlungsempfehlungen für die kritische ICT-Infrastruktur der Energieversorgungsunternehmen sowie einen Minimalstandard mit Vorgaben und Anweisungen für die EVU. Sie gilt in den Netzebenen 1 bis 4 als «Best Practice».

- ***Messwesen***: Im Rahmen der Kommissionsarbeiten wurden Themenpapiere zur «Verantwortlichkeit im Messwesen» und zum «Datenschutz und Datensicherheit bei Smart Metering» erarbeitet. Relevante Kernaussagen betreffen die zukünftige Rolle des Netzbetreibers im Messstellenbetrieb sowie die Aufgabe zur Sicherstellung einer integralen End-to-End Datensicherheit bei intelligenten Messsystemen. Ebenso wird auf die Notwendigkeit einer schweizweit einheitlichen Regelung der Datenschutzvorgaben hingewiesen.

Dokumente in Arbeit:

- ***Dokument «Grundschutz für «Operational Technology» in der Stromversorgung»***: Erläutert Konzepte, Empfehlungen und Massnahmen aus verschiedenen heute veröffentlichten Standards, Normen und Dokumente zur ICT-Security im Bereich kritische Infrastrukturen.

- ***Dokument «Sicheres Smart Metering»***: Spezifiziert Anforderungen an Architektur und Entwicklung eines intelligenten Messsystems, welche als Grundlage einer Konformitätsprüfung der entsprechenden Systeme dienen können.

- ***Dokument «Datensicherheit für intelligente Messsysteme»****:* Spezifiziert die detaillierten Anforderungen an ein intelligentes Messsystem hinsichtlich Informations- und Cybersicherheit sowie an Prüfstellen als Auflistung der Kriterien bei der Erstellung von Prüfkatalogen.

3. Trends

Mit Hilfe der aufgeführten Trends sollen die für die Daten relevanten Anwendungsfälle und der Rollen im Energiemarkt beschrieben werden. Um die Trends und damit die Rollen definieren zu können, wurden zukünftige Entwicklungen unter Einbeziehung der Energiestrategie 2050 und der fortschreitenden Digitalisierung ermittelt und in die folgenden vier kategorisierten Trends eingeteilt:

- ***Liberalisierungen:*** Rollen und Datenaustausche im Zuge der heutigen und zukünftigen Liberalisierungen im Energiebereich.

- ***Dezentralisierung und Fragmentierung:*** Rollen und Datenaustausche im Zuge der zunehmenden Dezentralisierung im Produktion-, Netz- und Marktbereich der Energielandschaft.

- ***Neue Geschäftsmodelle und Dienstleistungen:*** Rollen und Datenaustausche, welche auf Grund neuer Geschäftsmodelle und Energie-Dienstleistungen entstehen, soweit aus heutiger Sicht absehbar.

- ***Branchenschnittstellen:*** Rollen und Datenaustausche, welche auf Grund branchenübergreifenden Trends entstehen, wo energiefremde Stakeholder inhaltliche Schnittstellen zur Energiebranche haben.

Für jeden Trend werden im Folgenden die zukünftigen Entwicklungen und Technologien, die Rollen und das Zusammenspiel innerhalb des Trends, im Sinne eines Anwendungsfalles, beschrieben. Daraus werden dann die für die drei Themenbereiche Daten-Nutzung, Daten-Compliance und Daten-Governance relevanten Fragestellungen der Data Policy abgeleitet. Die exakte Beschreibung der im Weiteren verwendeten Rollen findet sich im Anhang.

3.1 Liberalisierungen

Im Bereich Liberalisierungen stehen primär die volle Strommarktöffnung und die Gasmarktöffnung im Vordergrund. Dieser Trend beinhaltet daher im Wesentlichen die heute bereits definierten Rollen und Datenaustausche rund um die Meter-Daten.

Rollen — Die entsprechenden Rollen sind der Prosumer[2], der Verteilnetzbetreiber (VNB), der Datenrouter und die Marktpartner (SDAT-Rollen).

Technologien — Wichtige Technologien und Systeme in diesem Bereich sind das Smart Metering, ein Datahub für den Datenrouter und das Energiedatenmanagement (EDM) beim VNB und den Marktpartnern.

Beschreibung Trend

Unter Prosumer verstehen wir den Energie-Endabnehmer, der auch in der Lage sein kann selber Energie zu produzieren. Er ist ausgerüstet mit einem intelligenten Messgerät (iMG) um die Meter-Daten zu generieren und dem Verteilnetzbetreiber zuzustellen. Er erhält in diesem Trend vom Verteilnetzbetreiber Daten zum Beispiel zur Visualisierung der Meter-Daten.

Der Verteilnetzbetreiber (VNB) ist in diesem Szenario zuständig für die Netznutzung. Er erhält die Meter-Daten der Prosumer, speichert Kundendaten und gibt Meter-Daten an einen potentiellen Datenrouter oder den Marktpartner weiter. Je nach Marktpartneranbindung erfolgt dabei der Datenaustausch direkt bidirektional oder über den Datenrouter.

[2] Die Rolle Prosumer, zusammengesetzt aus Energie-Endverbraucher (Englisch: Consumer) und Energie-Produzent (Englisch: Producer), umfasst in diesem Dokument sowohl reine Endverbraucher als auch Verbraucher mit zusätzlicher Produktions- resp. Speicherkapazitäten.

Der Datenrouter ist in diesem Trend zuständig für den kontrollierten Austausch von Daten zwischen definierten Teilnehmern. Er tauscht Meter-Daten mit dem VNB und dem Marktpartner aus und speichert ebenfalls Kundendaten.

Der Marktpartner ist zuständig für die Rechnungsstellung, die Prognosen, das Angebotsmanagement oder das Bilanzgruppenmanagement (je nach SDAT-Rolle). Marktpartner können Lieferanten, Erzeuger, VNB, Übertragungsnetzbetreiber (ÜNB), Bilanzgruppenverantwortlicher (BGV), Systemdienstleistungsverantwortlicher (SDV) oder die Herkunftsnachweis-Ausstellerin (HKN-Ausstellerin) sein.

Zwischen allen Rollen werden zusätzlich die Vertragsdaten ausgetauscht.

Die nachfolgende Abbildung illustriert diesen Trend:

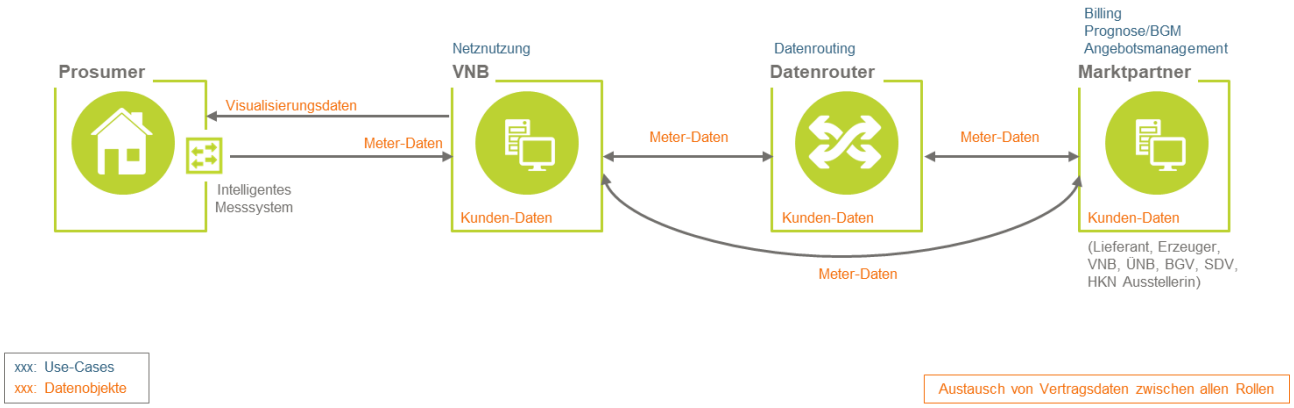

Abbildung 3: Trend «Liberalisierungen»

Auswirkungen Daten-Nutzung

Im Bereich Daten-Nutzung muss geklärt werden, wo die Nutzungsrechte der hier übergreifend genutzten Daten liegen, in diesem Trend also betreffend Meter-Daten, Kundendaten und Vertragsdaten. Ebenso ist generell bei den Nutzungsberechtigten festzuhalten, was im jeweiligen Fall eine zweckmässige Verwendung der Daten darstellt, d.h. was die primären Verwendungszwecke der Daten sind (Zweckbindung gemäss Datenschutzgesetz).

Auswirkungen Daten-Compliance

Das Thema Daten-Compliance beinhaltet die Schwerpunkte Datenschutz und Datensicherheit. Für den Datenschutz ist generell bei den Nutzungsberechtigten der Daten festzuhalten, welche Datenschutzvorgaben für die Haltung und Nutzung der hier betroffenen Daten zu berücksichtigen sind (Profiling, Weiterreichung, Portabilität, Anonymisierung etc.). Für die Datensicherheit sind Empfehlungen und Massnahmen zu definieren, welche die Sicherheit der Daten sowohl aus Sicht Datenschutz als auch aus Sicht Versorgungssicherheit gewährleisten.

Auswirkungen Daten-Governance

Im Bereich Daten-Governance sind die abzuleitenden Verantwortungen festzulegen, was insbesondere das Zusammenspiel der Rollen und Aufgaben innerhalb des Unternehmens betrifft, damit sichergestellt werden kann, dass die Data Policy nachhaltig umgesetzt und gelebt wird.

3.2 Dezentralisierung und Fragmentierung

Die Fragmentierung der Netze in Richtung Microgrids, die Dezentralisierung der Energie-Erzeugung im Prosumer-Bereich sowie die Nationalisierung, bzw. auch Internationalisierung der Energie-Lieferung und des

Energie-Handels sind im Trend Dezentralisierung und Fragmentierung zusammengefasst. Die Dezentralisierung und die damit einhergehende Fragmentierung der Energielandschaft ist sehr stark digitalisierungsgetrieben und bringt entsprechend neue Rollen und Datenaustausche mit sich.

Rollen	Dieser Trend beinhaltet die Rollen Microgrid / Eigenverbrauchsgemeinschaft (EVG) / Arealnetz (AN)-Betreiber, Prosumer, VNB, dezentraler Erzeuger und Energiehändler.
Technologien	Wichtige Technologien und System in diesem Szenario sind die Steuerungssysteme beim VNB und/oder Microgrid-Betreiber, der Einsatz der dezentralen Energieerzeugungsanlagen (EEA), mögliche Handelsplattformen im Prosumer-Bereich (ETRM-Systeme) sowie der Einsatz direkter Endnutzer-Transaktionstechnologien wie der Blockchain-Technologie.

Beschreibung Trend

Der Prosumer ist auch hier ausgestattet mit einem intelligenten Messgerät (iMG) und hat die Möglichkeit, selber Energie zu erzeugen. Er generiert und liefert Meter-Daten. Er fungiert in diesem Trend als Endverbraucher, Energie-Einspeiser und Eigenverbraucher. Der Prosumer kann in diesem Trend eigenständig oder Teil eines Microgrids, einer EVG oder eines AN sein.

Ist der Prosumer in einem Microgrid/EVG/AN (ab hier zusammengefasst benannt als Microgrid) integriert, erhält er die Steuersignale von der Microgrid-Führung statt vom VNB. Das Microgrid umfasst somit neben dem Prosumer noch die Rolle des Microgrid-Betreibers (MG/EVG/AN-Betreibers), der die Microgrid-Führung innehat. Der MG/EVG/AN-Betreiber liefert aufgrund der Meter-Daten vom Prosumer und den Steuersignalen von Ausserhalb des Microgrids die Steuersignale an den internen Prosumer. Er speichert zudem die Kundendaten der internen Prosumer. Der MG/EVG/AN-Betreiber liefert schliesslich die Meter-Daten des gesamten Microgrids an den VNB, für den Fall eines nicht-autarken Betriebs.

Der VNB hat in diesem Trend die Aufgabe der Netzführung. Er erhält die Meter-Daten der Netzteilnehmer und sendet netzdienliche Steuersignale an diese.

Neben der Produktion- und Netzseite ist auch eine Dezentralisierung im Handels-/Vertriebsumfeld denkbar, z.B. mittels digitalisierten Handelsplattformen. Der Prosumer stellt seinen Bedarf oder seine Flexibilitäten in Form von Prognose- oder Fahrplandaten auf der Plattform ein und initiiert entsprechend die Bedarfsdeckung oder den Kapazitätsverkauf.

Zusätzlich werden zukünftig möglicherweise direkte energiebezogene Transaktionen zwischen den Prosumern stattfinden, mit Hilfe entsprechender Technologien wie der Blockchain-Technologie. Ohne Zwischenstufe erfolgt der Energiehandel direkt zwischen den teilnehmenden Prosumern, welche mithin dann auch für ihre eigenen Daten verantwortlich sind.

Auch in diesem Trend werden zusätzlich die Vertragsdaten zwischen allen Rollen ausgetauscht.

Abbildung 4 illustriert diesen Trend.

Auswirkungen

Zusätzlich zu den oben bereits aufgeführten Fragestellungen ist aus Data Policy Sicht hier festzuhalten, dass in der Regel die minimal erforderlichen Empfehlungen und Massnahmen aus Sicht Datenschutz, -Sicherheit und -Governance zu definieren sind, damit sowohl grosse als auch kleine Unternehmen diese in ihren jeweiligen Rollen wahrnehmen können.

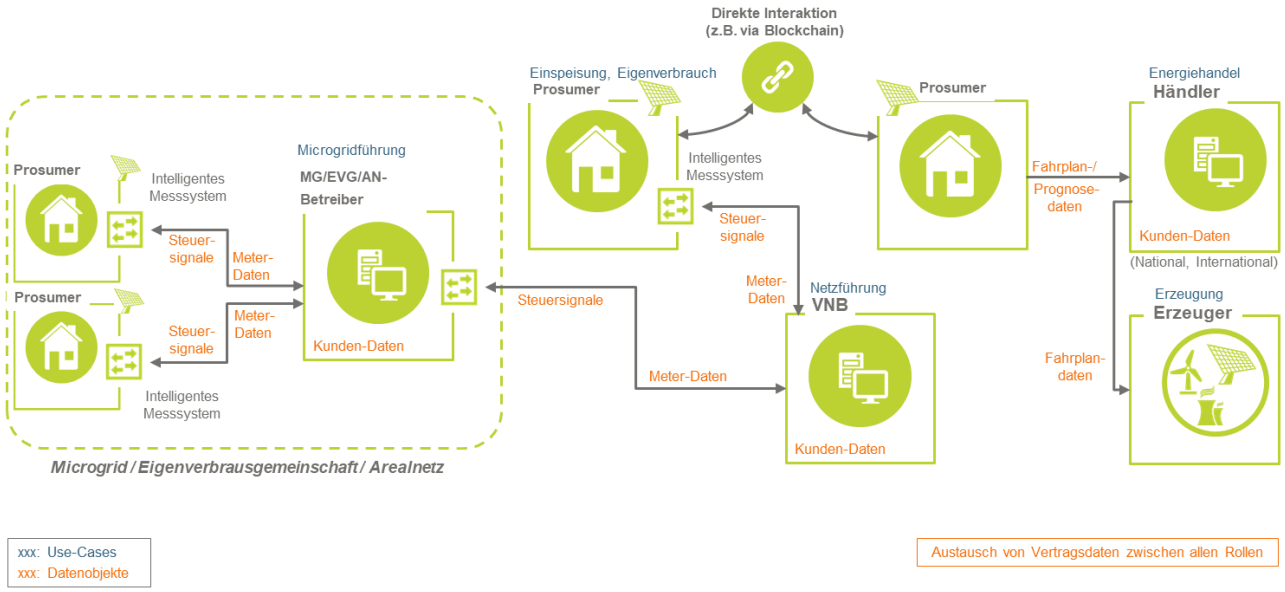

Abbildung 4: Trend «Dezentralisierung und Fragmentierung»

3.3 Neue Geschäftsmodelle und Dienstleistungen

Trends im Bereich Geschäftsmodelle und Dienstleistungen umfassen neben der klassischen Energieversorgung, die Bereitstellung von Energie-Dienstleistungen. Dies sowohl zu Hause (Anlagen-Management), für das Energienetz (Netzmanagement), aber auch sogenannte «Non-Energy-Dienstleister». Dies sind Dienstleister, welche nicht Teil der Energiewertschöpfung sind, jedoch auf Energiedaten zugreifen möchten. (bspw. für Kundenprofiling). Das Aufkommen neuer Geschäftsmodelle und Dienstleistungen bringt diverse neue Rollen, Datenzugriffsbedürfnisse und einen entsprechenden Datenaustausch mit sich. Die Rollen lassen sich entsprechend ihrer Kundenausrichtung als «Prosumer-Dienstleister», «Netz-Dienstleister» sowie «Non-Energy-Dienstleister» kategorisieren.

Rollen — Damit sind die Rollen in diesem Trend der Prosumer, der VNB, der Netz-Dienstleister, der Prosumer-Dienstleister, der Dienstleister «Non-Energy» sowie auch ggf. der Datenrouter für den Meter-Daten-Austausch.

Technologien — In diesem Trend gehören Smart Meter, Energie-Management-Systeme (EMS) und flexible Gebäudeanlagen (EEA, Lasten, Speicher) im Heim-Bereich, sowie Steuerungssysteme auf der Netzseite zu den wesentlichen Technologien. Lösungen im Bereich Internet of Things (IoT), Big Data und Data Analytics werden das Aufkommen dieser Dienstleistungen beschleunigen.

Beschreibung Trend

Die Rolle des Prosumers ist hier der Dienstleistungsempfänger, in dem dieser seine flexiblen Kapazitäten potentiellen Energiedienstleistern zur Verfügung stellt. Es werden auch hier wieder Meter-Daten an den VNB geliefert und zusätzlich Steuersignale von verschiedenen Rollen empfangen.

Der VNB hat in diesem Trend die Aufgabe der Sicherstellung eines stabilen Netzbetriebes. Hierzu misst er die Prosumer und hat die Möglichkeit, sie oder deren Dienstleister im Bedarfsfall zu steuern. Zusätzlich, bei Beauftragung eines Netz-Dienstleisters mit netzbetrieblichen Aufgaben, werden an dieser Schnittstelle Asset- und GIS-Daten, SCADA-Daten sowie Kundendaten ausgetauscht.

Der Prosumer-Dienstleister (Prosumer-DL) kommt in diesem Trend neu als Rolle hinzu, um Prosumer-Dienstleistungen anzubieten, die sich aus den flexiblen Kapazitäten des Prosumers ergeben. Solche

Dienstleistungen könnten zum Beispiel virtuelle Kraftwerke, Demand-Side-Response- oder integrierte Heim-Energiemanagement-Lösungen sein. Der Prosumer-DL erhält Anlage-Messdaten vom Prosumer sowie Meter-Daten und Anreiz-Signale vom VNB. Anhand dieser liefert er Steuersignale zum Prosumer. Zudem speichert der Prosumer-DL Kundendaten.

Eine weitere Rolle in diesem Trend ist der Netz-Dienstleister (Netz-DL), der aus dem VNB ausgegliederte Netzdienstleistung anbietet. Solche Dienstleistungen sind beispielsweise die Netzführung, das Asset Management oder der Messstellenbetrieb. Der Netz-DL erhält je nach ausgegliedertem Service die erforderlichen Auftrags-Daten, Asset-Daten, GIS-Daten und SCADA-Daten vom VNB und liefert diesem allfällige Ereignisdaten, z.B. zu Störungen. Im Fall eines Messstellenbetriebs werden die Meter-Daten und Kundendaten direkt vom Prosumer empfangen und dieser mit Steuer- und Anreiz-Signalen gesteuert.

Der VNB hat in diesem Trend auch die Möglichkeit, Meter-Daten an externe «Non-Energy»-Dienstleister («Non-Energy»-DL) weiterzugeben, welche Dienstleistungen ausserhalb der Energiebranche anbieten. «Non-Energy»-DL speichern Kundendaten und nutzen die gelieferten Meter-Daten für ihre Dienstleistungen, zum Beispiel für Werbezwecke. Ggf. werden die Meter-Daten hierfür via Datenrouter ausgetauscht.

Auch in diesem Trend werden zusätzlich die Vertragsdaten zwischen allen Rollen ausgetauscht.

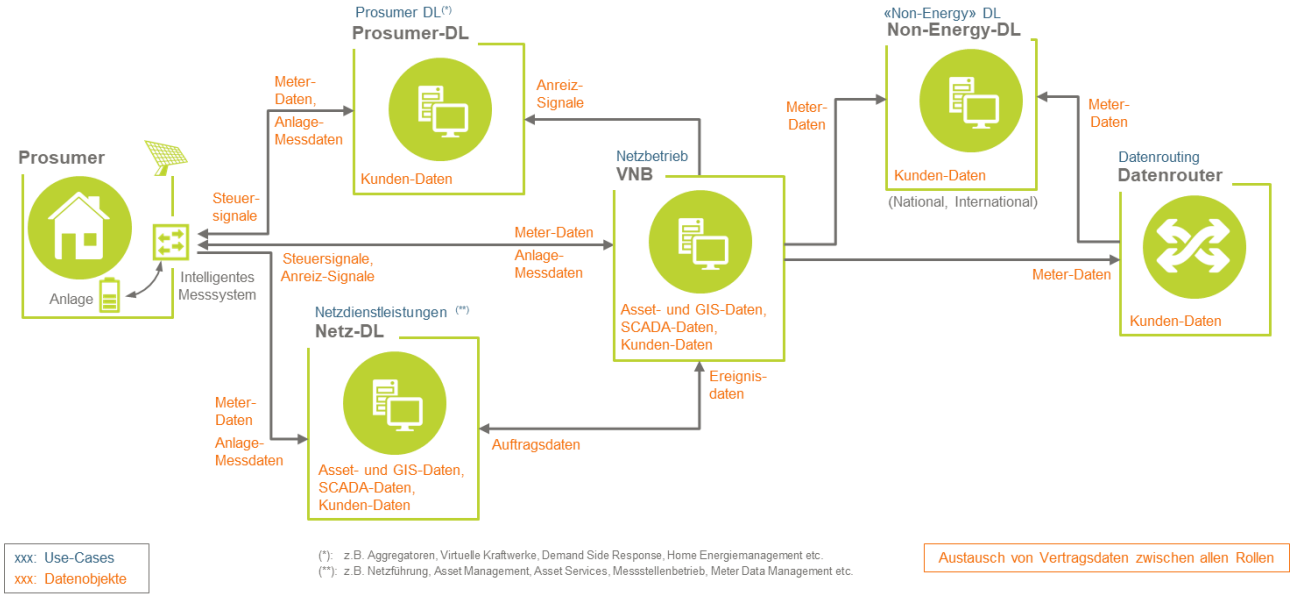

Abbildung 5: Trend «Neue Geschäftsmodelle» und Dienstleistungen

Auswirkungen

Die für die Data Policy relevanten Auswirkungen sind identisch wie bei den vorigen Trends.

3.4 Branchenschnittstellen

Branchenschnittstellen beinhalten Trends aus energiefremden Branchen, welche jedoch themenbezogene Schnittstellen zur Energielandschaft aufweisen. Prominente aktuelle Beispiele betreffen die Themenbereiche Smart City und Elektromobilität. Die diesbezüglichen Stakeholder haben Bedarf an Zugriff auf oder Austausch von Energiedaten und sind dementsprechend hier zu berücksichtigen. Als Spezialfall eines «branchenfremden» Akteurs wird hier zusätzlich auch der Cloud-Anbieter aufgeführt, welcher Outsourcing-Dienstleistung im ICT-Bereich an die Energieunternehmen anbietet.

Rollen

Die primären Stakeholder sind in diesem Fall aktuell die städtischen Verwaltungen und Behörden im Smart-City-Umfeld («Akteur Smart City») sowie Anbieter von Elektromobilitäts-Anwendungen im Sinne von Ladestationen (LS) oder Elektromobilen. Als

Spezialrolle werden in diesem Trend die Cloud-Anbieter für ihre Cloud-Dienstleistungen aufgeführt Dabei kann es sich neben typischen Cloud-Dienstleistungen auch um weiterführende Outsourcing-Dienstleistungen handeln.

Technologien — Zentrale Enabler-Technologien sind hier die zunehmende Verbreitung von Ladestationen für die Elektromobilität sowie die Cloud-Technologien.

Beschreibung Trend

Ausgangspunkt in diesem Trend ist wieder der Prosumer, der mit einem iMG ausgestattet ist und Meter-Daten an den VNB liefert.

Der VNB speichert die Meter-Daten und Kundendaten. Er leitet in diesem Trend die Meter-Daten an den Smart-City-Akteur weiter, zu deren Integration in dessen Smart-City-Aktivitäten und -Dienstleistungen.[3] Seine Schnittstelle zur Elektromobilität besteht aus dem Ablesen der Meter-Daten und netzdienlichen Ansteuerung bzw. Beeinflussung des Lade- und Einspeiseverhaltens. Ggf. könnten zukünftig auch weitere elektromobilitätsbezogene Daten dem VNB zur Verfügung gestellt werden (z.B. Batteriefüllstände).

Ebenfalls hier berücksichtigt ist die Rolle des Cloud-Anbieters. Er kann national oder international tätig sein und bearbeitet die Daten. Hier sind Schnittstellen zu jedem Marktteilnehmer möglich. Für die Datenbearbeitung im Ausland muss ein adäquater Schutzlevel sichergestellt werden.

Auch in diesem Trend werden zusätzlich die Vertragsdaten zwischen allen Rollen ausgetauscht.

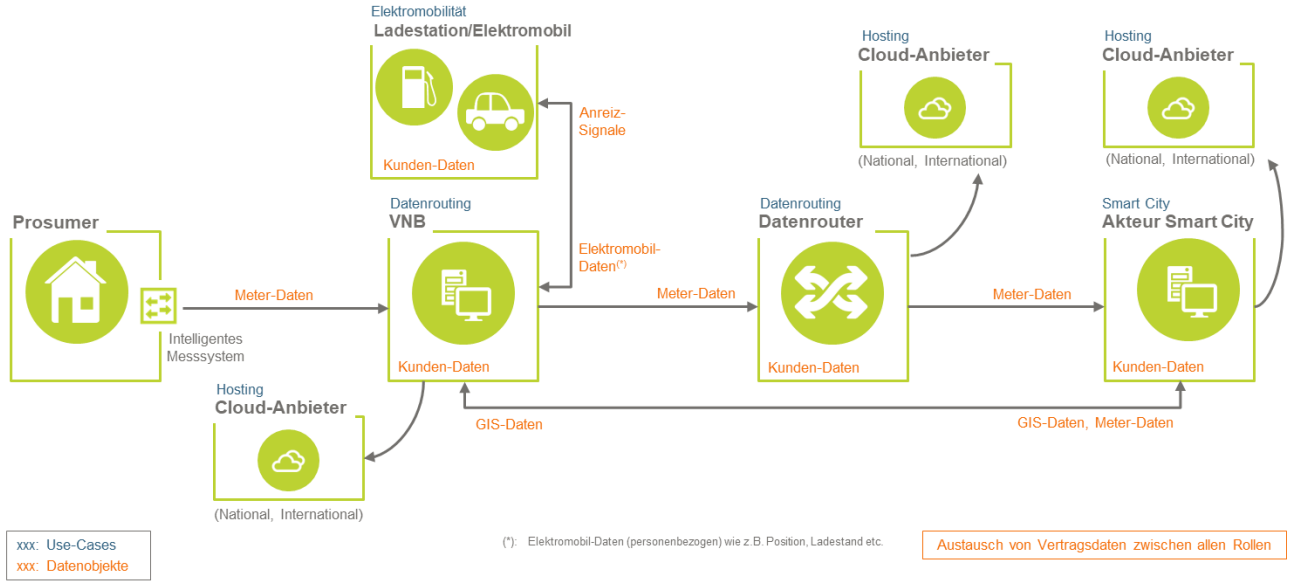

Abbildung 6: Trend «Branchenschnittstellen»

Auswirkungen

Die für die Data Policy relevanten Auswirkungen sind im Wesentlichen identisch wie bei den obigen Trends. Zusätzlich kommt hier auf Grund der Cloud-Dienstleistungen die Fragestellung nach der Anwendbarkeit resp. Pflicht zur Berücksichtigung von grenz- und raumüberschreitenden Aspekten zum Tragen. Dabei können in- und ausländische Regularien in Bezug auf den Datenschutz zur Anwendung kommen.

[3] Aufgrund der StromVV können keine Daten aus Mess-, Steuer-, und Regelsystemen ohne die ausdrückliche Einwilligung der betroffenen Person weitergegeben werden. Dabei unterscheidet die StromVV nicht zwischen natürlichen und juristischen Personen.

4. Datenmodell

Das Datenmodell fasst das Gesamtdatenmodell zusammen. Es beinhaltet die Darstellung des Gesamtmodells, welches aus obigen Teilmodellen (Abbildungen 3-6) zusammengesetzt ist. Da die für die Data Policy relevanten Auswirkungen vom Verwendungszweck der einzelnen Datensätze abhängig ist, wird das Datenmodell zweckmässig in die folgenden drei Domänen gegliedert:

- ***«Prosumer»:*** Die Domäne Prosumer umfasst das netz- und energiewirtschaftliche Messen sowie das Steuern der Prosumer-Kapazität.

- ***«Netzbetrieb»:*** Die Domäne Netzbetrieb beinhaltet den Datenaustausch mit Netz-Outsourcing-Dienstleistern für netzbetriebliche Aufgaben.

- ***«Marktpartner»:*** Diese Domäne vereint den Austausch von Verbrauchs- und Erzeugungsdaten mit den Marktpartnern für deren Abrechnung und sekundäre Nutzung (Prognose, Angebote, Non-Energy-Nutzung etc.).

Die folgende Abbildung stellt das Gesamtdatenmodell dar.

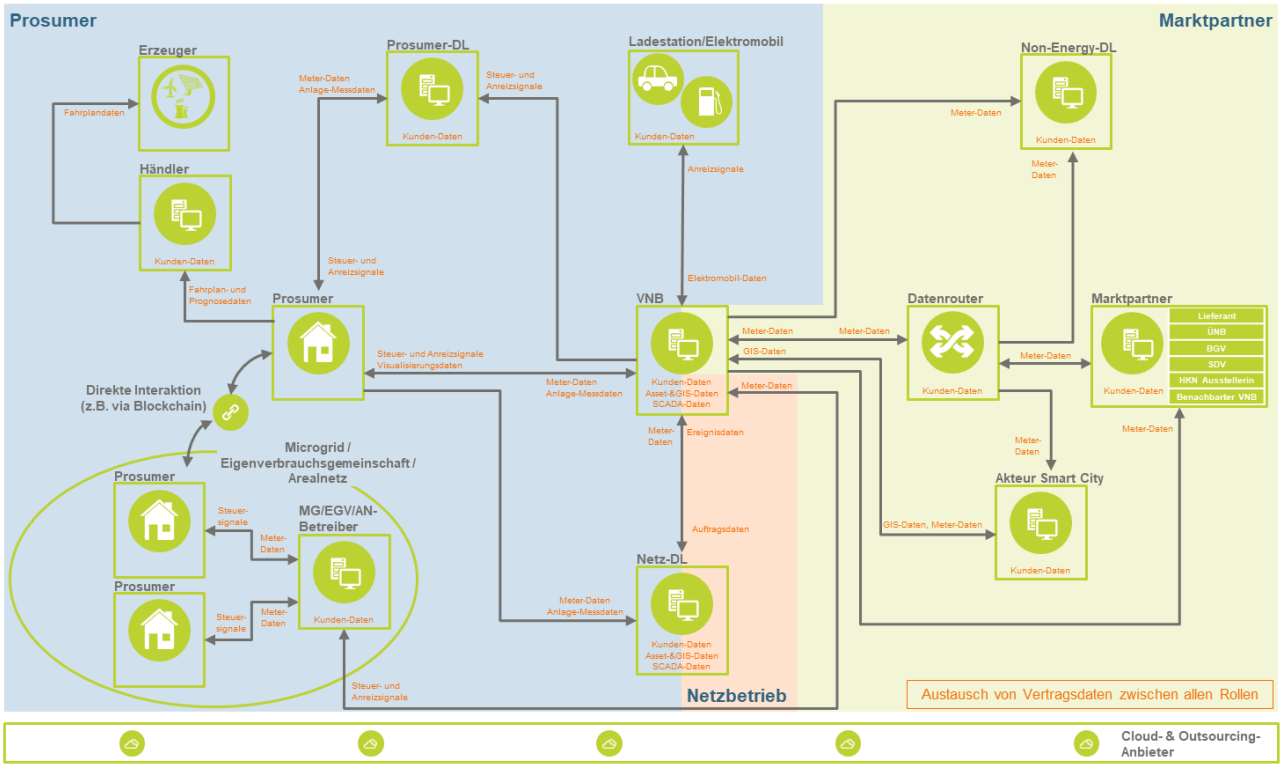

Abbildung 7: Datenmodell

5. Daten-Nutzung

Für die spätere Ableitung der notwendigen Massnahmen in den Bereichen Daten-Compliance, bestehend aus Datenschutz und Datensicherheit, sowie Daten-Governance, müssen zuerst die verwendeten Datenobjekte pro Rolle eruiert, sowie die Nutzungsrechte an diesen Datenobjekten definiert werden. Um die Ansprüche der beteiligten Rollen an den einzelnen Daten-Objekten genauer zu beschreiben, wird deren Verwendungszweck identifiziert und darauf basierend die Daten-Nutzung definiert.

Dieses Kapitel schafft entsprechende Grundlagen mit der Festlegung des Verwendungszweckes und der Nutzungsrechte pro Datenobjekt und Rolle. Aus Gründen der besseren Darstellbarkeit erfolgt diese Festlegung separat pro Domäne.

5.1 Daten-Nutzung Domäne «Prosumer»

Die Domäne «Prosumer» (siehe Tabelle 1) ist gekennzeichnet durch Daten-Objekte, welche mit einem individuellen Bezug auf den Prosumer erzeugt werden. Teilweise werden diese Daten direkt beim Prosumer erzeugt (z.B. Meter-Daten oder Anlage-Messdaten), teilweise werden sie aber auch durch eine andere Rolle erzeugt (z.B. Steuer- & Anreizsignale). Unabhängig vom Ort der Erzeugung liegt das Nutzungsrecht all dieser Daten bei der Rolle «Prosumer».

Ähnlich verhält es sich mit den Daten-Objekten, welche individuell für die Rolle «Ladestation & Elektromobilität» erzeugt werden. Solange es sich dabei um personenbezogene Daten handelt, liegt das Nutzungsrecht für diese Daten-Objekte bei der Rolle «Ladestation & Elektromobilität»

Ein Sonderfall sind die Vertragsdaten. Sie definieren das vertragliche Verhältnis zwischen mindestens zwei Partnern und enthalten vertragliche Konditionen wie beispielsweise Vertragslaufzeit, hinterlegte Produkte und Dienstleistungen oder kommerzielle Bedingungen. Das Nutzungsrecht liegt jeweils gemeinsam bei allen am Vertrag beteiligten Rollen, wofür eine «Joint»-Daten-Nutzung definiert wurde. Die Weitergabe und der Verwendungszweck dieser Vertragsdaten wird jeweils zwischen den beteiligten Parteien geregelt.

Die nachfolgende Tabelle zeigt für diese Domäne, bei welcher Rolle die Nutzungsrechte für die Daten liegen. In dieser Rollen-/Daten-Abbildungsmatrix sind für jeden Datensatz und jede Rolle die dedizierten Verwendungszwecke aufgeführt. Pro Datensatz (Tabellenspalte) ist die Rolle, welche über das Nutzungsrecht verfügt, mit einem «N» markiert.

Domäne «Prosumer»	Kundendaten	Vertragsdaten	Meter-Daten (inkl. Visualisierung)	Anlage-Messdaten	Elektromobil-Daten	Fahrplan- & Prognosedaten	Steuer- & Anreizsignale
Prosumer	• Generierung (N)	• Verwaltung (N)	• Generierung • Visualisierung (N)	• Generierung • Visualisierung (N)	• -	• Generierung (N)	• Anlagensteuerung (N)
Verteilnetz-betreiber	• Billing • Netznutzung	• Verwaltung (N)	• Billing • Netznutzung • Netzstabilität • Bilanzierung • Bereitstellung	• Netzstabilität	• Netzstabilität	• -	• Anlagensteuerung
Prosumer-Dienstleister	• Billing • Produkt-Entwicklung	• Verwaltung (N)	• Billing • Produkt-Entwicklung • Steuerung	• Billing • Produkt-Entwicklung • Steuerung	• -	• -	• Anlagensteuerung
Microgrid-Betreiber	• Billing • Netznutzung	• Verwaltung (N)	• Billing • Netzstabilität • Netznutzung • Bilanzierung	• -	• -	• -	• Anlagensteuerung
Ladestation & Elektromobilität	• Bereitstellung (N)	• Verwaltung (N)	• -	• -	• Bereitstellung • Visualisierung (N)	• -	• Anlagensteuerung (N)
Netz-Dienstleister	• Billing • Netznutzung	• Verwaltung (N)	• Billing • Netznutzung • Netzstabilität • Bilanzierung • Bereitstellung	• Netzstabilität	• Netzstabilität	• -	• Anlagensteuerung
Händler	• Billing • Produkt-Entwicklung	• Verwaltung (N)	• -	• -	• -	• Energiehandel	• -

Tabelle 1: Nutzungsrecht für Daten (N) und Verwendungszweck Domäne «Prosumer»

5.2 Daten-Nutzung Domäne «Netzbetrieb»

Wie die Domäne «Prosumer», enthält die Domäne «Netzbetrieb» (siehe Tabelle 2) ebenfalls die Datenobjekte Kundendaten, Vertragsdaten und Meter-Daten. Das Nutzungsrecht an diesen wird, wie bereits im vorigen Kapitel beschrieben, der Rolle «Prosumer» zugeordnet.

Neu in dieser Domäne sind diejenigen Datenobjekte, welche keinen direkten Bezug zur Rolle «Prosumer» haben und durch den Verteilnetzbetreiber selber erzeugt und verwendet, sowie ggf. an einen Netz-Dienstleister ausgelagert werden. Diese Datenobjekte (Asset-, GIS-, SCADA-, Auftrags- und Ereignisdaten) haben keinen Personenbezug und das Nutzungsrecht liegt bei der Rolle «Verteilnetzbetreiber».

Für die Vertragsdaten gilt wie bei der Domäne «Prosumer» die gemeinsame «Joint»-Daten-Nutzung an den Daten durch die beteiligten Vertragspartner.

Domäne «Netzbetrieb»	Kundendaten	Vertragsdaten	Meter-Daten (inkl. Visualisierung)	Asset- & GIS-Daten	SCADA-Daten	Auftragsdaten	Ereignisdaten
Prosumer	• Generierung (N)	• Verwaltung (N)	• Generierung • Visualisierung (N)	• -	• -	• -	• -
Verteilnetz-betreiber	• Billing • Netznutzung	• Verwaltung (N)	• Billing • Netznutzung • Netzstabilität • Bilanzierung • Bereitstellung	• Dokumentation • Asset Mgmt • Netzbetrieb (N)	• Netzführung • Netzstabilität (N)	• Asset Mgmt (N)	• Netzführung • Netzstabilität • Asset Mgmt (N)
Netz-Dienstleister	• Billing • Netznutzung	• Verwaltung (N)	• Billing • Netznutzung • Netzstabilität • Bilanzierung • Bereitstellung	• Dokumentation • Asset Mgmt • Netzbetrieb	• Netzführung • Netzstabilität	• Asset Mgmt	• Netzführung • Netzstabilität • Asset Mgmt

Tabelle 2: Nutzungsrecht für Daten (N) und Verwendungszweck Domäne «Netzbetrieb»

5.3 Daten-Nutzung Domäne «Marktpartner»

Die Domäne «Marktpartner» enthält keine neuen Datenobjekte. Das Nutzungsrecht an den dort verwendeten Datenobjekten liegt somit bei der Rolle «Prosumer» für die Kundendaten und Meter-Daten sowie beim Verteilnetzbetreiber für die GIS-Daten. Für die Vertragsdaten gilt, wie in den vorher beschriebenen Domänen, das Nutzungsrecht in Form von einer «Joint»-Daten-Nutzung bei den beteiligten Vertragspartnern.

Domäne «Marktpartner»	Kundendaten	Vertragsdaten	GIS-Daten	Meter-Daten
Prosumer	• Generierung (N)	• Verwaltung (N)	• Visualisierung	• Generierung • Visualisierung (N)
Verteilnetzbetreiber	• Billing • Netznutzung	• Verwaltung (N)	• Dokumentation • Asset Mgmt • Netzbetrieb (N)	• Billing • Netznutzung • Netzstabilität • Bilanzierung • Bereitstellung
Datenmanager	• Zuordnung	• Verwaltung (N)	• -	• Weiterverteilung • Bilanzierung
Non-Energy-Dienstleister	• Vergütung / Billing • Produktentwicklung	• Verwaltung (N)	• -	• Produktentwicklung
Öffentliche Verwaltung	• Service Public	• Verwaltung (N)	• Service Public	• Service Public
Marktpartner: Lieferant	• Billing • Energielieferung • Produktentwicklung	• Verwaltung (N)	• -	• Billing • Energielieferung • Produktentwicklung • Prognose
Marktpartner: ÜNB	• -	• Verwaltung (N)	• -	• Bilanzierung
Marktpartner: BGV	• -	• Verwaltung (N)	• -	• Bilanzierung
Marktpartner: SDV	• -	• Verwaltung (N)	• -	• -
Marktpartner: HKN Ausstellerin	• Vergütung	• Verwaltung (N)	• -	• Vergütung HKN / KEV
Marktpartner: Benachbarter VNB	• -	• Verwaltung (N)	• -	• Analog VNB (Handling Übergabepunkte)

Tabelle 3: Nutzungsrecht für Daten (N) und Verwendungszweck Domäne «Marktpartner»

6. Daten-Compliance

Dieses Kapitel beschreibt die durch die Rollen zu berücksichtigenden Gegebenheiten und die zu treffenden Massnahmen, um die in Kapitel 2 definierten Rahmenbedingungen aus regulatorischer Sicht einzuhalten sowie die aufgeführten Branchenempfehlungen konform umzusetzen. Die Compliance wird aufgeteilt in die beiden Aspekte Datenschutz und Datensicherheit. Das vorliegende Dokument liefert eine Übersicht über die zu berücksichtigenden Aspekte. Die AG Data Policy wird im Rahmen ihrer weiteren Tätigkeiten diese Aspekte weiter detaillieren und auch allfällig geänderte Rahmenbedingungen in die Betrachtung einbeziehen.

6.1 Datenschutz

Der Datenschutz regelt den Schutz von personenbezogenen Daten und basiert auf den in Kapitel 2 aufgeführten rechtlichen Vorgaben. Für die hier betrachteten Datenobjekte betrifft dies somit insbesondere das schweizerische Datenschutzgesetz und die Verordnung zum schweizerischen Datenschutzgesetz, die Datenschutzgrundverordnung DSGVO der EU, ggf. das jeweilig anzuwendende kantonale Datenschutzgesetz sowie spezialrechtliche Anforderungen aus unterschiedlichen Gesetzen und Verordnungen. Betreffend Letzterem ist insbesondere auf die Stromversorgungsverordnung (StromVV) zu verweisen, welche in Art. 8 das Messwesen und Informationsprozesse regelt. Mit dem ersten Massnahmenpaket der Energiestrategie 2050, welches auf den 1. Januar 2018 in Kraft getreten ist, erfolgt ebenfalls eine Teilrevision der StromVV. Mit dieser Teilrevision wird der Umgang mit Messdaten und anderen für den sicheren Betrieb der Verteilnetze notwendigen Daten neu und umfassender geregelt.

Gemäss der neuen Verordnung zum schweizerischen Datenschutzgesetz, welche aktuell noch nicht in Kraft ist, geniessen juristische Personen keinen Datenschutz, dieser ist ausschliesslich für natürliche Personen vorgesehen. Dieser Aspekt wurde in diesem Dokument bereits berücksichtigt.

6.1.1 Personenbezogene Daten mit primärem Anwendungsgebiet

Gemäss Art. 8d StromVV dürfen Netzbetreiber die Daten aus dem Einsatz von Mess-, Steuer- und Regelsystemen ohne Einwilligung der betroffenen Person unter der Einhaltung von Regeln (z.B. Pseudonymisierung) für die Messung, Steuerung und Regelung, für den Einsatz von Tarifsystemen sowie für den sicheren und effizienten Netzbetrieb und die Netzplanung verwenden. Diese Verwendungszwecke werden hier zusammengefasst als «primäres Anwendungsgebiet». Diese Daten dürfen zu in der StromVV klar definierten Anwendungszwecken ebenfalls ohne Einwilligung der betroffenen Person weitergegeben werden. In diese Kategorie der Daten fallen folgende in dieser Data Policy verwendeten Datenobjekte:

- ***Meter-Daten***
- ***Anlage-Messdaten***
- ***Fahrplan- & Prognosedaten***
- ***Steuer- & Anreizsignale***

Nachstehende Tabelle listet die verschiedenen zu berücksichtigenden Themen auf, jeweils mit Angabe der heute absehbaren Implikationen.

Thema	Beschreibung		Implikationen
Need-to-know Prinzip	Grundsatz, nach welchem Daten und Informationen nur denjenigen Stellen und Personen zur Verfügung stehen, welche sie für ihre Aufgaben benötigen.	→	Umsetzung des «Need-to-know Prinzip entspricht einer good practice aus Sicht Data Policy und umfasst sowohl technische wie auch organisatorische Massnahmen.
Anonymisierung	Daten werden so verändert, dass kein individueller Bezug hergestellt werden kann.	→	In der Regel können Daten anonymisiert werden, indem die Daten von mindestens 10-12 homogenen Einheiten (Empfehlung gemäss good practice aus der Bankenwelt) zusammengefasst werden. Dadurch handelt es sich nicht mehr um personenbezogene Daten und das Nutzungsrecht liegt nicht mehr bei der Rolle «Prosumer». Somit kommt die Gesetzgebung in Bezug auf den Datenschutz nicht mehr zur Anwendung.
Pseudo-nymisierung	Die Datensätze bleiben vorhanden (z.B. ein Lastprofil bestehend aus 15-Minuten Zählwerten), der Identifikator für den individuellen Bezug wird aber durch ein Pseudonym ersetzt.	→	Auch nach einer Pseudonymisierung handelt es sich bei den Datensätzen weiterhin um personenbezogene Daten, da ein Schlüssel existiert, um die Beziehung zum Individuum wiederherzustellen. Auch nach erfolgter Pseudonymisierung unterstehen die Daten weiterhin dem Datenschutz und die entsprechenden Regularien kommen zur Anwendung. Gemäss Art. 8d StromVV gültig ab 01.01.2018 müssen die Daten in pseudonymisierter Form bearbeitet werden, solange sie nicht für Abrechnungen oder Vergütungen in nicht pseudonymisierter Form vorliegen müssen. Ebenfalls wird die Weitergabe der Daten in pseudonymisierter Form vorgeschrieben.
Weiterverwendung der Daten	Jegliche Art von weitergehender Verwendung von Daten, z.B. Profiling (Verwendung der Daten um mithilfe von Analysen und Auswertungen Profile über das Individuum zu erstellen, aktualisieren oder verwenden. Dies dient oft zur Produktgestaltung oder dem Marketing.) oder die Weiterreichung der Daten an Dritte.	→	Grundsätzlich muss unterschieden werden zwischen gebundenen Kunden (Kunden in der Grundversorgung) und Kunden mit privatrechtlichen Verträgen. Entscheidend hierbei ist die «Alternativlosigkeit» von gebundenen Kunden. **Gebundene Kunden:** Für jede Art von Weiterverwendung der Daten muss ein explizites Einverständnis vorliegen. Eine entsprechende Regelung in den AGB ist somit nicht ausreichend. **Kunden mit privatrechtlichen Verträgen:** Entsprechende Weiterverwendung der Daten muss vertraglich geregelt sein, ein explizites Einverständnis durch den Kunden muss fallweise geklärt werden. Eine entsprechende Regelung in den AGB ist rechtlich ausreichend. Art. 8d StromVV gültig ab 01.01.2018 beschreibt den primären Verwendungszweck, für welchen keine Einwilligung der betroffenen Personen vorliegen muss. Ebenfalls wird definiert, welchen Personen die Daten weitergegeben werden dürfen. Diese Weitergabe der Daten muss immer in pseudonymisierter Form erfolgen. Die Weitergabe der Informationen für die Entschlüsselung der Pseudonyme erfolgt immer separat und nur an die dazu berechtigten Personen. Ebenfalls kann eine Weitergabe von Daten bei richterlichem Beschluss erlaubt resp. erforderlich sein, oder auch bei konträren und höher zu gewichtenden rechtlichen Regelungen.
Externe Verarbeitung	Verarbeitung der Daten (zum primären Zweck) bei einer anderen legalen Entität (gilt auch für Konzerngesellschaften).	→	Bei einer Datenverarbeitung ausserhalb der eigenen Rechtseinheit (Dritte, auch innerhalb des Konzerns) sind die massgebenden rechtlichen Grundlagen zu berücksichtigen.
Datenhaltung im Ausland	Datenhaltung ausserhalb der Schweiz.	→	Analog zu der externen Verarbeitung muss die Datenhaltung im Ausland im Vertrag oder in den AGB mit dem Kunden erwähnt sein. Hierbei finden Territorien und Räume (bspw. virtueller Raum Internet, Cloud etc. Anwendung). Falls das entsprechende Land keine adäquate Datenschutzgesetzgebung kennt und das notwendige Niveau auch nicht in anderer Art garantiert werden kann, muss zusätzlich ein explizites Einverständnis des Kunden eingeholt werden.

Thema	Beschreibung		Implikationen
Aufbewahrung & Archivierung	Vorgaben für die Aufbewahrung und elektronische Archivierung der Daten. Beinhaltet insbesondere Vorgaben zur Revisionssicherheit und zur Dauer der Aufbewahrung.	→	Für die Aufbewahrung und Archivierung der Daten müssen die relevanten Vorschriften gemäss Geschäftsbücherverordnung und verschiedenen weiteren spezialrechtlichen Regelungen eingehalten werden. Darüber hinaus existiert die Aufbewahrungspflicht für Netzbetreiber von Metering-Daten gemäss StromVV über eine Zeitdauer von 5 Jahre (Art. 8 Abs. 4 StromVV). Gemäss Art. 8d Abs. 3 im StromVV gültig ab 01.01.2018 müssen alle übrigen personenbezogenen Daten nach zwölf Monaten gelöscht werden.
Auskunfts-begehren	Recht der Kunden zum Wissen, welche Daten über sie gesammelt werden. Dieses Recht kann mithilfe eines Auskunftsbegehrens ausgeübt werden.	→	Gemäss Revision des Bundesgesetzes über den Datenschutz muss eine Anlaufstelle bestehen, an welche sich die Kunden mit Auskunftsbegehren zu den sie betreffenden personenbezogenen Daten wenden können. Hierfür stellt der eidgenössische Datenschutzbeauftrage ein Standardformular zur Verfügung. Auskunftsbegehren müssen innerhalb von 30 Tagen schriftlich beantwortet werden. Weitergehend kann in gewissen Fällen ebenfalls die Möglichkeit bestehen, dass die Kunden die Löschung, Berichtigung oder Sperrung ihrer Daten einfordern.
Daten-Portabilität	Bereitstellung aller von den Kunden bereitgestellten Daten in strukturierter und maschinenlesbarer Form. Dies beinhaltet nicht allfällig abgeleitete Daten.	→	Daten-Portabilität ist eine Anforderung in der neuen Europäischen Gesetzgebung (DSGVO). Durch diese Gesetzgebung betroffene Rechtseinheiten müssen die Daten-Portabilität somit umsetzen. Die schweizerische Gesetzgebung sieht voraussichtlich keine Anforderungen im Bereich Daten-Portabilität vor.

Tabelle 4: Vorgaben für den Umgang mit personenbezogenen Daten im primären Anwendungsgebiet

6.1.2 Weitere personenbezogene Daten

Bei den folgenden Datenobjekten handelt es sich normalerweise ebenfalls um personenbezogene Daten:

- ***Kundendaten***
- ***Vertragsdaten***
- ***Elektromobilität-Daten***

Sie unterliegen ebenfalls der in Kapitel 2 aufgelisteten rechtlichen Rahmenbedingungen, spezialrechtliche Anforderungen aus der StromVV kommen allerdings nicht direkt zur Anwendung. Als wichtiger Grundsatz gilt es dennoch zu berücksichtigen, dass jegliche personenbezogenen Daten, welche eine Rolle im Rahmen ihrer Aufgaben im primären Anwendungsgebiet erhält, nicht ohne explizites Einverständnis der betroffenen Person weiterverwendet werden dürfen. Die nachstehende Tabelle listet weitere für diese Datenobjekte zu berücksichtigenden Anforderungen auf.

Datenobjekt	Beschreibung der Anforderungen und Implikationen
Kundendaten	Versand von produkte- und dienstleistungsnaher Werbung ist aus Sicht Datenschutz kein Problem. Darüberhinausgehende Werbung sollte vertraglich resp. in den AGB geregelt werden bei nicht gebunden Kunden resp. ist ein explizites Einverständnis notwendig bei gebundenen Kunden.
Vertragsdaten	Pflicht auf Richtigkeit, Vollständigkeit und Aktualität der Daten besteht. Dabei haben alle Vertragspartner eine Beistellpflicht.
Elektromobilität-Daten	Solange die Daten aus netzbetrieblicher Sicht notwendig sind und keine Rückschlüsse auf den einzelnen Nutzer erlauben, ist die Verwendung der Daten unbedenklich. Für darüberhinausgehende Verwendungs-zwecke gelten die datenschutzrechtlichen Regelungen und eine privatrechtliche Regelung mit dem Kunden muss bestehen.

Tabelle 5: Vorgaben für den Umgang mit weiteren personenbezogenen Daten

6.1.3 Daten ohne Personenbezug

Folgende in dieser Data Policy verwendeten Datenobjekte haben normalerweise keinen direkten Personenbezug:

- ***Asset- & GIS-Daten***
- ***Auftrags- und Ereignisdaten***
- ***SCADA Daten***

Der Schutzbedarf an diese Datenobjekte stammt deswegen normalerweise aus Aspekten der Datensicherheit. Dennoch ist es auch bei diesen Datenobjekten prinzipiell denkbar, dass sie einer natürlichen Person zugeordnet werden können. Sobald dies der Fall ist, müssen die Anforderungen und Implikationen wie in den beiden vorigen Kapiteln beschrieben berücksichtigt werden. Die nachstehende Tabelle listet zu berücksichtigende Anforderungen an diese Datenobjekte auf.

Datenobjekt	Beschreibung der Anforderungen und Implikationen
Asset- & GIS-Daten	Vorgaben gemäss Leitungsverordnung (LeV) müssen eingehalten werden (bspw. die Regelung, welche Informationen öffentlich einsehbar sein müssen). Unklar ist, inwieweit die Dokumentation von kritischen Infrastrukturen wie z.B. Kernkraftwerken, Militäranlagen, Spitälern etc. gesichert werden muss.
Auftrags- und Ereignisdaten	Solange nur juristische Personen betroffen sind und keine Rückschlüsse auf natürliche Personen möglich sind gibt es datenschutzrechtlich keine Vorgaben. Sind natürliche Personen betroffen, gilt die Datenschutz-Gesetzgebung und der Umgang mit den Daten muss gemäss den entsprechenden Vorgaben erfolgen.
SCADA-Daten	Solange nur juristische Personen betroffen sind und keine Rückschlüsse auf natürliche Personen möglich sind gibt es datenschutzrechtlich keine Vorgaben. Sind natürliche Personen betroffen, gilt die Datenschutz-Gesetzgebung und der Umgang mit den Daten muss gemäss den entsprechenden Vorgaben erfolgen.

Tabelle 6: Vorgaben für den Umgang mit nicht personenbezogenen Daten

6.2 Datensicherheit

Die Datensicherheit beschreibt die Anforderungen und die Massnahmen, welche berücksichtigt respektive getroffen werden müssen, um die erforderliche Sicherheit der jeweiligen Daten einhalten zu können. Zu diesem Zweck muss in einem ersten Schritt der Schutzbedarf, d.h. die jeweilige Kritikalität, der Datenobjekte eruiert werden. In einem zweiten Schritt werden daraus abgeleitet die zu treffenden Massnahmen definiert.

6.2.1 Heute verfügbare Best-Practices und Standards

In Bezug auf die Datensicherheit bestehen bereits heute umfangreiche Arbeiten, welche je nach Anwendungsgebiet zu berücksichtigen sind. Folgende Tabelle listet die heute verfügbaren Best-Practices und Standards auf, aufgeteilt nach dem Verwendungszweck der Datenobjekte. Dabei wird unterschieden zwischen Datenobjekten, welche sehr «nahe» zu der Rolle «Prosumer» verordnet werden («Prosumer-nahe» Datenobjekte), und Datenobjekten, welche für Messung und vor allem auch Steuerung von Netzanlagen verwendet werden (Netzbetriebliche Datenobjekte).

«Prosumer-nahe» Datenobjekte	Netzbetriebliche Datenobjekte
• Kundendaten • Vertragsdaten • Meter-Daten (inkl. Vis.-Daten) • Anlagenmessdaten • Steuer- & Anreizsignale • Elektromobilitäts-Daten • Fahrplan- & Prognosedaten	• Asset-Daten • SCADA-Daten • GIS-Daten • Ereignis-Daten • Auftragsdaten
Individuelle Best-Practices & Standards	
• ISO/IEC 60870: Standard für Fernwirkeinrich-tungen und –systeme	Insbesondere … • BDEW Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme • NERC Critical Infrastructure Protection (CIP) • CIGRÉ TB 419: Treatment of Information Security for Electric Power Utilities • UP KRITIS: Anforderungen Informationssicherheit in kritischen Infrastrukturen • NIST 800-53, Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations • BSI IT-Grundschutz-Katalog • ISO/IEC 62443: Industrial communication networks – Network and system security • IEC 62351: Power systems management and associated information ex-change – Data and communications security
Übergreifende Best Practices & Standards	
• ISO/IEC-27000-Reihe: Standards zur IT-Sicherheit (insb. auch ISO/IEC TR 27019: Informationssicherheits-management von Steuerungssystemen der Energieversorgung) • NIST Cyber Security Framework • BWL Massnahmen zur Stärkung der IKT-Resilienz • VSE empfohlene Minimalstandards (in Arbeit) • NISTIR 7628: Guidelines for Smart Grid Cyber Security	

Tabelle 7: Best-Practices und Standards Datensicherheit

Weitere Informationen zu Best-Practices und Standards finden sich im Dokument «Grundschutz für «Operational Technology» in der Stromversorgung» (siehe Kapitel 2.2 Mitgeltende Dokumente).

6.2.2 Schutzbedarf der Datenobjekte

Der Schutzbedarf von Datenobjekten, resp. deren Kritikalität, setzt sich aus verschiedenen Komponenten zusammen. So kann sowohl aus datenschutzrechtlicher Sicht (d.h. dem Schutz von personenbezogenen Daten) als auch aus Gründen der Versorgungssicherheit ein hoher Schutzbedarf bestehen. Firmen können aus Business Continuity Überlegungen weitere Daten als kritisch einstufen, bspw. für die Aufrechterhaltung des Handels. Solche firmeninternen Aspekte der Kritikalität werden in diesem Dokument nicht betrachtet. Der Schutzbedarf wird aus den folgenden drei Komponenten zusammengestellt und aufgrund der englischen Anfangsbuchstaben der Begriffe mit «CIA» bezeichnet:

- ***Vertraulichkeit*** (Englisch: **C**onfidentiality): Schutz vor Einsicht bzw. Zugriff durch Unbefugte

- ***Integrität*** (Englisch: **I**ntegrity): Schutz vor unerlaubter Manipulation

- ***Verfügbarkeit*** (Englisch: **A**vailability): Systeme, Dienste, Daten und Informationen sind in geforderter Masse zugänglich und nutzbar. Die Verfügbarkeit impliziert den Schutz gegen Zerstörung und Verlust.

Abbildung 8 und Abbildung 9 zeigen die Kritikalität der Datenobjekte. Ebenfalls dargestellt ist, welche Rolle die jeweiligen Datenobjekte verwendet. Mit dieser Beziehung lassen sich die integralen Anforderungen in Bezug auf die Vertraulichkeit, Integrität und Verfügbarkeit pro Rolle einfach ableiten. Es gilt zu beachten, dass die Kritikalität der Datenobjekte auch vom jeweiligen Anwendungsfall abhängt. So besteht beispielsweise eine andere Anforderung an die Verfügbarkeit der Meter-Daten, je nachdem ob sie ausschliesslich für die Abrechnung verwendet werden oder ob sie für Anwendungsfälle zu Sicherung der Netzstabilität verwendet werden. In den Abbildungen dargestellt sind jeweils die höchsten bestehenden Anforderungen an den Schutzbedarf.

In Bezug auf die Vertraulichkeit besteht für alle Rollen ein hoher Schutzbedarf. Dies beruht darauf, dass alle Rollen personenbezogene Daten benötigen für die Ausübung ihrer Aufgaben. Ebenfalls verwenden alle Rollen Daten, welche einen hohen Schutzbedarf in Bezug auf die Integrität aufweisen. Diese Einschätzung beruht teilweise auf Daten, welche für den Netzbetrieb verwendet werden (z.B. Steuer- & Anreizsignale oder SCADA Daten) oder Daten, welche zu Abrechnungszwecken verwendet werden (z.B. Kundendaten oder Meter-Daten). Nur bei der Verfügbarkeit besteht für einzelne Rollen kein hoher Schutzbedarf. Dies betrifft die Rollen Datenrouter, Marktpartner und «Non-Energy»-Dienstleister, da diese keine für den Netzbetrieb notwendigen Daten – welche einen hohen Schutzbedarf in Bezug auf die Verfügbarkeit implizieren – verwenden. Ein Sonderfall ist die Rolle des Cloud-Anbieters. Sein Schutzbedarf ist abhängig davon, welche Daten er verwendet und kann deswegen nicht einheitlich definiert werden.

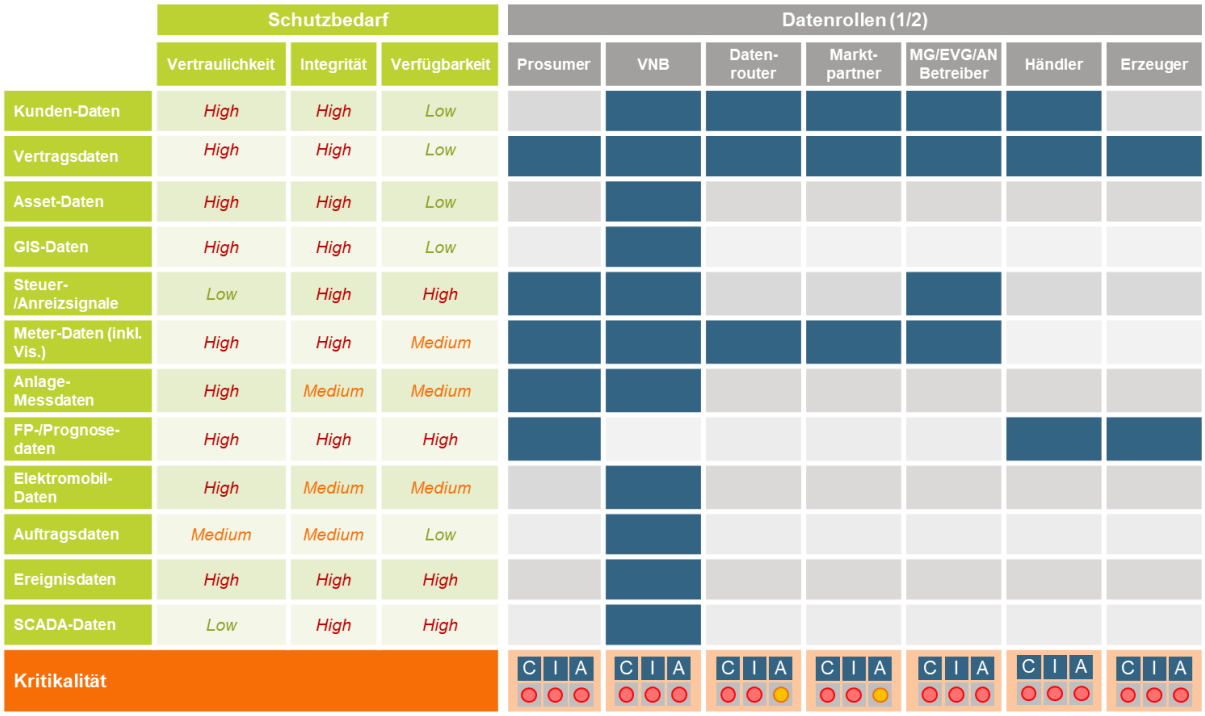

Abbildung 8: Schutzbedarf Datenobjekte und betroffene Datenrollen (1/2)

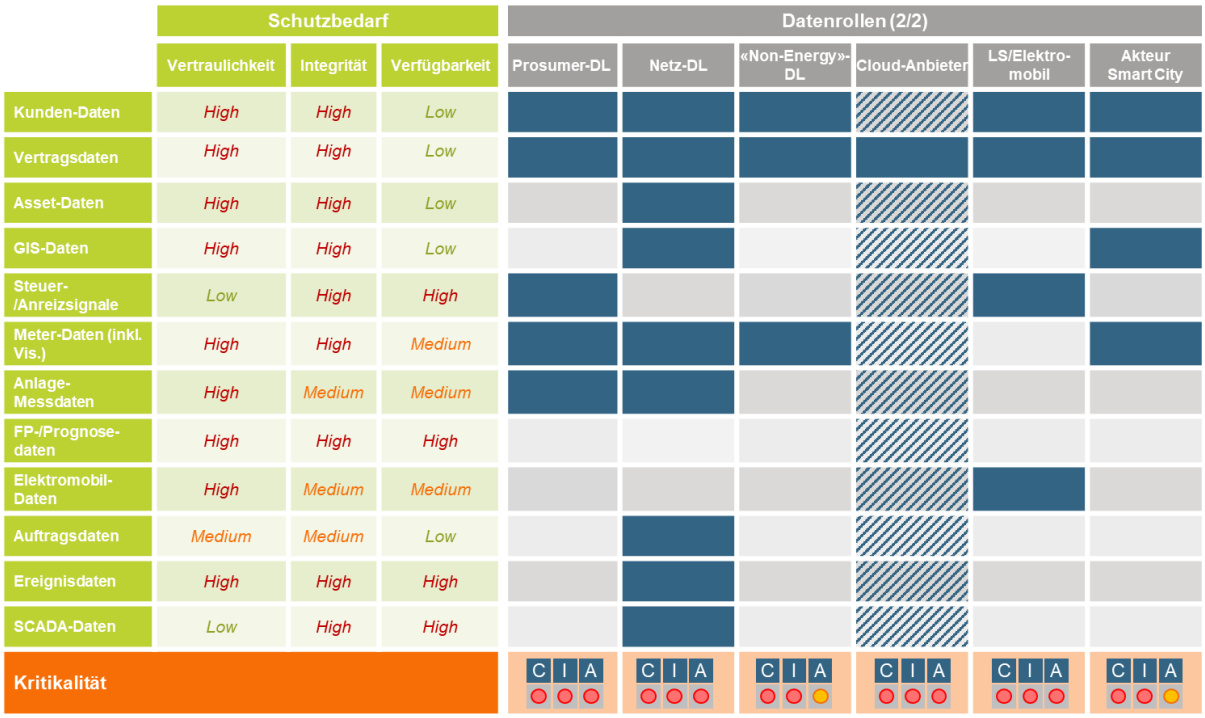

Abbildung 9: Schutzbedarf Datenobjekte und betroffene Datenrollen (2/2)

6.2.3 Anforderungen an die Erfüllung des erforderlichen Schutzbedarfs

Je nach Schutzbedarf in den drei Bereichen Vertraulichkeit, Integrität und Verfügbarkeit sind unterschiedliche Anforderungen umzusetzen. Die nachfolgende Tabelle zeigt die hierzu zu betrachtenden Kategorien an Anforderungen. Ebenfalls dargestellt ist die Art von Massnahmen, welche helfen, die Anforderung zu erfüllen. Dabei sind organisatorische (inklusive prozessuale) und technische Massnahmen möglich. In den bisherigen Arbeiten in der AG «Data Policy» wurden ausschliesslich Anforderungskategorien definiert. Die einzelnen umzusetzenden Anforderungen und Massnahmen sollen in einem nächsten Schritt in der Arbeitsgruppe detaillierter ausgearbeitet werden.

	Anforderungskategorien		Massnahmen
Vertraulichkeit (C) und Integrität (I)	Zugriffsschutz	Der logische Zugriff auf die Datenobjekte und/oder deren Veränderung soll nur autorisierten Personen ermöglicht werden (bspw. mittels geeigneter Authentifizierung).	org tech
	Geschützter Fernzugriff	Der Fernzugriff auf die Datenobjekte und/oder deren Änderung von Fern soll nur autorisierten Personen ermöglicht werden (z.B. mittels geeigneter Authentifizierung). Die Übertragung muss dabei den datenschutzrechtlichen Anforderungen entsprechen und gegebenenfalls verschlüsselt erfolgen.	tech
	Netzwerktrennung	Um die Vertraulichkeit und/oder Integrität der Datenobjekte zu schützen, kann gegebenenfalls ein getrenntes Netzwerk eingerichtet werden, je nach erfolgter Risikoabschätzung.	tech
	Sichere Datenübertragung	Vertraulichkeit und/oder Integrität bei der Übertragung der kritischen Datenobjekte über das gewählte Netzwerk muss gewährt sein. Allenfalls hat die Kommunikation verschlüsselt zu erfolgen (on-the-fly).	tech
	Sichere Datenablage	Vertraulichkeit und/oder Integrität der kritischen Datenobjekte bei deren Ablage muss gewährt sein. Allenfalls müssen die Datenträger oder Datenobjekte verschlüsselt werden (on-the-rest).	org tech
	Benutzer- und Berechtigungs-verwaltung	Die für den Zugriff und/oder für die Bearbeitung der Datenobjekte berechtigten Systeme, Gruppen und User sind zu definieren und deren Rechte zu regeln (z.B. mit einer Identity & Access Management (IAM) Lösung).	org tech
	Schutz gegen Angriffe von aussen	Die Informationssicherheit soll gewährleistet werden und die entsprechenden Systeme ausreichend vor Angriffen von aussen (Viren, Malware etc.) geschützt werden.	org tech
	Wartung der Komponenten	Für die Systeme und Komponenten sollen klare Vorgaben zur präventiven und korrektiven Wartung und Pflege bestehen.	org
	Klassifizierung der Datenbestände	Einteilung der Daten gemäss ihrer Kritikalität, beispielsweise öffentlich, intern, vertraulich, geheim.	tech
(C)	Entsorgung von Komponenten	Sicherstellen, dass auf kritische Datenobjekte auch nach Betriebsende der Komponenten (und deren physischen Entsorgung) nicht durch unbefugte Stellen zugegriffen werden kann.	org tech
(I)	Konfigurations-management	Bestimmung und Pflege der grundlegenden Konfigurationen (von Systemen, Benutzer- und Berechtigungsverwaltung und Datenobjekten).	org tech
	Schutz vor unbeabsichtigten Änderungen	Organisatorische und technische Massnahmen zur Verhinderung von unbeabsichtigten Manipulationen.	org tech
Verfügbarkeit (A)	Unterbrechungsfreier Betrieb	Bei einem Unterbruch sollen die kritischen Funktionen zur Erhaltung der Versorgungssicherheit aufrecht erhalten bleiben.	org tech
	Kommunikationssystem für Ereignisfälle	Es sollen Kommunikationssysteme in Betrieb, gewartet und getestet sein, welche im Ereignisfall den Wiederaufbau der Versorgungssicherheit unterstützen.	org tech
	Schutz gegen Angriffe von aussen	Die kritischen Kommunikationssysteme müssen gegen Angriffe von aussen auf die Verfügbarkeit oder Erreichbarkeit (z.B. Distributed Denial of Service) geschützt werden.	org tech

tech Anforderung führt zu technischen Massnahmen

org Anforderung führt zu organisatorischen und betrieblichen Massnahmen

Tabelle 8: Anforderungen an die Erfüllung des erforderlichen Schutzbedarfs

7. Daten-Governance

Das Ziel der Daten-Governance im Rahmen der Data Policy ist die Festlegung der Mechanismen zur Steuerung, Umsetzung sowie nachhaltigen Weiterentwicklung und Pflege der Data Policy Regelungen, sowohl unternehmensintern als auch branchenübergreifend. Inhaltlich werden hierfür die erforderlichen Governance-Aufgaben, -Rollen, -Gremien und -Prozesse sowohl innerhalb als auch zwischen den beteiligten Rollen identifiziert.

7.1 Ziele der Daten-Governance

Die folgenden Ziele sollen mit der Festlegung einheitlicher Grundsätze für die Daten-Governance im Rahmen der Data Policy erreicht werden:

- Sicherstellung der Umsetzung der Data Policy: Die hier definierten Aufgaben, Rollen und Prozesse sollen den betroffenen Unternehmen helfen, die Data Policy umsetzen zu können.

- Sicherstellung eines ausreichenden Datenschutzes: Für die personenbezogenen Daten sowie für die Sicherheit der kritischen Daten soll mit der Daten-Governance sichergestellt werden, dass unternehmensinterne Aufgaben und Rollen für die Wahrnehmung der erforderlichen Schutz- und Sicherheitsmassnahmen definiert sind.

- Sicherstellung einer adäquaten Datenqualität: Für die branchenweit ausgetauschten Daten soll mit der Daten-Governance sichergestellt werden, dass unternehmensinterne Aufgaben und Rollen für die Wahrnehmung der Datenqualität definiert sind.

- Sicherstellung des erforderlichen Daten-Reportings: Zusätzlich sollen Rollen und deren Aufgaben definiert werden, welche das adäquate branchenübergreifende Daten-Reporting sicherstellen helfen.

Die hier aufgeführten organisatorischen Strukturen und Massnahmen stellen dabei Überlegungen der AG für einen Minimalstandard an Grundsätzen dar, welche eine nachhaltige Umsetzung der Data Policy sicherstellen sollen.

7.2 Aufgaben der Daten-Governance

Die Aufgaben im Bereich Daten-Governance teilen sich auf branchenübergreifende sowie firmeninterne Aufgaben auf. Für die branchenübergreifenden Aufgaben soll eine fortlaufend aktive Arbeitsgruppe «Data Policy» besorgt sein, während die firmeninternen Aufgaben durch entsprechende interne Verantwortliche wahrgenommen werden.

Der VSE ist über die Arbeitsgruppe «Data Policy» für das «Data Policy Management» zuständig. Dies beinhaltet primär die fortlaufende Pflege und Aktualisierung der Data Policy. Neue Vorgaben, Entwicklungen, Trends und Rahmenbedingungen, sowohl politischer, regulatorischer, fachlicher oder technologischer Natur, sollen sukzessive auf deren Auswirkungen auf die Data Policy geprüft und im Bedarfsfall eingearbeitet werden. Die aktualisierten Data Policy Versionen werden dann in geeigneter Form branchenweit kommuniziert.

Neue Anforderungen der Stakeholder werden von der Arbeitsgruppe aufgenommen und in die Data Policy eingearbeitet.

Im Bereich Daten-Reporting ist davon auszugehen, dass zukünftig weitere regulatorische Anforderungen an die Energieunternehmen gestellt werden. Hier bietet sich an, dass im Rahmen der Aktivitäten der Arbeitsgruppe diesbezügliche standardisierte Frameworks als Hilfestellung für die Unternehmen zur Verfügung gestellt werden, zum Beispiel Reporting-Templates.

Die Unternehmen, bzw. die Markt-Teilnehmer, sind für die Umsetzung der Data Policy und deren Aktualisierungen zuständig, was insbesondere die folgenden Aufgaben beinhaltet:

- ***Strategisches Datenmanagement:*** Das strategische Datenmanagement beinhaltet die Definition und Umsetzung unternehmensübergreifender Vorgaben, Richtlinien und Policies sowie verbindlicher Zielsetzungen für den Datenschutz und die Datensicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) sowie für die operativen Aufgaben des Datenmanagements, insbesondere hier die Datenqualitätssicherung und das Daten-Reporting.

- ***Datenqualitätsmanagement:*** Im Rahmen des Datenqualitätsmanagements wird die Datenqualität der zumindest kritischen und branchenweit auszutauschenden Daten sichergestellt. Dazu werden geeignete Messgrössen und Instrumente verwendet.

- ***Dateninventarisierung:*** Zwecks Sicherstellung des erforderlichen Datenschutzes und der notwendigen Datensicherheit ist eine umfassende Dateninventarisierung unabdingbar. Entsprechend gilt es ein Dateninventar zu den obigen Datensätzen aufzubauen und fortlaufend zu pflegen.

- ***Daten-Reporting:*** Beim Daten-Reporting geht es um die Erstellung und den Versand der erforderlichen regulatorischen Datenreports sowie um die Datenauskunft gegenüber den betroffenen Bedarfsträgern. Die Unternehmen sind auch für die Datenauskunft und das Daten-Reporting mit adäquater Qualität gegenüber Daten-Nutzungsberechtigten, Behörden und Regulatoren verantwortlich. Diese Aufgabe enthält ebenfalls die allfällige Auskunftspflicht gegenüber den Behörden im Sinne der EU-Vertretung gemäss EU DSGVO.

Die folgende Abbildung fasst das Aufgabenspektrum der firmenübergreifenden und unternehmensinternen Daten-Governance sowie deren externen Schnittstellen zusammen.

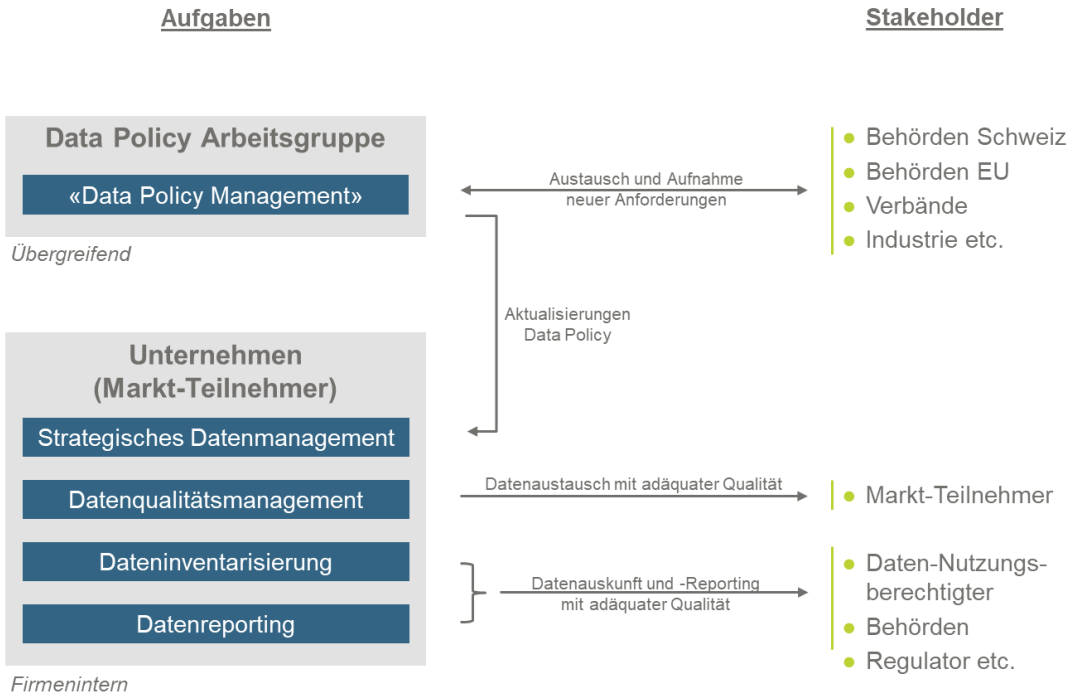

Abbildung 10: Aufgaben der Daten-Governance

7.3 Rollen und Gremien in der Daten-Governance

Zwecks Wahrnehmung der obigen Aufgaben werden im Folgenden die umzusetzenden organisatorischen Strukturen empfohlen. Sie stellen im Sinne eines «Minimalstandards» ein Set von Gremien und Rollen dar, welche ein nachhaltiges Datenmanagement ermöglichen sollen.

Gremium

Der VSE verantwortet über die Arbeitsgruppe «Data Policy» fortlaufend das «Data Policy Management». Mitglieder der Arbeitsgruppe sind der VSE sowie Vertreter aus Energieversorgungsunternehmen, Energie-Dienstleistern und Industrie.

Rollen, Gremien und Funktionen

Auf der Ebene der Unternehmen finden sich in der Praxis folgende zentrale Rollen zur Wahrnehmung der obigen Aufgaben. Im vorliegenden Dokument wird die Rollenbezeichnung des DPO verwendet, wobei in der Praxis auch andere Bezeichnungen zu finden sind.

Chief Information Security Officer (CISO)	Der Chief Information Security Officer (Leiter Informationssicherheit des Unternehmens) hat die Verantwortung für das Themenfeld **IT-Sicherheit** innerhalb des Unternehmens. Er definiert die Sicherheits-Regeln für die Geräte und Netze innerhalb der Firma und ist für die Definition der Datensicherheitsvorgaben im Unternehmen sowie für deren Umsetzung, Einhaltung und Überwachung zuständig.
Datenmanagement	Datenmanagement ist die Menge aller methodischen, konzeptionellen, organisatorischen und technischen Maßnahmen und Verfahren zur Behandlung der Ressource Daten mit dem Ziel, sie mit ihrem maximalen Nutzungspotenzial in die Geschäftsprozesse einzubringen und im laufenden Betrieb deren optimale Nutzung zu gewährleisten. Darüber hinaus muss ein professionelles Datenmanagement auch die Aspekte der Daten-/Informationsqualität und des Datenschutzes berücksichtigen. Über die gesamte Prozesskette hinweg soll für Datenkonsistenz gesorgt werden. Angefangen von der Geschäftserfassung, über die Bestandsführungs-systeme das Risikocontrolling, bis hin zur Bilanz ist eine komplexe Prozesskette zu berücksichtigen, die viele Bereiche eines Unternehmens betrifft. Die Datenqualität spielt dabei in jedem einzelnen Prozessschritt eine entscheidende Rolle.[4]
Data Protection Officer (DPO)	Der Rolleninhaber ist zuständig für Umsetzung, Einhaltung und Überwachung des Datenschutzes. ER kann als «Single Point of Contact» für alle Themen und Anliegen agieren, welche den Schutz personenbezogener Daten betreffen. Mögliche Aufgaben, Kompetenzen und Verantwortungen sind: – Bearbeitung von Anfragen von Behörden, Kunden oder Lieferanten – Auskünfte gegenüber Medien und anderen Stakeholdern – Aufbau und Verwaltung des Datenschutzprogramms (Privacy Program) – Definition von Prozessen für den Schutz von personenbezogenen Daten – Behandlung von Vorfällen (Data Breaches, Data Leaks, Security Incidents) – Interne Beratung für Projekte, Mitarbeitende, Management und Verwaltungsrat – Heute sind in ähnlichen Aufgaben auch Datenschutzbeauftragte tätig.[5]

[4] Quelle Wikipedia https://de.wikipedia.org/wiki/Datenmanagement

[5] In der bisherigen Schweizerischen Datenschutzgesetzgebung wurde diese Rolle mit «Datenschutzbeauftragter» bezeichnet. Der Entwurf für das revidierte Gesetz definiert die Rolle «Datenschutzberater», die daraus ableitbaren Rechte und Pflichten sind aktuell noch nicht klar bestimmbar. Gemäss DSGVO Art. 37 – 39 ist die Rolle des Datenschutzbeauftragten mit gesetzlich verankerten Rechten und Pflichten verbunden. Der Bestellung und Benennung dieser Rolle(n) ist deswegen ein hohes Gewicht beizumessen.

Weitere Rollen	Je nach Unternehmensgrösse kann es weitere Datenrollen geben, welche die Datenmanagementaufgaben in dedizierten Teilrollen übernehmen. Beispiele sind die Rollen eines Datenarchitekten für die logische und technische Umsetzung der Datenarchitekturen, oder eines Datenqualitätsmanagers für die Umsetzung des Datenqualitätsmanagements. Diese Rollen sind jeweils unternehmensspezifisch und hängen stark von der Grösse und strategischen Ausrichtung des Unternehmens ab.
Weitere Funktionen	Abhängig von der Unternehmensorganisation und der Unternehmensgrösse können bestimmte Funktionen optional durch Dritte abgewickelt werden (Beispielsweise CERT, siehe Anhang).

8. Anhänge

8.1 Glossar

Aggregator

Ein Aggregator bündelt Endkunden, um deren Eigenschaften (Verbrauch, Erzeugung, Speicherung) und Bedürfnisse ökonomisch zu optimieren.

Arealnetz

Gemäss VSE (Branchenempfehlung Strommarkt Schweiz Arealnetze) liegt ein Arealnetz vor, wenn das Netz der Feinverteilung von elektrischer Energie dient, es im Eigentum von einem Besitzer oder denselben Miteigentümern ist und mindestens ein juristisch unabhängiger Dritter ohne direkten Netzanschluss zum VNB an das Netz angeschlossen ist.

Blockchain

Eine Blockchain ist eine kontinuierlich erweiterbare Liste von Datensätzen, genannt „Blöcke“, welche mittels kryptographischer Verfahren miteinander verkettet sind. Die Blockchain ist ein Konzept mit dem ein Buchführungssystem dezentral geführt werden kann und dennoch ein Konsens über den korrekten Zustand der Buchführung erzielt wird, auch wenn sehr viele Teilnehmer an der Buchführung beteiligt sind. Entscheidend ist, dass spätere Transaktionen auf früheren Transaktionen, über deren Gültigkeit Konsens besteht, aufbauen und es dadurch unmöglich ist, die Existenz oder den Inhalt der früheren Transaktionen zu manipulieren oder zu tilgen. Der dezentrale Konsensmechanismus ersetzt die Notwendigkeit einer vertrauenswürdigen dritten Instanz (z.B. einer Bank) zur Integritätsbestätigung von Transaktionen. Blockchain ist die Basis vieler Kryptowährungen. Die älteste und bekannteste in Betrieb befindliche Blockchain ist die Kryptowährung Bitcoin.

Computer Emergency Response Team (CERT)

Das Konzept des CERT wurde in den späten 80er Jahren an der amerikanischen Carnegie Mellon University (CMU) entwickelt, um Computersysteme proaktiv gegen „Computerwürmer“ und andere Bedrohungen zu schützen. Zu den Hauptaufgaben eines Computer Emergency Response Teams gehört es, Bedrohungen frühzeitig zu erkennen und Gegenmassnahmen einzuleiten, bevor Probleme entstehen, den CERT Kunden bzw. Mitgliedern bei der Bewältigung von Sicherheitsvorfällen zu helfen, deren Auswirkungen zu reduzieren und zukünftige Ereignisse zu verhindern.

Heute verfügen die meisten Industrieländer über CERTs, die auf internationaler Ebene eng kooperieren und sich beim Auftreten von Security Incidents gegenseitig unterstützen. Die Professionalisierung der Internetkriminalität und die Entwicklungen im militärischen Bereich führen heute in Kombination mit der fortschreitenden Digitalisierung zu einer hohen Dynamik der Bedrohungslage.

Für Unternehmen, die damit konfrontiert sind, leistet ein CERT durch die Bündelung von Kräften und das Teilen von Know-how einen wichtigen Betrag zur Erhöhung der Informationssicherheit und der Widerstandsfähigkeit gegen Angriffe auf die ICT-Infrastruktur. In der Schweiz betreibt der Bund mit MELANI ein nationales CERT für die Bundesverwaltung und eine Melde-und Analysestelle für die kritischen Infrastrukturen. Zusätzlich haben sich Universitäten, Teile des Finanzsektors (Banken) und Industrie/Logistik in branchenspezifischen CERTs zusammengeschlossen. Letztere werden von SWITCH-CERT, das von CMU als nationales CERT eingestuft ist, in enger Zusammenarbeit mit MELANI betrieben.

Eigenverbrauchsgemeinschaft (EVG)

Eine EVG dient der Abwicklung der Eigenverbrauchsregelung zwischen Produzenten, Endverbrauchern und Energieversorgungsunternehmen. Sie besteht aus mehreren (mindestens zwei) Prosumern und

Endverbrauchern, die sich hinter dem selben Netzanschlusspunkt befinden und untereinander selber erzeugte elektrische Energie austauschen.

Intelligentes Messgerät (iMG)

Ein intelligentes Messgerät ist im engeren Sinne ein Stromzähler, der digital Daten empfängt und sendet.

Intelligentes Messsystem (iMS)

Ein intelligentes Messsystem ist im engeren Sinne ein Stromzähler, der digital Daten empfängt und sendet. Dazu ist er in ein Kommunikationsnetz eingebunden. Modellabhängig können intelligente Messsysteme auch Daten im schnellen Rhythmus an das Energieversorgungsunternehmen übertragen um bessere Netz- und Ressourcensteuerung zu ermöglichen. Intelligente Messsysteme sind zusammen mit automatischem Last- und Ressourcenmanagement Bestandteil von intelligenten Stromnetzen («Smart Grids»). Neben Stromzählern werden im weiteren Sinne auch zur Fernübertragung ausgerüstete Zähler für den Gas-, Wasser- und Fernwärmeverbrauch als intelligente Messsysteme bezeichnet. Solche Messgeräte werden auch Smart-Meter genannt. (Quelle: https://de.wikipedia.org/wiki/Intelligenter_Z%C3%A4hler)

Internet of Things (IoT)

Das IoT (Deutsch: Internet der Dinge oder «Allesnetz») bezeichnet die Vision einer durch Informations- und Kommunikationstechniken in globalen Informationsgesellschaften vernetzten Infrastruktur von Alltagsgegenständen. Im Internet der Dinge registrieren Sensoren an den vernetzten Gebrauchsgegenständen vorhandene Datenmengen und übertragen diese zur Erfüllung koordinierender Aufgaben an eingebettete Computer. So werden beispielsweise Kleidungsstücke mit miniaturisierten Computern, sogenannten Wearables, besetzt, die deren Lagepositionen ermitteln. (Quelle: https://de.wikipedia.org/wiki/Internet_der_Dinge)

Meter-Daten

Meter-Daten sind die von intelligenten Messsystemen generierten Daten mit dem Verbrauch oder der Erzeugung des jeweiligen Anschlusses.

Microgrid

Ein Microgrid ist ein Elektrizitätsverteilungssystem mit Lasten und verteilter Erzeugung. Es kann kontrolliert und gesteuert werden mit oder ohne Verbindung zu einem vorgelagerten Verteilnetz. Ein Inselbetrieb ist somit möglich.

Rollen

Für die verschiedenen Trends und das Gesamtdatenmodell wurden folgende Rollen definiert:

Rolle	Beschreibung	Aufgaben
Prosumer	Die Rolle Prosumer, zusammengesetzt aus Energie-Endverbraucher (Englisch: Consumer) und Energie-Produzent (Englisch: Producer), beinhaltet in diesem Dokument sowohl reine Endverbraucher als auch Verbraucher mit zusätzlicher Produktions- resp. Speicherkapazitäten.	- Einspeisung - Eigenverbrauch
VNB	Die Rolle Verteilnetzbetreiber umfasst alle Marktakteure, welche ein Elektrizitätsnetz in der Schweiz betreiben. In der Regel sind dies die Elektrizitätsversorgungsunternehmen (EVU), welche einen sicheren und zuverlässigen Betrieb ihres	- Netznutzung - Netzführung - Netzbetrieb - Datenrouting

Rolle	Beschreibung	Aufgaben
	Verteilnetzes gewährleisten und damit die Stromversorgung an ihre Endkunden sicherstellen. In der Schweiz existieren zurzeit zirka 800 Verteilnetzbetreiber. (Quelle: www.swissgrid.ch)	
Datenrouter	Ein Datenrouter hat die Aufgabe, den einheitlichen Messdatenaustausch zwischen den Marktpartnern bereitzustellen. Dabei müssen die Aspekte der Datenqualität, der Datenkonsistenz und des Datenschutzes berücksichtigt werden.	- Datenrouting
Marktpartner	Hier sind die Markpartner-Rollen für den Datenaustausch gemäss dem SDAT-Dokument des VSE gemeint. Zu den Marktpartnern gehören die Lieferanten, Erzeuger, VNB, ÜNB, BGV und SDV und HKN-Ausstellerin.	- Billing - Prognose/BGM - Angebotsmanagement
MG/EVG/AN-Betreiber	Leitet und betreibt ein Microgrid, eine Eigenverbrauchergemeinschaft oder ein Arealnetz. Übernimmt die Funktion des VNB auf dieser Ebene. Er ist die Schnittstelle vom untergelagerten Netz nach aussen zum VNB.	- Microgridführung
Händler	Der Händler handelt im In- und Ausland mit Energie	- Energiehandel
Erzeuger	Der Erzeuger erzeugt Energie mit verschiedenen Technologien.	- Energieerzeugung
Prosumer-DL	Der Prosumer-Dienstleister bietet dem Prosumer direkte Energiedienst-leistungen an, oft in Bezug auf seine energiespeichernden Anlagen. Beispiele solcher Dienstleistungen betreffen virtuelle Kraftwerke, Home Energiemanagementsysteme oder Demand Side Response Leistungen.	- Prosumer DL
Netz-DL	Der Netz-Dienstleister bietet Dienstleistungen an, die vom VNB ausgelagert wurden. Diese könnten unter anderem Netzführung, Asset Management, Asset Service, Messstellenbetrieb oder Meter Data Management sein.	- Netzdienstleistungen
«Non-Energy»-DL	Der «Non-Energy»-Dienstleister bezieht in seine Wertschöpfungskette Meter-Daten mit ein, um sie für Zwecke zu nutzen, die nicht mit der Energiebranche in Verbindung stehen.	- «Non-Energy»-DL
Cloud-Anbieter	Ein Cloud-Anbieter ist ein Unternehmen (Dritter), das Software-as-a-Service, Platform-as-a-Service und Infrastructure-as-a-Service anbietet - national oder international. Er stellt seine Infrastruktur und Systeme für das Speichern und Sichern von Daten seinen Kunden zur Verfügung. Der	- Hosting

Rolle	Beschreibung	Aufgaben
	Kunde kann standortunabhängig auf seine Daten zugreifen.	
LS/Elektromobil	Die Rolle Ladestation und Elektromobil sind als «Prosumer» im Bereich der Elektromobilität zu verstehen. Zusätzlich zum Austausch von Messdaten und Steuersignalen sind hier auch die Übermittlung mobiliätsbezogener Daten denkbar, z.B. der Ladezustand der Batterie, als Input zur Netzstabilitätsanalyse eines VNB.	- Elektromobilität
Akteur Smart City	Der Akteur Smart City kann eine Behörde oder eine andere Verwaltungseinheit sein, die ein intelligentes Energie-Management-System einer Stadt oder einer Gemeinschaft verwaltet.	- Smart City

Technologien

Nachfolgend wird eine Auswahl neuer, datengestützter Technologien beschrieben:

Technologie	Beschreibung
Digitalisierung	Die Digitalisierung wird immer stärker zur treibenden Kraft für Innovationen in Wirtschaft und Gesellschaft. Die Energiestrategien des Bundes, der Kantone und der Städte zeichnen einen Weg vor, auf dem dezentrale Erzeugung, erneuerbare Energie und Elektromobilität eine immer wichtigere Rolle spielen wird. Dieser als „3D“ – dekarbonisiert, dezentral, digital – bezeichnete Trend, führt zu einem Energiesystem, dessen Stabilität nur durch den vermehrten Einsatz von Informations- und Kommunikationstechnologie gewährleistet werden kann. Hauptkomponenten der Digitalisierung in der Energiewirtschaft werden daher digitale (Simulations-)Modelle von Versorgungssystemen, Prozessautomatisierung und neue digitale Kanäle zu Kunden und Partnerunternehmen sein, die entlang der Wertschöpfungskette positioniert sind.
Big-Data	Big Data ist ein Synonym für die Bedeutung grosser Datenvolumen in verschiedensten Anwendungsbereichen sowie der damit verbundenen Herausforderung, diese verarbeiten zu können. Big Data beschreibt Datenbestände, die aufgrund ihres Umfangs, Unterschiedlichkeit oder ihrer Schnelllebigkeit nur begrenzt durch aktuelle Datenbanken und Daten-Management-Tools verarbeitet werden können. Neben der Zunahme des Datenvolumens lässt sich die Bedeutung von Big Data auch damit erklären, dass der betriebswirtschaftliche Wert von Unternehmensdaten zunehmend erkannt wird. Informationen, die sich nur aus der Analyse von großen Mengen an Rohdaten erschliessen lassen, stellen oft einen Wettbewerbsvorteil dar.
Data-Mining	Data Mining steht dabei als Sammelbegriff für verschiedene rechnergestützte Verfahren, die zur Analyse großer Datenbestände eingesetzt werden. Data Mining zielt demnach darauf ab, Muster in einer Datenbasis zu finden, die mithilfe von logischen oder mathematischen Beschreibungen dargestellt werden können. Data Mining bietet im Gegensatz zu traditionellen statistischen Verfahren, die zur Überprüfung vorgegebener Hypothesen herangezogen

	werden, die Möglichkeit der automatischen Generierung neuer Hypothesen.
Predictive Analytics / Predictive Maintenance	Der neuere Begriff ‚Predictive Analytics' beschreibt im Wesentlichen die Anwendung von Data Mining mit besonderem Fokus auf die Generierung von Vorhersage-orientierten Modellen, wird jedoch in Teilen auch durch die stärkere Fokussierung auf statistische Methoden (im Gegensatz zur Orientierung an Datenbanken) begründet. Besonders interessant ist z.B. die Anwendung im Bereich der Wartung von Anlagen und bei der Planung von Ersatzinvestitionen.
Data Science / Data Scientist	Bei Data Science steht eine zweckorientierte Datenanalyse und die systematische Generierung von Entscheidungshilfen und -Grundlagen, um ökonomische Wettbewerbsvorteile erzielen zu können. Dabei ist es wichtig zu berücksichtigen, dass eine Datenanalyse nur erfolgreich sein kann, wenn sich diese auf eine konkrete Fragestellung bezieht. Ein Data Scientist benötigt (mindestens) Kenntnisse in zwei klassischen Fächern: Mathematik und Informatik. Dazu kommt idealerweise noch Wissen aus dem jeweiligen Anwendungsgebiet, denn Kernaufgabe eines Data Scientist ist es, aus diversen Datenquellen Antworten auf Fragen zu finden, die dem (internen oder externen) Kunden einen Mehrwert für einen konkreten Themenkomplex gibt.

Quellen:

https://www.strom.ch/de/energie/energiewelten/digitale-wirtschaft.html
https://www.seco.admin.ch/seco/de/home/wirtschaftslage---wirtschaftspolitik/wirschaftspolitik/digitalisierung.html
http://www.ey.com/Publication/vwLUAssets/ey-stadtwerkestudie-2017/$FILE/ey-stadtwerkestudie-2017.pdf
https://www.pwc.at/de/publikationen/pwc-studie-digitalisierung-energiewirtschaft-01-2016-screen.pdf
https://www.mckinsey.de/files/et_12.15_peters_mohr.pdf
http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/Informatik--Grundlagen/digitalisierung/index.html/?searchterm=digitalisierung
http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/daten-wissen/Datenmanagement/Datenmanagement--Konzepte-des/Big-Data/index.html?searchterm=big+data
http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/daten-wissen/Business-Intelligence/Analytische-Informationssysteme--Methoden-der-/Data-Mining/index.html?searchterm=predictive
http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/KI-und-Softcomputing/Kunstliche-Intelligenz/index.html?searchterm=KI
https://en.wikipedia.org/wiki/Data_science
http://www.datenbanken-verstehen.de/business-intelligence/data-science-grundlagen/data-science/

8.2 Abkürzungen

Abkürzung	Beschreibung
A	Availability
AG	Arbeitsgruppe
AGB	Allgemeine Geschäftsbedingungen
AN	Arealnetz
BDEW	Bundesverband der Energie- und Wasserwirtschaft (Deutschland)
BGV	Bilanzgruppenverantwortlicher
BWL	Bundesamt für wirtschaftliche Landesversorgung (Schweiz)
BSI	Bundesamt für Sicherheit in der Informationstechnik
C	Confidentiality
CIGRÉ	Conseil International des Grands Réseaux Électriques
CISO	Chief Information Security Officer
DL	Dienstleister
DSG	Bundesgesetz über den Datenschutz
DSGVO	Datenschutzgrundverordnung
E-DSG	Entwurf zum Datenschutzgesetz
EDM	Energiedaten-Management
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EEA	Energieerzeugungsanlage
EMS	Energie-Management-System
ETRM	Energy Trading, Transaction and Risk Management
EU	Europäische Union
EVG	Eigenverbrauchsgemeinschaft
EVU	Energieversorgungsunternehmen
GIS	Geoinformationssystem
HKN	Herkunftsnachweis
I	Integrity
IAM	Identity and Access Management
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnologie
iMG	intelligentes Messgerät
iMS	intelligentes Messsystem. Betrifft die ganze Messkette ab iMG bis Head End System, durch Datenkonzentrator oder Gateway.
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Informationstechnologie / Information Technology
LeV	Leitungsverordnung
LS	Ladestation
MG	Microgrid
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology (Vereinigte Staaten)
SCADA	Supervisory Control and Data Acquisition

Abkürzung	Beschreibung
SDAT	Standardisierter Datenaustausch - Umsetzungsdokument für Datenaustauschprozesse
SDV	Systemdienstleistungsverantwortlicher
StromVV	Stromversorgungsverordnung
ÜNB	Übertragungsnetzbetreiber
UP KRITIS	Umsetzungsplan zum Schutz Kritischer Infrastrukturen (Deutschland)
VNB	Verteilnetzbetreiber
VSE	Verband Schweizerischer Elektrizitätsunternehmen

8.3 Auswirkungen Revision Datenschutzgesetz

DATENSCHUTZ: DSGVO UND REVISIONSENTWURF DES DSG[6]

1. Ausgangslage[7]

Die rasante Entwicklung von Informations- und Telekommunikationstechnologien und die Digitalisierung der Gesellschaft, die sie bewirkt, haben eine komplette Überarbeitung der Datenschutzgesetzgebungen von Europarat und Europäischer Union erforderlich gemacht. Diese Überarbeitung hat wiederum dazu geführt, dass das seit 1993 geltende Bundesgesetz über den Datenschutz einer Totalrevision unterzogen werden musste. Der vom Bundesrat vorgestellte Gesetzesentwurf will den Datenschutz stärken, insbesondere durch eine Verbesserung der Transparenz von Datenbearbeitungen und der Kontrolle, die die betroffenen Personen über ihre Daten haben. Ziel des Entwurfs ist es, das Datenschutzniveau zwischen der Schweiz und der EU auf einem gleichwertigen Stand zu halten. Die Angleichung dieses Schutzniveaus ist vor allem für die Schweizer Wirtschaft von massgeblicher Bedeutung, zumal die neue Europäische Datenschutz-Grund-verordnung, die am 25. Mai 2018 in Kraft trat, für viele Schweizer Unternehmen direkte Auswirkungen haben wird.

**** Betrachtung EU ****

2. Europäische Datenschutz-Grundverordnung (DSGVO)

Das Europäische Parlament hat am 14. April 2016 die DSGVO verabschiedet, die am 25. Mai 2018 in Kraft trat. Diese Verordnung wirkt sich in zweierlei Hinsicht auf die Schweiz aus. Erstens hat sie eine grenzüberschreitende Reichweite. Sie gilt nämlich für alle Unternehmen ausserhalb der Europäischen Union, einschliesslich der Schweiz, die (i) personenbezogene Daten für europäische Unternehmen verarbeiten oder (ii) personenbezogene Daten von Einwohnern der Europäischen Union verarbeiten. Zweitens diente sie als Inspirationsquelle für den Revisionsentwurf des Bundesgesetzes über den Datenschutz (DSG).

Die wichtigsten Massnahmen der DSGVO sind die folgenden:

a. *Pflicht für die für die Datenverarbeitung verantwortliche Person und ihren Vertreter, ein **Verzeichnis von Verarbeitungstätigkeiten** zu führen (Art. 30 DSGVO) (gilt unter gewissen Bedingungen nicht für Unternehmen mit weniger als 250 Mitarbeitenden);*

b. *Die Datenverarbeitung bedingt die **Einwilligung der betroffenen Person.** Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (vgl. Erwägung Nr. 32 DSGVO).*

c. ***Erweiterte Rechte der betroffenen Person***
   - *Informationspflicht (Art. 13 und 14)*
   - *Auskunftsrecht (Art. 15)*
   - *Recht auf Berichtigung (Art. 16)*
   - *Recht auf Löschung («Recht auf Vergessenwerden») (Art. 17)*
   - *Recht auf Einschränkung der Verarbeitung (Art. 18)*

[6] In diesem Dokument werden zahlreiche Stellen der Botschaft des Bundesrates zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz zitiert.

[7] EDÖB – Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz

- *Recht auf Datenübertragbarkeit (Art. 20)*[8]
- *Widerspruchsrecht bezüglich bestimmter Verarbeitungen, z. B. um Direktwerbung zu betreiben oder zu Profilingzwecken (Art. 21)*
- *Recht, einer nicht ausschliesslich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden (Art. 22)*

d. ***Übermittlung von Daten ausserhalb der EU*** *(Art. 44): Falls das Land, an das die Daten übermittelt werden, kein angemessenes Datenschutzniveau bietet, braucht es die ausdrückliche Einwilligung der betroffenen Person, es sind aber auch zusätzliche Massnahmen zu treffen (Art. 46).*

e. *Über eine Verletzung des Schutzes personenbezogener Daten hat* ***der Verantwortliche die Aufsichtsbehörde*** *unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, zu unterrichten (Art. 33). Die Verletzung ist der betroffenen Person umgehend mitzuteilen (Art. 34).*

f. *Benennung eines* ***Vertreters in der EU*** *unter bestimmten Voraussetzungen (Art. 27), sofern personenbezogene Daten von betroffenen Personen, die sich in der EU befinden, durch einen nicht in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeiter verarbeitet werden.*

g. ***Benennung eines Datenschutzbeauftragten*** *unter bestimmten Voraussetzungen (Art. 37).*

h. ***Datenschutz-Folgenabschätzung*** *unter bestimmten Voraussetzungen (Art. 35).*

i. ***Rechtsbehelfe, Haftung und Sanktionen*** *(Art. 77 ff.): Betroffene Personen können gegen Verantwortliche vorgehen, und zwar für jegliche Art von Schäden, die ihnen infolge einer unangemessenen Verarbeitung ihrer Daten entstanden sind. Die Aufsichtsbehörde kann Verwaltungsmassnahmen oder Geldbussen von bis zu EUR 20 000 000.– oder im Fall eines Unternehmens von bis zu 4 Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängen.*

**** Betrachtung Schweiz ****

3. Revisionsentwurf des DSG

Das heutige DSG ist seit 1993 in Kraft. Der Bundesrat hat eine Revision dieses Gesetzes initiiert, um die Rechte der Dateninhaber sowie die Handlungsmöglichkeiten zu verbessern. Das Bundesamt für Justiz (BJ) hat Ende 2016 einen letzten Vorentwurf des Gesetzes veröffentlicht. Das BJ hat die Stellungnahmen von 222 Personen zusammengetragen und sie teilweise in die Vorbereitung des Gesetzesentwurfs (E-DSG) einfliessen lassen, der vom Bundesrat am 15. September 2017 verabschiedet wurde. Die Artikel 63 ff. E-DSG sehen Übergangsbestimmungen für die Umsetzung des Gesetzes vor. Gemäss diesen Bestimmungen richtet sich insbesondere die Informationspflicht bei der Beschaffung von Personendaten während zwei Jahren nach Inkrafttreten des neuen Gesetzes nach dem bisherigen Recht.

[8] Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat unter bestimmten Voraussetzungen das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln.

3.1 Grundsätze und Neuerungen des E-DSG

3.1.1 Einwilligung (Art. 5 Abs. 6 E-DSG)

Die betroffene Person muss ihre Einwilligung nach angemessener Information, freiwillig und eindeutig erteilen.

Eine schriftliche Einwilligung ist nicht zwingend, kann sich aber verhaltensbedingt ergeben. Eine Person kann ihre Einwilligung auch durch entsprechendes Handeln kundtun. In zwei Fällen muss die Einwilligung ausdrücklich erfolgen (z. B. ein Kästchen in einem Formular ankreuzen): für die Bearbeitung von besonders schützenswerten Personendaten (Gesundheitsdaten, Daten zur politischen Meinung oder zur religiösen Gesinnung usw.) und für das Profiling. Profiling ist die Bewertung bestimmter Merkmale von Verhaltensweisen (z. B. führt eine Bank ein Profiling durch, um ein Risikoprofil zu erstellen).

3.1.2 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 6 E-DSG)

Artikel 6 Absatz 1 E-DSG verlangt vom Verantwortlichen, ab dem Zeitpunkt der Planung eine Datenbearbeitung so auszugestalten, dass durch die getroffenen Vorkehren die Datenschutzvorschriften umgesetzt werden. Damit wird neu die Pflicht zum «Datenschutz durch Technik» (Privacy by Design) eingeführt.

Gemäss Artikel 6 Absatz 3 E-DSG ist der Verantwortliche verpflichtet, mittels geeigneter Voreinstellungen dafür zu sorgen, dass grundsätzlich nur so wenige Personendaten bearbeitet werden, wie im Hinblick auf den Verwendungszweck möglich ist, soweit die betroffene Person nicht etwas Anderes bestimmt. Dies führt neu die Pflicht zur Verwendung datenschutzfreundlicher Voreinstellungen (Privacy by Default) ein.

3.1.3 Datenschutzberaterin oder -berater (Art. 9 E-DSG)

Gemäss Artikel 9 können private Verantwortliche eine Datenschutzberaterin oder einen Datenschutzberater ernennen.

Die Datenschutzberaterin oder der Datenschutzberater überwacht die Einhaltung der Datenschutzvorschriften innerhalb eines Unternehmens und berät den Verantwortlichen in Datenschutzbelangen. Der Verantwortliche trägt jedoch allein die Verantwortung dafür, dass die Personendaten datenschutzkonform bearbeitet werden.

Wurde ein Datenschutzberater oder eine Datenschutzberaterin benannt, kann der Verantwortliche unter bestimmten Voraussetzungen von der Durchführung einer Datenschutz-Folgenabschätzung befreit werden.

3.1.4 Verhaltenskodizes (Art. 10 E-DSG)

Der Bundesrat möchte die Erarbeitung von Verhaltenskodizes fördern. In solchen Kodizes können einzelne Begriffe wie das hohe Risiko (Art. 20 E-DSG) oder die Modalitäten von Pflichten wie der Informationspflicht (Art. 17–19 E-DSG) und der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 20 E-DSG) präzisiert werden. Ausserdem sollen präzisere Lösungen gefunden werden in Bereichen, die heute zahlreiche Fragen aufwerfen, beispielsweise bei der Videoüberwachung, dem Cloud-Computing oder sozialen Netzwerken.

Indem der Bundesrat den interessierten Kreisen ermöglicht, selbst aktiv zu werden und zur Regulierung der einzelnen Bereiche beizutragen, möchte er konzertierte und breit abgestützte Branchenlösungen fördern. Zur Förderung der Selbstregulierung schlägt er zudem vor, dass Verantwortliche, die Verhaltenskodizes einhalten, unter bestimmten Voraussetzungen auf die Durchführung einer Datenschutz-Folgenabschätzung verzichten können (Art. 20 Abs. 5 E-DSG).

Im privaten Sektor müssen die Verhaltenskodizes von Berufs- oder Wirtschaftsverbänden stammen, die nach ihren Statuten zur Wahrung der wirtschaftlichen Interessen ihrer Mitglieder befugt sind. Einzelne Verantwortliche oder Auftragsbearbeiter können dem EDÖB keine Verhaltenskodizes vorlegen, da die Verhaltenskodizes eine gewisse Vereinheitlichung innerhalb einer bestimmten Branche zum Ziel haben. Im öffentlichen Sektor können Verhaltenskodizes hingegen von einem einzelnen Bundesorgan stammen. Dies rechtfertigt sich insbesondere aufgrund der zahlreichen gesetzlichen Grundlagen und der Vielfalt der Aufgaben der verschiedenen Organe.

3.1.5 Verzeichnis der Bearbeitungstätigkeiten (Art. 11 E-DSG)

Die Pflicht zur Führung eines Verzeichnisses obliegt dem Verantwortlichen und dem Auftragsbearbeiter. Diese Pflicht ersetzt die heutige Pflicht, die Datensammlung beim Beauftragten anzumelden. Artikel 11 Absatz 2 E-DSG zählt die Mindestangaben auf, die das Verzeichnis enthalten muss. Dazu gehören die Identität (der Name) des Verantwortlichen, der Bearbeitungszweck sowie eine Beschreibung der Kategorien betroffener Personen (z. B. Konsumenten, Mitglieder des Verbands x, Arbeitnehmer) sowie der Kategorien bearbeiteter Personendaten. Aufgeführt werden müssen ebenfalls die Kategorien von Empfängern, denen gegebenenfalls die Personendaten bekannt gegeben werden. Das Verzeichnis muss auch die Aufbewahrungsdauer der Personendaten sowie eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit enthalten. Anhand dieses Dokuments lässt sich überprüfen, ob eine Datenverarbeitung gesetzeskonform ist.

3.1.6 Bekanntgabe von Personendaten ins Ausland (Art. 13 E-DSG)

Gemäss Artikel 13 Absatz 1 E-DSG dürfen Personendaten ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder ein internationales Organ ein angemessenes Schutzniveau gewährleistet. Gemäss dem heutigen Gesetz obliegt es dem Verantwortlichen, zu prüfen, ob die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet.

Liegt kein Entscheid des Bundesrates nach Absatz 1 vor, sieht Artikel 13 Absatz 2 E-DSG vor, dass Personendaten ins Ausland bekannt gegeben werden können, wenn ein geeigneter Datenschutz gewährleistet wird. Ein geeigneter Schutz kann (a) durch einen völkerrechtlichen Vertrag, (b) durch Datenschutzklauseln in einem Vertrag, (c) durch spezifische Garantien, (d) durch Standarddatenschutz-klauseln und (e) durch verbindliche unternehmensinterne Datenschutzvorschriften gewährleistet werden.

Ist keine der oben genannten Bedingungen erfüllt, können die Personendaten dem Drittland trotzdem bekannt gegeben werden, sofern die betroffene Person ausdrücklich darin einwilligt und sofern diese über die Risiken bei der Übermittlung informiert wurde. Die Übermittlung ist ebenfalls möglich unter anderen Annahmen als gemäss Artikel 14 E-DSG wie beim Abschluss eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person oder bei der Wahrung des überwiegenden öffentlichen Interesses.

3.1.7 Informationspflicht bei der Beschaffung von Personendaten (Art. 17–19 E-DSG)

Die der betroffenen Person oder indirekt einer Drittperson mitzuteilenden Informationen sind die Identität, die Kontaktdaten des Verantwortlichen, der Bearbeitungszweck und gegebenenfalls die Weitergabe an Dritte oder ins Ausland. Der Verantwortliche muss sicherstellen, dass die betroffene Person die Information tatsächlich in einfach zugänglicher Weise zur Kenntnis nehmen kann.

3.1.8 Datenschutz-Folgenabschätzung (Art. 20 E-DSG)

Artikel 20 E-DSG führt neu die Pflicht zum Erstellen einer Datenschutz-Folgenabschätzung ein.

Begriff und Funktion der Datenschutz-Folgenabschätzung ergeben sich aus Artikel 20 Absatz 3 E-DSG. Eine Datenschutz-Folgenabschätzung ist ein Instrument, um Risiken zu erkennen und zu bewerten, die für die betroffene Person durch den Einsatz bestimmter Datenbearbeitungen entstehen können. Auf der Basis dieser Abschätzung sollen gegebenenfalls angemessene Massnahmen definiert werden, um diese Risiken für die betroffene Person zu bewältigen. Eine solche Abschätzung ist daher auch für den Verantwortlichen vorteilhaft, weil sie ihm erlaubt, allfällige datenschutzrechtliche Probleme präventiv anzugehen und dadurch nicht zuletzt Kosten zu sparen.

3.1.9 Meldung von Verletzungen der Datensicherheit (Art. 22 E-DSG)

Verletzungen der Datensicherheit sind dem EDÖB und je nachdem der betroffenen Person zu melden. Der Begriff «Verletzung» ist sehr breit gefasst. Er umfasst jegliche Verletzung der Datensicherheit, die dazu führt, dass Personendaten verloren gehen, gelöscht oder vernichtet, verändert oder Unbefugten offengelegt oder zugänglich gemacht werden.

3.1.10 Rechte der betroffenen Person (Art. 23–25 und 28 E-DSG)

Die Rechte der betroffenen Person wurden gestärkt. Artikel 23 E-DSG behandelt das Auskunftsrecht: Jede Person kann vom Verantwortlichen kostenlos Auskunft darüber verlangen, ob Daten über sie bearbeitet werden.

Gemäss Artikel 28 E-DSG kann jede betroffene Person zudem die Berichtigung unrichtiger Personendaten, die Löschung und/oder die Vernichtung von Personendaten verlangen. Weiter kann die betroffene Person verlangen, dass die Datenbearbeitung untersagt wird.

Das E-DSG sieht im Gegensatz zum europäischen Recht kein Recht auf Datenportabilität vor. Die betroffene Person kann folglich nicht verlangen, dass ihr ein Datenträger mit ihren Daten ausgehändigt wird. Ausserdem sieht das E-DSG nicht wie das europäische Recht ein Recht auf Vergessenwerden vor.

3.1.11 Beauftragte oder Beauftragter (7. Kapitel E-DSG)

Die Befugnisse des Beauftragten werden gestärkt. Der EDÖB kann Untersuchungen eröffnen. Seine Untersuchungs- und Durchsetzungsbefugnisse werden erweitert. Bei Verletzungen kann der EDÖB gewisse Verwaltungsmassnahmen ergreifen mit dem Ziel eines Verbots, Personendaten bekannt zu geben oder zu verarbeiten, jedoch im Gegensatz zum europäischen Recht keine Verwaltungssanktionen aussprechen.

3.1.12 Strafbestimmungen (Art. 54 ff. E-DSG)

Das Strafregime wurde gegenüber dem geltenden Recht verschärft. Allerdings stellt nur eine absichtliche Verletzung eine Straftat dar. Die Bussenobergrenze beträgt 250 000 Franken, liegt also deutlich unter der vom europäischen Recht vorgesehenen Geldstrafe.