Branchenempfehlung

Data Policy in der Energiebranche

Rahmenwerk für den gesamtheitlichen Umgang mit Daten in der Energiebranche

DPE – CH 2022

Impressum und Kontakt

Herausgeber
Verband Schweizerischer Elektrizitätsunternehmen VSE
Hintere Bahnhofstrasse 10
CH-5000 Aarau
Telefon +41 62 825 25 25
Fax +41 62 825 25 26
info@strom.ch
www.strom.ch

Autoren der Erstausgabe

Vorname Name	Firma	Funktion
Daniel Füglistaller	Axpo	Mitglied der Arbeitsgruppe
Gunnar Greiter	Sysdex	Mitglied der Arbeitsgruppe
Patrick Hauser	AEW	Mitglied der Arbeitsgruppe
Stéphane Henry	Romande Energie	Leiter der Arbeitsgruppe
Christoph Jörg	BKW Energie AG	Mitglied der Arbeitsgruppe
Wolfgang Korosec	St.Galler Stadtwerke	Mitglied der Arbeitsgruppe
Claudio Maag	EKZ	Mitglied der Arbeitsgruppe
Georg Meier	Axpo	Mitglied der Arbeitsgruppe
Susanne Weidmann	VSE / AES	Fachsekretariat
Jörg Weyermann	esolva	Mitglied der Arbeitsgruppe

Autoren der Zweitausgabe

Daniel Füglistaller	Axpo	Mitglied der Task Force
Barbara Gassmann	SIG	Mitglied der Task Force
Gunnar Greiter	Sysdex	Mitglied der Task Force
Bjoern Gross	IWB	Mitglied der Task Force
Patrick Hauser	AEW	Mitglied der Task Force
Christoph Jörg	BKW Energie AG	Leiter der Task Force
Wolfgang Korosec	St.Galler Stadtwerke	Mitglied der Task Force
Claudio Maag	EKZ	Mitglied der Task Force
Adrian Mettler	Repower	Mitglied der Task Force
Markus Riner	VSE / AES	Fachsekretariat
Vincent Rits	Primeo Netz AG	Mitglied der Task Force
Peter Schneider	Energie 360	Mitglied der Task Force
Hansjürg Stiffler	Swissgrid	Mitglied der Task Force
Jörg Weyermann	esolva	Mitglied der Task Force

Verantwortung Arbeitsgruppe
Für die Pflege und die Weiterentwicklung des Dokuments zeichnet die VSE Task Force Data Policy & Analytics verantwortlich.

Chronologie

Juni 2018	Planung der Arbeiten für die Branchenempfehlung
Juli 2019	Genehmigung der Erstausgabe durch den VSE Vorstand
März 2022	Genehmigung der Zweitausgabe durch den VSE Vorstand

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

Der VSE verabschiedete das Dokument am 23.03.2022.

Druckschrift Nr. 2002/d, Ausgabe 2022

Sprachliche Gleichstellung der Geschlechter.
Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort

Beim vorliegenden Dokument handelt es sich um ein Branchendokument des VSE. Es ist Teil eines umfassenden Regelwerkes für die Elektrizitätsversorgung im Strommarkt. Branchendokumente beinhalten branchenweit anerkannte Richtlinien und Empfehlungen zur Nutzung der Strommärkte und der Organisation des Energiegeschäftes und erfüllen damit die Vorgabe des Stromversorgungsgesetzes (StromVG) sowie der Stromversorgungsverordnung (StromVV) an die Energieversorgungsunternehmen (EVU).

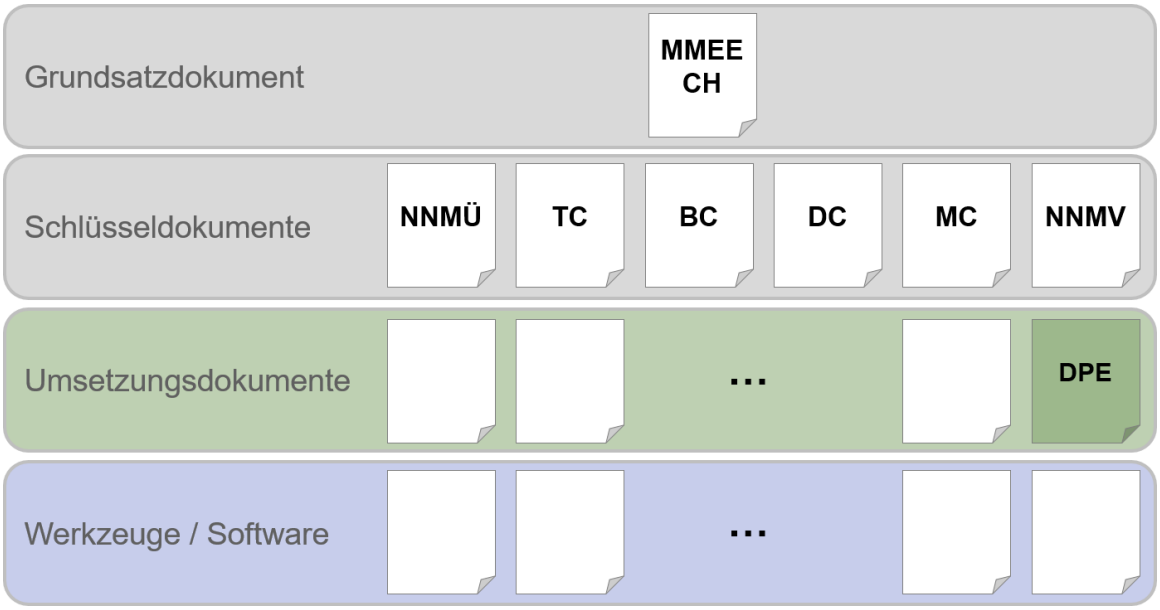
Branchendokumente werden von Branchenexperten im Sinne des Subsidiaritätsprinzips ausgearbeitet, regelmässig aktualisiert und erweitert. Bei den Bestimmungen, welche als Richtlinien im Sinne des StromVV gelten, handelt es sich um Selbstregulierungsnormen.

Die Dokumente sind hierarchisch in vier unterschiedliche Stufen gegliedert

Grundsatzdokument: Marktmodell für die elektrische Energie – Schweiz (MMEE – CH)
Schlüsseldokumente
Umsetzungsdokumente
Werkzeuge/Software

Beim vorliegenden Dokument Data Policy in der Energiebranche handelt es sich um ein **Umsetzungsdokument**.

Dokumentstruktur



1. Einleitung

1.1 Allgemeines

(1) Die durch Kundenbedürfnisse und neue technische Möglichkeiten angestossene Digitalisierung führt dazu, dass eine mehrwertgenerierende Bearbeitung und Nutzung geschäftsrelevanter Daten zunehmend an Bedeutung gewinnt. Technische Innovationen, umfangreiche Datenbestände sowie weitreichende Möglichkeiten der Analyse und Verknüpfung von Daten liefern Grundlagen für neue Geschäftsfeldentwicklungen. Diese Entwicklungen gelten auch für die Energiebranche.

(2) Dieses Dokument basiert auf dem Bundesgesetz über den Datenschutz (DSG), welches voraussichtlich per 1. Januar 2023 in Kraft treten wird. Stromversorgungsrechtlich wurden per 1. Januar 2018 die Rahmenbedingungen für ein EVU – primär in dessen Funktion als Netzbetreiber – zur Erhebung und Bearbeitung der Daten aus intelligenten Mess-, Steuer- und Regelsystemen festgelegt (insbesondere StromVG Art. 17c, StromVV Art. 8d).

(3) Zu berücksichtigen sind ebenso die Vorgaben zum **informatorischen Unbundling** gemäss StromVG Art. 10 Abs. 2

(4) Es gilt zu beachten, dass Verstösse gegen geltende regulatorische Anforderungen im Umgang mit Daten **auf allen Organisationsstufen** sowohl **persönliche** wie auch unternehmensspezifische Sanktionen zur Folge haben können.

(5) Wird im Rahmen dieses Dokuments der Begriff Netznutzer verwendet, sind damit Endverbraucher und/oder Erzeuger und/oder Speicherbetreiber gemeint.

1.2 Ziel des Dokuments

(1) Das vorliegende Dokument dient als Empfehlung für einen branchenweiten, geordneten und rechtskonformen Umgang mit Daten sowie als praxisnahe Data Policy für die Energiebranche. Diese umfasst Grundsätze für relevante Fragestellungen zu Daten-Nutzung, Data Compliance (d.h. Datenschutz, Datensicherheit) sowie Data Governance. Diese Grundsätze werden abgebildet in Form von Handlungsempfehlungen, Hilfsmitteln sowie organisatorischen Vorschlägen für datenrelevante Themen innerhalb eines mit der Energiebranche verbundenen Unternehmens.

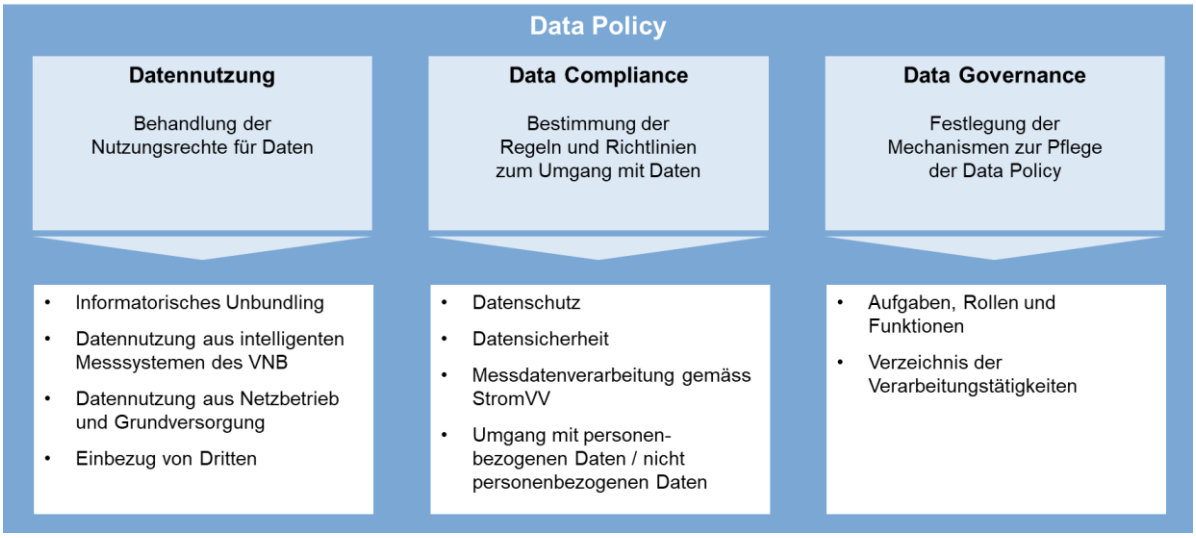


Abbildung 1 Schlüsselthemen der Data Policy

(2) Die vorliegende Data Policy dient als praxisbezogener Leitfaden bzw. Arbeitsmittel für mit der Energiebranche verbundene Unternehmen zum Zweck eines gesamtheitlichen Umgangs mit Daten. Das Dokument verfolgt den Ansatz der Best Practice. Dabei werden Risikoaspekte jedes einzelnen Datenbearbeitungsprozesses berücksichtigt (risikoorientierter Ansatz). Wo Inhalte nicht direkt anwendbar sind, liegt es in der Verantwortung der betroffenen Unternehmen, eine sinngemässe und konforme Lösung für den eigenen Zuständigkeitsbereich zu finden.

(3) Das vorliegende Dokument soll Bewusstsein schaffen für

- die zunehmende Komplexität und die Herausforderungen im Umgang mit Daten
- die Erarbeitung einer gesamtheitlichen, unternehmensweiten Data Policy
- Möglichkeiten im Umgang mit Daten im Rahmen der Digitalisierung und der digitalen Transformation

1.3 Einbettung der Data Policy in die VSE-Dokumentenlandschaft

(1) Die relevante Gesetzgebung wird sowohl in der Data Policy selbst wie auch in denjenigen Dokumenten, die über das Rahmenwerk referenziert sind, berücksichtigt.

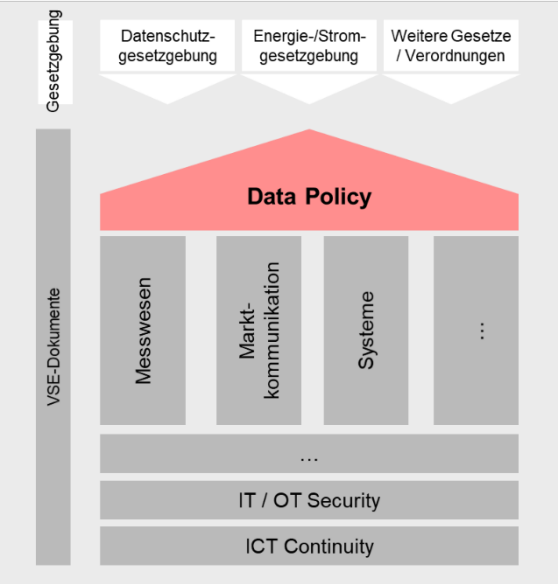


Abbildung 2 Die Data Policy als Rahmenwerk für themenverwandte VSE-Dokumente

(2) Folgende VSE-Dokumente können den einzelnen Themen in Abbildung 2 zugeordnet werden:

Thema	Dokument
Data Policy	– Bericht «Data Policy in der Energiebranche» – Branchenempfehlung «Data Policy in der Energiebranche»
Messwesen	– Schlüsseldokument «Metering Code Schweiz» – Richtlinien für die Datensicherheit von intelligenten Messsystemen – Handbuch «Messdatenmanagement» – Handbuch «Intelligente Messsysteme» – Themenpapier «Datenschutz und Datensicherheit bei Smart Metering» – Themenpapier «Verantwortlichkeit im Messwesen»
Marktkommuni-kation	– Branchenempfehlung «Standardisierter Datenaustausch für den Strommarkt Schweiz SDAT» – Branchenempfehlung «Bilanzgruppeninterner Datenaustausch»
Systeme	– Handbuch «Intelligente Steuer- und Regelsysteme für den Netzbetrieb»
IT / OT Security	– Handbuch «Grundschutz für «Operational Technology» in der Stromversorgung»
ICT Continuity	– Branchenempfehlung «ICT Continuity»
Abrechnung	– Branchenempfehlung «E-Invoice im Strommarkt Schweiz»

Tabelle 1 Übersicht der von der Data Policy betroffenen VSE-Dokumente

2. Geltungsbereich

(1) Die Data Policy konzentriert sich auf Daten mit eindeutigem Bezug zur Energiebranche. Dazu gehören auch Personendaten von natürlichen Personen (Ausnahme StromVG, Art. 17c). Nicht Bestandteil der Data Policy sind Daten für den Betrieb einer Organisation und ohne direkten Bezug zur Energiebranche. Für andere Daten mit vergleichbaren Datenschutz- und Datensicherheits-Anforderungen (Personal, Vertrieb, Marketing, Finanzen, usw.) gelten grundsätzlich dieselben Überlegungen, sie werden aber im vorliegenden Dokument nicht spezifisch behandelt.

(2) Basis für die konforme Umsetzung der regulatorischen Anforderungen ist die Erstellung und Implementierung einer unternehmensweiten Data Policy.

3. Definitionen

(1) **Data Policy**
Die Data Policy definiert Grundsätze und Richtlinien für die Themen **Daten-Nutzung**, **Data Compliance** (Datensicherheit, Datenschutz) und **Data Governance**. Die Definition dieser Themen findet sich zu Beginn des jeweiligen Umsetzungs-Kapitels.

(2) **Datenschutz**
Zweck und Ziel des Datenschutzes ist der Schutz der Persönlichkeit der Personen, über welche Daten bearbeitet werden sowie die Sicherung des Grundrechts auf informationelle Selbstbestimmung. Jeder soll selbst bestimmen können, wem er wann, warum und wie lange, welche seiner Daten zu welchem Zweck zugänglich macht.

(3) **Datenbearbeitung**
Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten (DSG, Art. 5, lit. d)

(4) **Datenbekanntgabe**
Das Übermitteln oder Zugänglichmachen von Personendaten (DSG, Art. 5 lit. e)

(5) **Datensicherheit**
Summe der technischen und organisatorischen Massnahmen (TOM) zur Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität von Daten.

(6) **Need-to-know Prinzip**
Grundsatz, nach welchem Daten und Informationen nur denjenigen Stellen, Personen, Funktionen und Rollen zur Verfügung stehen, welche sie für ihre Aufgaben benötigen. Die Umsetzung des «Need-to-know Prinzips» umfasst sowohl technische wie auch organisatorische Massnahmen (TOM).

(7) **Pseudonymisierung**

Mechanismus, wonach personenbezogene Daten einer bestimmten Person nicht mehr ohne Verwendung zusätzlicher Informationen zugeordnet werden können. Pseudonymisierte Daten sind nach wie vor Personendaten, für die das Datenschutzrecht anzuwenden ist.

Ein Pseudonym stellt den Bezug zwischen den unveränderten Daten und der Person her. Bspw. stellt das Pseudonym Messpunktbezeichnung den Bezug zum Kunden her. Folgt man der Branchenempfehlung «Metering Code Schweiz», keine sprechenden Schlüssel zu verwenden, kann die Pseudonymisierung über die Messpunktbezeichnung vorgenommen werden. Siehe auch Kapitel 6.2 Abs. (3).

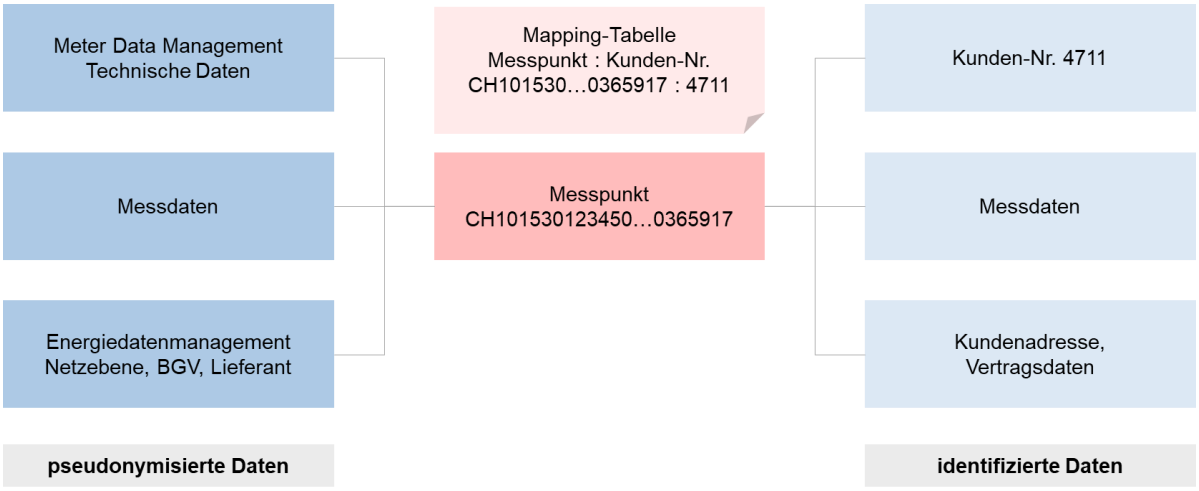


Abbildung 3 Beispiel für die Umsetzung der Pseudonymisierung mit Mapping-Tabelle

(8) **Anonymisierung**

Anonymisieren bedeutet, Personendaten so weit zu verändern, dass aus den resultierenden Daten nicht mehr oder nur noch mit unverhältnismässigem Aufwand auf die einzelne Person zurückgeschlossen werden kann. Die so erzeugten Daten sind keine Personendaten mehr und haben keinen entsprechenden Schutzbedarf, d.h. auf solche Daten ist das Datenschutzrecht nicht mehr anwendbar. Beispielhafte Auswahl von möglichen Anonymisierungsmethoden:

- Mehrere[1] homogene Datensätze können aggregiert verwendet werden, indem die Summe, ein arithmetisches Mittel oder ein Median für die weitere Bearbeitung eingesetzt wird
- Löschung aller personenidentifizierenden Informationen (z.B. Name und Vorname, Adresse, Telefonnummer, E-Mail, Anschlussobjekt, Zählernummer)
- Reduzierung der Menge an Datenattributen
- Optional muss für eine Anonymisierung eine Kombination der vorgängig genannten Methoden erfolgen

[1] Die genaue Anzahl ist situationsspezifisch festzulegen, sodass ein Rückschluss auf die betreffende Person nicht mehr möglich ist.
Als **Orientierungshilfe** gilt die Annahme, dass wenn 7 und mehr spezifische Werte / Attribute / Selektionskriterien mit Hilfe mathematschen Verfahren (arithmetisches Mittel oder Median) in die Bewertung aufgenommen werden, dass so ein genügender Grad der Anonymisierung erreicht werden kann. Es gilt im Einzelfall zu prüfen.

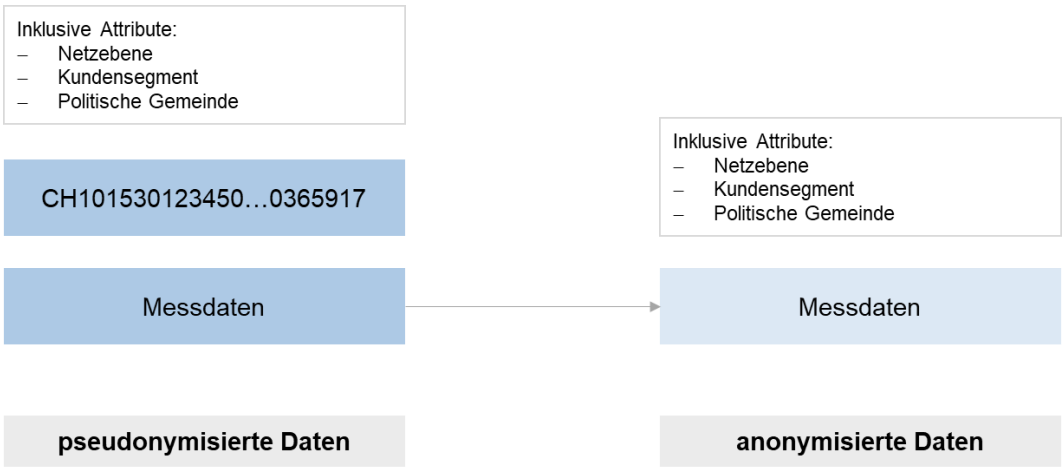


Abbildung 4 Beispiel für die Umsetzung der Anonymisierung

(9) **Personenbezogene Daten im EVU**
Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (DSG Art. 5 lit. a) und bspw. aus intelligenten Messsystemen, Anlage-Messdaten, Fahrplan- und Prognosedaten, Steuer- und Anreizsignale, Kundendaten, Vertragsdaten, Elektromobilitätsdaten stammen. Weiterführende Informationen finden sich im Anhang «Data Compliance - Datenmodelle und Anwendungen».

(10) **Sachdaten im EVU**
Sachdaten, im Sinne von nicht personenbezogenen Daten, sind bspw. Asset-Daten, Auftrags- und Ereignisdaten, SCADA-Daten. Für diese Gruppe von Daten gelten branchenspezifische Anforderungen betreffend Datensicherheit. Weiterführende Informationen finden sich im Anhang «Data Compliance - Datenmodelle und Anwendungen».

(11) **Security by Design**
Datensicherheit muss bereits frühzeitig während der Erarbeitung von technischen und organisatorischen Massnahmen im Rahmen der Umsetzung von Lösungen berücksichtigt werden (DSG Art. 8).

(12) **Privacy by Design / by Default**
Für den Schutz personenbezogener Daten gelten die Grundsätze sinngemäss wie unter «Security by Design» beschrieben. Privacy by Default stellt sicher, dass in der Grundeinstellung von Anwendungen und Systemen die Privacy sichergestellt ist (DSG Art. 7).

(13) **Profiling**
Jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen (DSG Art. 5 lit. f).

(14) **Profiling mit hohem Risiko**
Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt (DSG Art. 5 lit. g).

(15) **Technische und organisatorische Massnahmen (TOM)**
Die TOMs sind zentraler Teil der Dokumentation zum Datenschutz und sind wesentlich für das Verzeichnis der Bearbeitungstätigkeiten (VDB), die Auftragsbearbeitung und die entsprechenden Verträge, sowie für Informations- und Transparenzpflichten (Kapitel 11 Anhang Data Governance - Verzeichnis der Bearbeitungstätigkeiten und DSG Art. 7 Abs. 2).

(16) **Datenherausgabe und -übertragung (Portabilität)**
Herausgabe und -übertragung von Personendaten in einem gängigen elektronischen Format (DSG Art. 28 Abs. 1).

(17) **Datenschutz-Folgenabschätzung (DSFA)**
Eine DSFA ist vorgängig zu erstellen, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann (DSG Art. 22 Abs. 1). Von der Erstellung einer DSFA ausgenommen sind private Verantwortliche, wenn sie gesetzlich zur Bearbeitung der Daten verpflichtet sind (DSG Art. 22 Abs. 4 z.B. Bearbeitung von Daten aus intelligenten Messsystemen sowie Energiedaten in der Grundversorgung gemäss StromVV).

(18) **Verzeichnis der Bearbeitungstätigkeiten**
Prozess- und Ablauforientierte Zusammenstellung der Bearbeitungstätigkeiten (DSG Art. 12). Vergleiche hierzu auch Kapitel 8.3 «Verzeichnis der Bearbeitungstätigkeiten».

(19) **Verantwortlicher**
Private Person (im Sinne von natürlichen und juristischen Personen) oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel entscheidet (DSG Art. 5 lit. j).

(20) **Auftragsbearbeiter**
Private Person (im Sinne von natürlichen und juristischen Personen) oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet (DSG Art. 5 lit. k).

4. Übersicht zur Umsetzung der Data Policy

(1) Eine Umsetzung der regulatorischen und rechtlichen Anforderungen sowie der Data Policy durch ein EVU bedingt eine Reihe von Arbeitsschritten, um alle datenrelevanten Aspekte berücksichtigen zu können. Ein entsprechender unternehmensweiter Kulturwandel mit Massnahmen, welche alle Hierarchiestufen mit einbezieht und von Verwaltungsrat und Geschäftsleitung geführt wird, ist für eine effektive Umsetzung empfohlen.

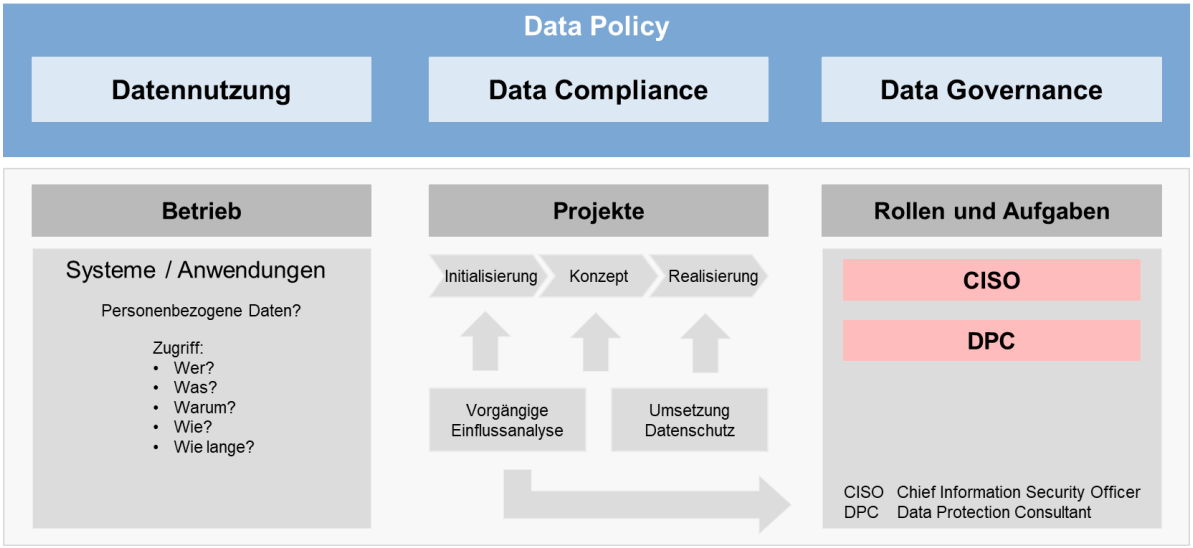


Abbildung 5 Themen bei der Umsetzung der Data Policy

(2) Dafür sind innerhalb eines Unternehmens klar definierte Rollen und Verantwortlichkeiten für einen gesamtheitlichen Umgang mit Daten zu klären. Kapitel 8 «Umsetzungsempfehlungen Data Governance» beschreibt wichtige Rollen und/oder Funktionen, die zugewiesen bzw. wahrgenommen werden müssen.

(3) Als ein zentrales Element für die Festlegung des korrekten Umgangs mit Daten wird empfohlen, ausgehend von den Prozessen, sowie einer Übersicht der Datenflüsse und einem Dateninventar ein «Verzeichnis der Bearbeitungstätigkeiten» (VDB) gemäss Kapitel 8.3 zu erstellen sowie ein Verzeichnis der ICT Infrastruktur.

(4) Bei der Durchführung von Projekten (Vorhaben, Veränderungen …), bspw. zum Design von Dienstleistungen und Geschäftsprozessen, muss die Handhabung von Daten frühzeitig festgelegt werden. Berücksichtigt werden müssen:

- Anforderungen an den Datenschutz (Bspw. Datenschutz-Folgenabschätzungen (DSFA), Privacy by Design / by Default)
- Anforderungen an die Datensicherheit (Bspw. Security by Design)
- Gewährleistung von Betroffenenrechten (z.B. Auskunft, Datenberichtigung, -sperrung, -löschung)
- Anforderungen an die Datennutzung bzgl. regulatorischer Rahmenbedingungen

Beim Projektabschluss muss die Umsetzung aller datenbezogenen Anforderungen gewährleistet sein. Kapitel 7 «Umsetzungsempfehlungen Data Compliance» beschreibt diesbezügliche Grundlagen.

(5) Bei der Festlegung der Handhabung von Daten muss der gesamte Lebenszyklus betrachtet werden, von der Beschaffung, Speicherung, Aufbewahrung, Verwendung, Veränderung, Bekanntgabe, Archivierung, Löschung oder Vernichtung der Daten.

(6) Jegliche Form von Daten ist grundsätzlich zu klassifizieren und entsprechend zu schützen und die rechtskonforme Datennutzung ist sicherzustellen. Die korrekte Datennutzung muss jederzeit sichergestellt werden. Dies unter Berücksichtigung der Vorgaben für den Umgang mit personenbezogenen Daten (Personendaten) bzw. mit Daten ohne Personenbezug (Sachdaten). Zudem gilt es, die Rechte von betroffenen Personen zu gewährleisten. Grundlagen zum Thema Datennutzung sind in Kapitel 6 «Umsetzungsempfehlungen Datennutzung» ausgeführt.

(7) Die Bearbeitung personenbezogener Daten muss jederzeit erklärbar sein und im Einklang mit den jeweils einschlägigen datenschutzrechtlichen Bestimmungen stehen. Die Regeln müssen den Mitarbeitenden bekannt sein.

(8) Ein Leitfaden zu den wichtigsten Umsetzungspunkten findet sich in Kapitel 13.

5. Rechtliche Grundlagen

(1) Auf allfällige weitergehende Regelungen in kantonalen Datenschutzgesetzen wird in diesem Dokument nicht eingegangen.

(2) Aus branchenspezifischer Sicht sind die Regulierungen zur Datennutzung des informatorischen Unbundling gemäss StromVG Art. 10 Abs. 2 für einen diskriminierungsfreien Netzzugang und zum Schutz des Wettbewerbs zentral. Für weitere Ausführungen siehe Kapitel 6.1 Entflechtung (Unbundling).

(3) Für die Messdatenbearbeitung im Zusammenhang mit intelligenten Mess-, Steuer- und Regelsystemen gelten die spezialrechtlichen Vorgaben gemäss StromVV Art. 8d. Diese Vorgaben gehen den eidgenössischen und kantonalen Regelungen betreffend Datenschutz vor. Für weitere Ausführungen siehe Kapitel 7.3 «Messdatenbearbeitung gemäss StromVV».

5.1 Übersicht Regularien, Gesetze und Normen sowie Abgrenzungen

(1) Im vorliegenden Dokument werden die strommarktrelevanten regulatorischen Rahmenbedingungen für die Energiebranche und artverwandte Branchen thematisiert. Es handelt sich hierbei um:

Regularium	Abkürzung
Energiegesetz	EnG
Energieverordnung	EnV
Bundesgesetz über die Stromversorgung	StromVG
Stromversorgungsverordnung	StromVV
Bundesgesetz über den Datenschutz vom 25. September 2020	DSG
Kantonale Datenschutzgesetze	-
Verordnung zum Bundesgesetz über den Datenschutz	VDSG
Datenschutz-Grundverordnung der Europäischen Union	DSGVO
Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (Geschäftsbücherverordnung)	GeBüV

Tabelle 2 Übersicht der Regularien

(2) Die Anwendbarkeit der DSGVO für Schweizer EVU kann in folgenden drei Situationen gegeben sein:

- Wenn das EVU eine Niederlassung in der EU hat
- wenn das EVU Waren oder Dienstleistungen in der EU anbietet
- wenn das EVU das Verhalten seiner Kundinnen und Kunden in der EU beobachtet, um ihnen personalisierte Angebote zu unterbreiten

Vergleiche auch 12. Anhang FAQ DSGVO.

(3) Das vorliegende Dokument fokussiert ausschliesslich auf den im Kapitel 2 beschriebenen Geltungsbereich.

5.2 Personendaten

(1) Die Gesetzgeber in der Schweiz und der EU haben eine beschreibende Definition vorgenommen, welche nicht abschliessend ist.

(2) Datenschutzgesetz Schweiz (DSG), Art. 5, lit. a:
Personendaten (Daten): alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

(3) Daraus lässt sich ableiten, dass es Daten gibt, welche eindeutig einer bestimmten Person zugewiesen werden können (bspw. Name, Vorname, Geburtsdatum, Adresse). Die Definition umfasst auch jegliche Form von Daten, aus welchen eine Person bestimmbar wird (bspw. durch Datenanalyse, Profiling). Diese Bestimmbarkeit kann aber auch aus beliebigen Daten erfolgen. Ergibt sich die Bestimmbarkeit einer natürlichen Person aus dem Kontext, so sind solche Daten ebenfalls dem Datenschutz unterstellt.

(4) Häufige Geschäftsanwendungen, bei welchen ein Personenbezug direkt (bestimmte Person) oder indirekt (bestimmbare Person) gegeben ist oder gegeben sein kann, sind insbesondere:

- Customer-Relationship-Management (CRM)
- Anlagen- und Gebäudedokumentation, z.B. mit personenbezogenen Informationen angereicherte GIS-Daten
- Messdatensysteme
- Dokumentenmanagement, z.B. Verträge, Dienstbarkeiten
- Enterprise-Resource-Planning (ERP)
- Energiebezogene Buchhaltungs- und Abrechnungssysteme mit Kunden-, Kreditoren- und Debitorendaten
- Lösungen, welche analytische Verfahren für Kategorisierungen, Segmentierungen, Gruppierungen, Clustering, Scoring usw. verwenden

5.3 Besonders schützenswerte Personendaten

(1) Weiter existieren besonders schützenswerte Personendaten. Diese dürfen grundsätzlich nur erhoben und gespeichert werden, wenn sie für die Geschäftstätigkeit eines EVU relevant sind. In der Regel fallen solche Daten nicht in den Kerntätigkeiten eines EVU an. Einzelfälle müssen separat beurteilt werden.

(2) Das Schweizer Datenschutzgesetz definiert in Art. 5, lit. c. entsprechende Daten. Besonders schützenswerte Personendaten sind zusätzlichen Restriktionen unterworfen.

(3) Es können die nachfolgenden, besonders schützenswerten Kategorien abgeleitet werden:

Kategorie
Religiöse, weltanschauliche, politische, gewerkschaftliche Ansichten und Tätigkeiten
Daten über Gesundheit, Intimsphäre, Rasse, Ethnie
Massnahmen der sozialen Hilfe
Verwaltungs- und strafrechtliche Verfolgung und Sanktionen
Genetische Daten
Biometrische Daten, die eine natürliche Person eindeutig identifizieren

Tabelle 3 Kategorien von besonders schützenswerten Personendaten

5.4 Profiling & Profiling mit hohem Risiko

(1) Beim Einsatz von Profiling (für Definition siehe Kapitel 3 «Definitionen» Abs. (13) & (14)) sind dem Schutzbedarf angemessene technische und organisatorische Massnahmen zu treffen. Für die Abklärung des Schutzbedarfes ist bei einem Profiling mit hohem Risiko eine Datenschutz-Folgenabschätzung durchzuführen und im öffentlich-rechtlichen Bereich zusätzlich ein Bearbeitungsreglement zu erstellen.

(2) Im Kontext dieser Data Policy ist die Thematik unter anderem im Bereich Smart Metering (beispielsweise gemäss StromVG Art. 17c in Verbindung mit StromVV Art. 8d «Umgang mit Daten aus intelligenten Messsystemen») von Relevanz.

5.5 Datenbearbeitung

(1) Die Begriffe Datenbearbeitung und Datenverarbeitung stammen aus den Datenschutzgesetzgebungen der Schweiz und der EU und stimmen in ihrer Bedeutung grundsätzlich überein.

(2) Der Begriff Datenbearbeitung umfasst alle Tätigkeiten und Aktivitäten im Zusammenhang mit Daten und Informationen, unabhängig davon

a. welche Medien (bspw. IT, Papier) verwendet werden
b. ob sie aktiv (bspw. erfassen) oder passiv (Einsicht gewähren) ausgeführt werden
c. in welcher Phase des Lebenszyklus (Phase 1: Generierung/Beschaffung/Erstellung, Phase 2: Verwendung/Bearbeitung, Phase 3: Aufbewahrung/Archivierung/Löschung) sie sich befinden. Siehe dazu auch Kapitel 3 Abs. (3)

(3) In welcher Form bzw. unter welchen Bedingungen diese Tätigkeiten und Aktivitäten ausgeübt werden, ist unerheblich: bspw. durch Personen, Computer, durch die eigene Rechtseinheit oder Dritte, in der Schweiz oder im Ausland.

(4) Wichtig für die korrekte Datenbearbeitung ist eine zentrale Quelle, welche sämtliche Datenbearbeitungstätigkeiten prozess-/ablauforientiert dokumentiert (DSG Art. 12, Verzeichnis der Bearbeitungstätigkeiten).

(5) Daten sind darüber hinaus weiteren regulatorischen Restriktionen unterworfen, wie bspw. wettbewerbs- oder kartellrechtliche Vorgaben (z.B. Unbundling gemäss StromVG und StromVV), Bestimmungen über Amts- und/oder Geschäftsgeheimnis. Hierbei können dieselben Daten betroffen sein, welche auch für den Datenschutz relevant sind.

5.6 Auftragsdatenbearbeitung

(1) Wenn personenbezogene Daten durch Dritte (ungleich eigene Rechtseinheit) bearbeitet werden, bedarf es grundsätzlich einer vertraglichen Regelung im Sinne der Auftragsbearbeitung gemäss DSG Art. 9. Abs. 1 (Ausnahmen müssen im Einzelfall geprüft werden, beispielsweise wenn eine gesetzliche Grundlage zur Datenweitergabe besteht). Der Verantwortliche bestimmt dabei Zweck und Mittel der Verarbeitung und definiert die erforderlichen technischen und organisatorischen Massnahmen (TOM). Diese Vorgaben gelten auch für Untervertragsnehmer, Unterauftragsbearbeiter sowie deren Zulieferer und Vertragspartner. Die Verantwortung verbleibt grundsätzlich jedoch immer beim Auftraggeber (Verantwortlicher gemäss DSG) und somit obliegen diesem auch entsprechende Kontrollpflichten (vgl. DSG Art. 9 Abs. 2).[2]

(2) Wo mehrere Rechtseinheiten eine wirtschaftliche Einheit bilden, bspw. Konzerne oder öffentlich-rechtliche Konstrukte, bedarf es einer detaillierten Analyse und Regelung. Im Grundsatz besteht nach wie vor kein sog. «Konzernprivileg». Konzerngesellschaften sind unter dem Aspekt des Datenschutzes untereinander wie separate, eigenständige Gesellschaften zu betrachten.

(3) Der Beizug von Dritten zur Datenbearbeitung ist den betroffenen Personen im Rahmen der Transparenz- und Informationspflichten in allgemeiner Form (ohne zwingende Nennung von Namen) offen zu legen (beispielsweise in der Datenschutzerklärung).

(4) Typische Einsatzbereiche können sein: Cloudnutzung generell, Nutzung von externen Rechenzentren, Auslagerung von Geschäftsprozessen wie z.B. Messdienstleistungen, Einsatz und Nutzung von Portalen, Onlineshops oder ähnlich.

[2] Technische und organisatorische Massnahmen des Datenschutzes EDÖB: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html

5.7 Umgang mit Daten von juristischen Personen

(1) Daten von juristischen Personen unterstehen nicht dem Schweizerischen DSG (vorbehalten bleiben weitergehende Vorgaben in den kantonalen Datenschutzgesetzen). Auf Daten aus intelligenten Mess-, Steuer- und Regelsystemen von juristischen Personen findet das DSG sinngemäss Anwendung (StromVG, Art. 17c Abs. 1)[3].

6. Umsetzungsempfehlungen Datennutzung

(1) Die Umsetzungsempfehlungen Datennutzung umfassen Themen, welche für die Behandlung bzw. Berücksichtigung der Nutzungsrechte für Daten von Bedeutung sind.

(2) Werden Dienstleistungen (inkl. Datenbearbeitung und Datenspeicherung) für Kunden auf Schweizer Territorium erbracht, gilt grundsätzlich die Schweizer Gesetzgebung. In allen anderen Fällen kommen ergänzende (ausländische) regulatorische Bestimmungen zur Anwendung. Vergleiche auch Kapitel 5.1 Abs. (2).

6.1 Entflechtung (Unbundling)

(1) Die informatorische Entflechtung (Unbundling) beschreibt die Trennung des Netzbetriebs von den übrigen Tätigkeitsbereichen eines EVU (StromVG Art. 10 Abs. 2 «*Wirtschaftlich sensible Informationen, die aus dem Betrieb der Elektrizitätsnetze gewonnen werden, müssen von den Elektrizitätsversorgungsunternehmen unter Vorbehalt der gesetzlichen Offenlegungspflichten vertraulich behandelt werden und dürfen nicht für andere Tätigkeitsbereiche genutzt werden*.»). Andere Tätigkeitsbereiche können bspw. der Energieverkauf im freien Markt, die Energieberatung, das Installationsgeschäft oder das Contracting sein.

(2) Im Rahmen der Teilliberalisierung des Strommarktes wurden durch das Unbundling Wettbewerbsstrukturen geschaffen sowie ein diskriminierungsfreier Netzzugang für Dritte sichergestellt. Das Informatorisches Unbundling soll die unzulässige Nutzung von Informationen aus dem natürlichen Monopol für Aktivitäten im freien Markt verhindern, sodass keine Marktvorteile in den Tätigkeitsbereichen eines EVU ausserhalb des natürlichen Monopols entstehen und dadurch der Wettbewerb geschützt ist. Ein unzulässiger Marktvorteil gegenüber anderen Marktteilnehmern kann beispielsweise entstehen durch:

- einen Minderaufwand
- einen zeitlichen Vorsprung
- einen Mehrertrag

(3) Beim Unbundling ist nicht der Datenschutz Zweck der Bestimmungen, sondern der Schutz eines fairen Wettbewerbs. Es muss sichergestellt sein, dass im Rahmen einer Markttätigkeit kein Marktteilnehmer bevorzugt wird oder von einer bevorzugten Position profitieren kann (Prinzip der «gleich langen Spiesse der Marktteilnehmer»). Daten sind somit neben den Aspekten Datensicherheit und Datenschutz auch unter dem Aspekt Unbundling und Wettbewerbsneutralität zu betrachten und entsprechend zu behandeln.

[3] Quelle: https://www.fedlex.admin.ch/eli/fga/2020/1998/de , s. 70

(4) Obschon in bestimmten Fällen eine Datenverwendung datenschutzrechtlich möglich wäre, können die Vorgaben zum informatorischen Unbundling diese untersagen. Die Datenverwendung in Zusammenhang mit dem informatorischen Unbundling muss immer im konkreten Einzelfall beurteilt werden.

6.2 Datennutzung aus Netzbetrieb und Grundversorgung

(1) Als Grundsatz gilt Daten von Netznutzern, von denen ein Netzbetreiber aufgrund des Netzbetriebs und Erfüllung des Grundversorgungsauftrages Kenntnis hat, dürfen nicht für wettbewerbliche Tätigkeiten genutzt werden. Es sind Massnahmen zu treffen, um die Vorgaben des Unbundling sicherzustellen (Bspw. technische und organisatorische Massnahmen (TOM), Schulungen, Handlungsanweisungen etc.).

(2) Daten von Netznutzern sind in der Regel **wirtschaftlich sensible** Informationen, weil sich der Netzbetreiber mit den gewonnenen Informationen einen Wettbewerbsvorteil verschaffen kann (StromVG Art. 10 Abs. 2). Dazu gehören:

- Name, Adresse und andere Stammdaten von Netznutzern
- Verbrauchsdaten, die aus intelligenten Mess-, Steuer- und Regelsystemen gewonnen werden
- in Zusammenhang stehende Meta- und Strukturdaten wie bspw. wartungsrelevante Informationen

Eine Datennutzung ausserhalb von Netzbetrieb und Grundversorgung durch das EVU, Dritte und ggfs. die Weitergabe an Dritte ist insbesondere möglich, wenn eine explizite Einwilligung dafür vorliegt. Diese Einwilligung darf jedoch nicht auf Basis von Informationen und Ressourcen aus dem Netzbetrieb oder der Grundversorgung eingeholt und bearbeitet werden (vgl. Kapitel 6.1 Entflechtung (Unbundling), Absatz (1) und (2)). Eine Einwilligung liegt beispielsweise dann vor, wenn ein Kunde die Daten selbst an das EVU oder Dritte weitergibt.

(3) Nicht pseudonymisiert sind abrechnungs- und vergütungsrelevante Daten (siehe Definition in Kapitel 7.3 «Messdatenbearbeitung gemäss StromVV») grundsätzlich in:

- Systemen für die Abrechnung von Netznutzung, Energie, Abgaben, Netzzuschlag
- Vergütungen für den Einsatz von Steuer- und Regelsystemen

Die Zuordnung der Personendaten (insbesondere 15-Minuten-Lastgänge) zum entsprechenden Kunden ist nur für Berechtigte (intern oder extern) bearbeitbar, welche abrechnungs- und vergütungsrelevante Prozesse ausführen. Siehe Anhang «Data Compliance - Daten aus Netzbetrieb und Grundversorgung».

(4) Gemäss StromVG werden Messeinrichtungen in den nächsten Jahren auf intelligente Messsysteme umgerüstet. Soweit Lastgangwerte oder Registerwerte abrechnungsrelevant sind, dürfen diese Daten in nicht pseudonymisierter Form zum Zweck der Abrechnung, Vergütung und Verbrauchsvisualisierung verwendet werden (StromVV Art. 8a Abs. 2 lit. c in Verbindung mit Art. 8d Abs. 1, lit. b). Die Weitergabe von Lastgangdaten in die Verrechnungssysteme ist, wenn immer möglich, in aggregierter Form durchzuführen. Beispiel: Wird zur Abrechnung ein Monatswert benötigt, so ist aus dem Messdatenmanagement- oder Energiedatenmanagement-System eine aus den Lastgangdaten aggregierte Monatssumme bzw. der entsprechende Registerwert ins Abrechnungssystem zu übertragen.

(5) Werden Lastgänge für Netznutzer visualisiert, muss die Pseudonymisierung im anzeigenden System so weit aufgelöst werden, dass dem Netznutzer nur die berechtigten Lastgänge bzw. Einspeisegänge verständlich dargestellt werden können.

(6) Für Daten in einem Testsystem gelten dieselben Anforderungen wie für ein Produktivsystem, unabhängig davon, ob die Daten aktuell sind.

6.3 Datennutzung aus intelligenten Messsystemen des EVU

(1) Der Verwendung von Daten aus intelligenten Messsystemen werden gesetzlich enge Schranken gesetzt. Ohne Einwilligung des Endkunden dürfen die Netzbetreiber die Daten zur Verbrauchsvisualisierung nach Art. 8a Abs. 2 lit. c StromVV sowie zum Zweck der Abrechnung und zur Sicherstellung des Netzbetriebs gemäss Art. 8d StromVV bearbeiten.

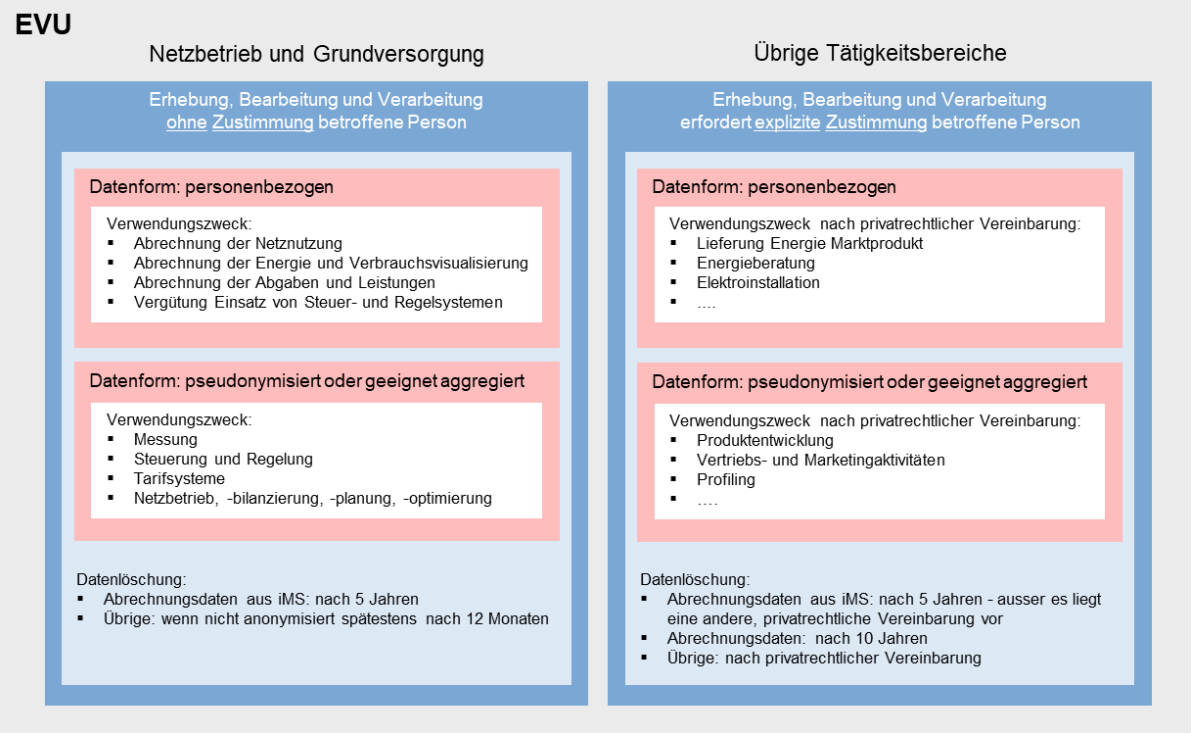


Abbildung 6 Verwendung von Daten aus iMS (Art. 8d StromVV) in Verbindung mit informatorischem Unbundling (Art. 10 Abs. 2 StromVG)

(2) Eine weitergehende Datenverwendung als die in Art. 8a Abs. 2 lit. c und Art. 8d StromVV definierten Anwendungsbereiche ist nur mit einer explizit erlangten Zustimmung des Endkunden (Opt-in) möglich. Für das Einholen der explizit erlangten Zustimmung zur Datennutzung des Endkunden dürfen ausserhalb von Netzbetrieb und Grundversorgung nur (Adress-) Daten verwendet werden, welche nicht aus dem Netzbetrieb und der Grundversorgung stammen (bspw. eingekaufte Adressdaten)[4]. Bei der explizit erlangten Zustimmung ist ein abschliessender Verwendungszweck dem Endkunden anzugeben. Für grundversorgte Endkunden kann dies nicht über die allgemeinen Geschäftsbedingungen geregelt werden. Die explizite Zustimmung sollte nachweisbar sein.

6.4 Einbezug von Dritten

(1) Bezieht ein Unternehmen Leistungen von Dritten, ist sicherzustellen, dass der Datenschutz – und die Datensicherheit, sowie weitere regulatorisch relevante Bestimmungen von diesen eingehalten werden (bei bestehenden und neuen Verträgen). Dritte (vgl. 5.6 «Auftragsdatenbearbeitung») sind bspw. vom Verteilnetzbetreiber (VNB) beauftragte Messdatendienstleister, Energie-Abrechner, Data-Hub-Betreiber, Betreiber von Cloud-Systemen, Systembetreuer eines Outsourcing-Partners oder Supportpersonen eines Software-Herstellers. Als Dritte aus datenschutzrechtlicher Sicht sind jegliche Rechtseinheiten zu verstehen, die ungleich der Rechtseinheit sind, welche die Daten erhebt/bearbeitet. Dies gilt grundsätzlich auch innerhalb von Konzernstrukturen.

[4] Vgl. Kapitel 6.2 Datennutzung aus Netzbetrieb und Grundversorgung

7. Umsetzungsempfehlungen Data Compliance

(1) Data Compliance[5] in der Energiebranche umfasst die Einhaltung von Gesetzen, Verordnungen, Branchendokumenten und eigenen internen Richtlinien insbesondere im Hinblick auf Erhebung, Bearbeitung, Weitergabe und Verwendung von Daten. Dabei ist Bearbeitung ein umfassender Begriff für Erfassung, Speicherung, Löschung, Veränderung, Backup, Transfer, Einsichtnahme, Auswertung usw. Data Compliance in der Energiebranche wird primär unter den Gesichtspunkten Datenschutz, Datensicherheit und Unbundling betrachtet.

- Der Datenschutz wahrt die Privatsphäre von Personen. Er soll die informationelle Selbstbestimmung im Umgang mit relevanten Daten und Informationen ermöglichen und sichern
- Die Datensicherheit beschreibt Anforderungen und Massnahmen, um die erforderliche physische und logische Sicherheit der Daten und Informationen sicherzustellen
- Massgebliche rechtliche Grundlagen für die Sicherstellung der Data Compliance sind unter anderen die Stromversorgungsverordnung (StromVV, Art.8 und Art. 8d), das Datenschutzgesetz (DSG) und die Verordnung zum Datenschutzgesetz (VDSG)
- Die Grundlagen zur Sicherstellung von Data Compliance sind im VSE-Bericht «Data Policy in der Energiebranche (2018)», in Kapitel 6 «Data Compliance», beschrieben. Darin aufgezeigt werden technische und organisatorische Massnahmen
- Datenschutz und Datensicherheit bedingen sich gegenseitig

(2) Die konkrete Ausgestaltung der Data Compliance berücksichtigt die Rahmenbedingungen der einzelnen EVU (Unternehmensgrösse, -organisation, Tätigkeitsbereiche usw.).

7.1 Datenschutz

(1) Die rechtlichen Anforderungen der Datenschutzgesetzgebung im Umgang mit Personendaten bedingen eine Umsetzung im Unternehmen in Form von Weisungen, Richtlinien, Checklisten, Manuals etc.

(2) Für die Umsetzung und die Sicherstellung des erforderlichen Datenschutzes müssen die im Zusammenhang mit der Datennutzung identifizierten personenbezogenen Daten hinsichtlich Schutzbedarf, regelkonforme Bearbeitung, Nutzung und Weitergabe untersucht werden. Zudem sollen benötigte technische und organisatorische Massnahmen (TOM) festgehalten und umgesetzt werden. Die entsprechenden Informationen werden u.a. im Verzeichnis der Bearbeitungstätigkeiten (VDB) festgehalten. Siehe dazu Kapitel 8.3 «Verzeichnis der Bearbeitungstätigkeiten».

(3) Eine vollständige Datenschutzanalyse umfasst alle Daten, d.h. auch diejenigen, die keinen speziellen Bezug zur Energiebranche haben. Beispiele dafür sind Mitarbeitenden-Daten (Unfallberichte, Arztzeugnisse, o.ä.), Kunden- und Lieferantendaten, Buchhaltung, Verträge, Inventar, Prozessdokumentationen, Verfahren und Abläufe, Aufträge, Rechnungen, Betriebsgeheimnisse. Gemäss Kapitel 5.5 «Datenbearbeitung» Abs. (5) kommen verschiedene gesetzliche Grundlagen für die genannten Daten zur Anwendung. Grundsätzlich müssen alle Personendaten im Verzeichnis der Bearbeitungstätigkeiten (VDB) erfasst und festgehalten werden. Siehe dazu Kapitel 8.3 «Verzeichnis der Bearbeitungstätigkeiten».

[5] Compliance = Regeltreue oder Regelkonformität

(4) Insbesondere durch Auswertung, Anreicherung und Kombination von Daten können neue oder andere Personendaten entstehen, weshalb vorgängig die Notwendigkeit einer systematischen Risikoabschätzung (Datenschutz-Folgenabschätzung DSFA) zu prüfen ist. Im Internet lassen sich diverse Vorlagen dazu finden.

(5) Eine Datenschutz-Folgenabschätzung hat im Vorfeld einer Datenbearbeitung von personenbezogenen Daten mit einem hohen Risiko für die Persönlichkeit oder die Grundrechte für die betroffenen Personen in Form einer detaillierten Risikoabschätzung für den Datenbearbeitungsprozess zu erfolgen (Ausnahmen siehe Art. 22 DSG).

7.2 Datensicherheit

(1) Für die Gewährleistung der Datensicherheit werden die notwendigen Anforderungen und Massnahmen identifiziert. Zu diesem Zweck muss in einem ersten Schritt der Schutzbedarf der Datenobjekte festgestellt werden. Daraus werden in einem zweiten Schritt die Massnahmen abgeleitet. Siehe dazu VSE-Bericht «Data Policy in der Energiebranche (2018)», Kapitel 6.2 «Datensicherheit».

(2) Für alle Datenobjekte wird eine CIA-Analyse und Bestimmung auf Basis der VDB durchgeführt.

- C = Confidentiality = Vertraulichkeit
- I = Integrity = Integrität
- A = Availability = Verfügbarkeit

Zusätzlich sind die Datenobjekte auch bezüglich der

- A = Authentication = Authentifizierung
- A = Authorization = Autorisierung
- A = Accounting = Nachverfolgung

zu beurteilen. Damit ergibt sich eine umfassende CIA-AAA-Analyse.

7.3 Messdatenbearbeitung gemäss StromVV

Zur besseren Übersicht wird die Messdatenbearbeitung gemäss StromVV in der nachfolgenden Grafik zusammengefasst.

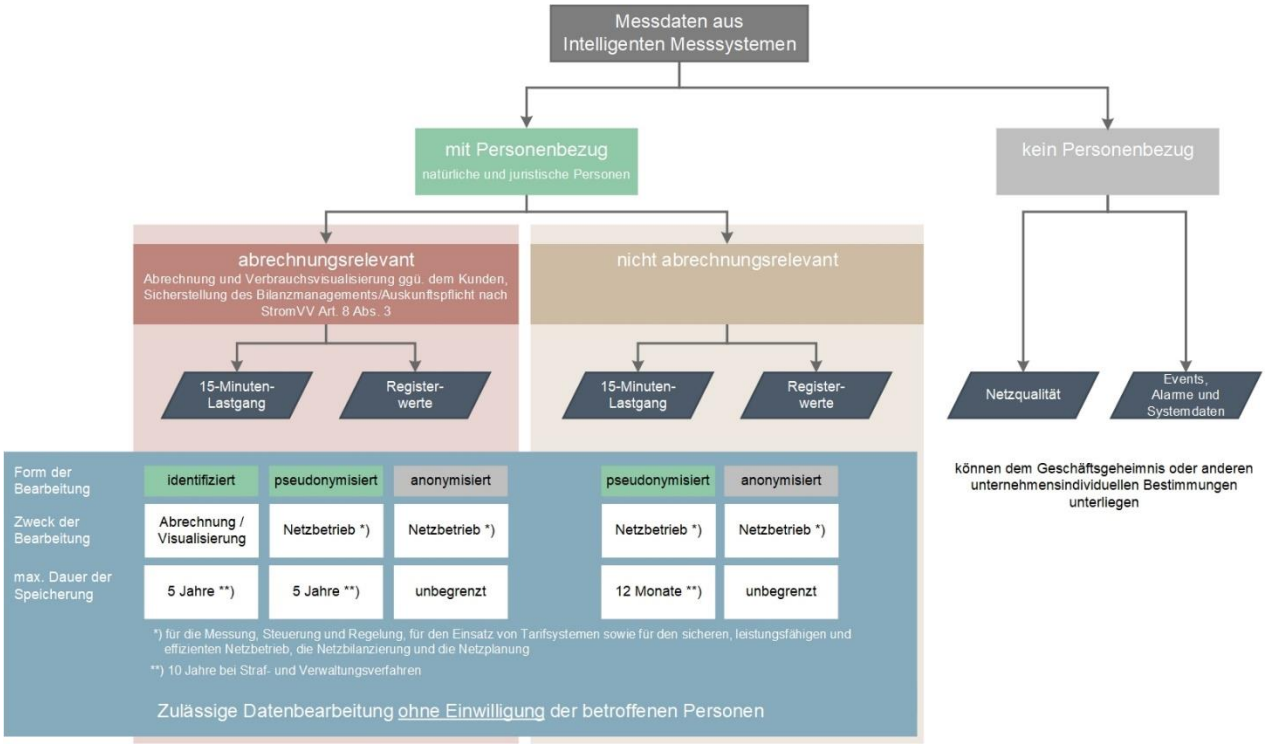


Abbildung 7 Messdatenbearbeitung gemäss StromVV

7.3.1 Messdatenbearbeitung mit Personenbezug (abrechnungsrelevante Daten)

(1) Auf Personendatenbearbeitungen im Zusammenhang mit intelligenten Mess-, Steuer- und Regelsystemen findet gemäss StromVG Art. 17c das Datenschutzgesetz Anwendung. Diese Regelung gilt auch für Daten von juristischen Personen. Messdaten mit Personenbezug dürfen folgendermassen bearbeitet und aufbewahrt werden, dabei ist es unerheblich, ob es sich um Lastgangdaten (maximal mit 15 min-Auflösung) oder Registerwerte handelt.

- Nach StromVV Art. 8d Abs. 3 müssen die Daten nach zwölf Monaten vernichtet oder anonymisiert werden, es sei denn, sie sind abrechnungsrelevant oder dienen der Visualisierung für den Kunden
- Daten sind abrechnungsrelevant, wenn sie zur Erstellung von Abrechnungen und zur Sicherstellung des Bilanzmanagements oder der Auskunftspflicht gemäss StromVV Art. 8 Abs. 3 und 4 verwendet werden
- Daten, welche abrechnungsrelevant oder der Visualisierung für den Kunden dienen, dürfen ohne Einwilligung der betroffenen Kunden in nicht pseudonymisierter Form (d.h. personenidentifizierter Form, gemäss StromVV 8d, Abs. 1 lit. b) bearbeitet und bis zu 5 Jahre aufbewahrt werden

(StromVV Art. 8 Abs. 4 «*Es müssen alle in den letzten fünf Jahren erhobenen Daten geliefert werden.*»). Die Daten sind anschliessend zu löschen oder in eine geeignete Anonymisierung bzw. in ein geeignetes Aggregat zu überführen (vergleiche Kapitel 7.1)

- Daten zur Sicherstellung des Netzbetriebs (gemäss StromVV 8d, Abs. 1 lit. a) dürfen ohne Einwilligung der betroffenen Kunden in pseudonymisierter Form bearbeitet und bis zu 5 Jahre aufbewahrt werden
- Daten aus Straf- und Verwaltungsverfahren sowie die eigentliche Stromrechnung müssen während 10 Jahren aufbewahrt werden (EnV Art. 70)
- Für eine längere Datenaufbewahrung muss die ausdrückliche Einwilligung des Kunden vorliegen

7.3.2 Messdatenbearbeitung mit Personenbezug (nicht abrechnungsrelevante Daten)

(1) Nach StromVV Art. 8d Abs. 3 müssen diese Daten (z.B. zur Sicherstellung des sicheren Netzbetriebes) nach zwölf Monaten vernichtet oder anonymisiert werden.

- Sie dürfen ohne Einwilligung der betroffenen Kunden in pseudonymisierter Form bearbeitet und bis 12 Monate aufbewahrt werden
- Daten aus Straf- und Verwaltungsverfahren müssen während 10 Jahren aufbewahrt werden (EnV Art. 70)
- Für eine längere Datenaufbewahrung muss die ausdrückliche Einwilligung des Kunden vorliegen

7.3.3 Messdatenbearbeitung ohne Personenbezug

(1) Als Messdaten ohne Personenbezug werden Events, Alarme, PQ-Daten usw. bezeichnet.

- Sie dürfen uneingeschränkt bearbeitet und aufbewahrt werden
- Diese Daten können dem Geschäftsgeheimnis oder weiteren Unternehmens-internen Bestimmungen unterliegen

7.3.4 Weitere Bestimmungen

(1) Anonymisierte Daten

- Anonymisierte Daten dürfen unbeschränkt bearbeitet und aufbewahrt werden (siehe Kapitel 3 «Definitionen»). In diesem Fall können die Daten jedoch nicht mehr für die Erfüllung der Auskunftspflicht nach StromVV Art 8 Abs. 4 genutzt werden, da die Zuweisung an einen Netznutzer nicht mehr möglich ist

(2) StromVV, Art. 8 Messwesen und Informationsprozesse, Abs. 4:
«Die Netzbetreiber liefern den Verantwortlichen von Bilanzgruppen sowie anderen Beteiligten im Einverständnis mit den betroffenen Endverbrauchern oder Erzeugern auf Begehren und gegen eine kostendeckende Abgeltung zusätzliche Daten und Informationen. Es müssen alle in den letzten fünf Jahren erhobenen Daten geliefert werden.»

- Für die Weitergabe zusätzlicher Daten und Informationen muss das Einverständnis des Netznutzers vorliegen

(3) Die Unternehmen müssen für alle Datenbestände ein Lebenszyklusmanagement sicherstellen. Dies umfasst bspw. die Erfassung/Erhebung, Bearbeitung, Aufbewahrung, Archivierung, Löschung, Auskunft (siehe auch Kapitel 5.5 «Datenbearbeitung», Abs. (3).

7.4 Weiterer Umgang mit personenbezogenen Daten

(1) Für jegliche Art der weitergehenden Verwendung von Daten, z.B. für die Bekannt- oder Weitergabe der Daten, muss grundsätzlich unterschieden werden zwischen Daten aus der Tätigkeit innerhalb der Grundversorgung (öffentlich-rechtliches Vertragsverhältnis) und Daten aus der Tätigkeit ausserhalb der Grundversorgung (privatrechtliches Vertragsverhältnis). Entscheidend hierbei ist die «Alternativlosigkeit» von gebundenen Kunden.

- **Daten aus der Tätigkeit innerhalb der Grundversorgung**: Die im Rahmen der Grundversorgung bearbeiteten Daten dürfen grundsätzlich nicht zweckentfremdet weiterverwendet werden. Sollen diese Daten für Zwecke ausserhalb der Grundversorgung verwendet werden, müssen sie separat am freien Markt beschafft werden (Vermeidung von Wettbewerbsverzerrung)
- **Daten aus der Tätigkeit ausserhalb der Grundversorgung**: Eine entsprechende Weiterverwendung von Daten ausserhalb der Tätigkeit der Grundversorgung muss vertraglich geregelt sein (z.B. durch ein explizites oder implizites Einverständnis des Kunden). Eine entsprechende Regelung in den AGB, unter Berücksichtigung zwingender Vorgaben des Datenschutzgesetzes sowie des Unbundling gemäss StromVG, 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 mindestens in pseudonymisierter Form erfolgen. Die Weitergabe der Informationen für die Entschlüsselung der Pseudonyme erfolgt immer separat und nur an die dazu berechtigten Personen (bspw. für die Messdatenlieferung an den Energielieferanten)

(2) Die Datenherausgabe und -übertragbarkeit nach StromVV, Art. 8a, Abs 2, lit. c zielt darauf ab, betroffenen Personen resp. Kunden nebst einer Visualisierung auch den Zugang und Download ihrer 15-Minuten Messdaten der letzten 5 Jahre unentgeltlich in einem gängigen internationalen Datenformat zu ermöglichen (z.B. im .csv oder .xml Format).

(3) Die Datenherausgabe und -übertragung nach DSG Art. 28 zielt darauf ab, dass im Falle einer automatisierten Datenbearbeitung die betroffene Person das Recht hat, vom Verantwortlichen die Herausgabe ihrer Personendaten in einem gängigen elektronischen Format zu verlangen. Dies gilt auch für bestehende resp. die Anbahnung von Verträgen. Sofern keine unverhältnismässigen Aufwände anfallen, kann die betroffene Person auch eine Übertragung ihrer Daten an einen anderen Verantwortlichen verlangen.

(4) Bei einer Datenbearbeitung ausserhalb der eigenen Rechtseinheit (Dritte oder andere Rechtseinheit innerhalb eines Konzerns) sind die spezifischen rechtlichen Grundlagen zu berücksichtigen.

(5) Werden Personendaten ins Ausland bekanntgegeben, so ist die Person bei deren Beschaffung unter Angabe des Staates darüber zu informieren. Hierbei ist besonders auf Territorien und Räume (bspw. virtueller Raum Internet, Cloud, Anwendung) zu achten. Falls das entsprechende Land keine adäquate Datenschutzgesetzgebung[6] kennt und das notwendige Niveau auch nicht in anderer Art garantiert werden kann, muss zusätzlich ein explizites Einverständnis des Kunden eingeholt und zusätzliche technische und organisatorischen Massnahmen getroffen werden (siehe dazu DSG Art. 17 Abs. 1 lit. a).

(6) Für die Aufbewahrung und Archivierung der Daten müssen die relevanten Vorschriften gemäss Geschäftsbücherverordnung und verschiedenen weiteren spezialrechtlichen Regelungen eingehalten werden. Dies beinhaltet insbesondere Vorgaben zur Revisionssicherheit und zur Dauer der Aufbewahrung. Darüber hinaus existiert die Aufbewahrungspflicht für Netzbetreiber von Metering-Daten gemäss StromVV. Siehe dazu Kapitel 7.3 «Messdatenbearbeitung gemäss StromVV».

(7) Die betroffene Person hat das Recht, Auskunft über ihre bearbeiteten Daten zu erhalten. Hierfür stellt der eidgenössische Datenschutzbeauftrage ein Standardformular (einfaches Auskunftsbegehren) zur Verfügung. Auskunftsbegehren müssen grundsätzlich innerhalb von 30 Tagen kostenlos beantwortet werden. Weitergehend besteht in gewissen Fällen ebenfalls die Möglichkeit, dass Personen eine Berichtigung, Sperrung oder Löschung ihrer Daten einfordern. Rechtlich und regulatorisch höher gestellte Rechte und Pflichten bleiben vorbehalten.

7.5 Umgang mit Daten ohne direkten Personenbezug (Sachdaten)

(1) **Asset- und GIS-Daten**
Die Vorgaben gemäss Leitungsverordnung (LeV) müssen eingehalten werden (bspw. die Regelung, welche Informationen öffentlich einsehbar sein müssen). Noch offen ist, inwieweit die Dokumentation von kritischen Infrastrukturen wie z.B. Kernkraftwerken, Militäranlagen, Spitälern besonders gesichert werden muss.

(2) **Auftrags- und Ereignisdaten**
Sind natürliche oder juristische Personen (StromVG Art. 17c) betroffen, gilt die Datenschutzgesetzgebung und der Umgang mit den Daten muss gemäss den entsprechenden Vorgaben erfolgen, sofern sie aus intelligenten Mess-, Steuer- und Regelsystemen stammen. Siehe dazu auch Kapitel 5.7 «Umgang mit Daten von juristischen Personen».

(3) **SCADA-Daten**
Sind natürliche oder juristische Personen (StromVG Art. 17c) betroffen, gilt die Datenschutzgesetzgebung und der Umgang mit den Daten muss gemäss den entsprechenden Vorgaben erfolgen, sofern sie aus intelligenten Mess-, Steuer- und Regelsystemen stammen. Siehe dazu auch Kapitel 5.7 «Umgang mit Daten von juristischen Personen».

7.6 Schutzbedarf von Daten

(1) Um den Schutzbedarf der vorhandenen Daten zu bestimmen, können die unternehmensrelevanten Daten auf Basis eines Datenmodells sowie einer Übersicht der eingesetzten Anwendungen erhoben werden.

[6] Siehe Liste des Eidgenössischen Datenschutzbeauftragten (EDÖB) «Liste der Staaten, deren Gesetzgebung einen angemessenen Datenschutz gewährleistet (Art. 6 Abs. 1 DSG)» https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/staatenliste.pdf.download.pdf/20200908_Staatenliste_d.pdf

(2) **Datenmodell**

Für EVU, welche primär als Netzbetreiber auftreten, kann ein vereinfachtes Datenmodell im Sinne eines Datenkataloges verwendet werden. Es umfasst Daten, welche zur Abwicklung des Versorgungsauftrages für seine Kunden und zur Dokumentation des Verteilnetzbetriebs erforderlich sind:

- Kundendaten, wobei die Kunden eines EVU mehrheitlich natürliche Personen sind
- Daten für die Dokumentation der eigenen Anlagen und die Verträge des EVU mit Dritten
- Beispiele sind im Anhang «Data Compliance - Datenmodelle und Anwendungen» beschrieben

(3) Der Schutzbedarf erstreckt sich sowohl auf personenbezogene Daten als auch auf Sachdaten:

- Personenbezogene Daten sind gemäss Datenschutzgesetz angemessen bezüglich Vertraulichkeit und Integrität zu schützen. Auch Daten von juristischen Personen haben gemäss StromVG Art. 17c diesen Schutzbedarf
- Daten für den Netzbetrieb sind u.a. nötig, um die Versorgungssicherheit zu garantieren. Dazu sind besonders ihre Integrität und Verfügbarkeit relevant
- Beispiele sind im «Anhang Data Compliance - Datenmodelle und Anwendungen» zu finden

(4) **Definition des Schutzbedarfs**

Die beispielhafte Anwendungslandschaft eines EVU ist im «Anhang Data Compliance - Datenmodelle und Anwendungen» beschrieben. Aufgrund der zu bearbeitenden Daten und der abzuwickelnden Prozesse lässt sich der Schutzbedarf für einzelne Anwendungen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit ableiten. Sind in einem Prozess mehrere Systeme beteiligt, werden die zu erfüllenden Mindestanforderungen vom System mit dem höchsten Schutzbedarf bestimmt, sofern systemisch keine Abgrenzung erfolgen kann.

Anwendungen	Vertraulichkeit	Integrität	Verfügbarkeit
Abrechnungssystem	Hoch	Hoch	Normal
Mobile Zählerauslesung	Normal	Normal	Normal
Messdatenauslesesystem (HES, MDM, ZFA, Smart Metering)	Hoch	Hoch	Normal
EDM	Hoch	Hoch	Normal
Rundsteuerung / Lastmanagement	Normal	Hoch	Hoch
SCADA-System	Normal	Hoch	Hoch
Anlagedokumentation / Fileablage	Normal	Hoch	Normal

Tabelle 4 Beispiel des Schutzbedarfs für Anwendungen

(5) **Sicherstellung des Schutzbedarfs und der Verantwortlichkeiten**

Für Systeme mit erhöhten Anforderungen bezüglich des Schutzbedarfs sind spezielle Massnahmen zur Risikoreduktion umzusetzen. Wichtig ist, dass Anforderungen wie Zugriffsrechte, Datensicherung oder auch Verschlüsselung angemessen und auf dem aktuellen Stand der Technik realisiert werden.

(6) Die Verantwortung für das Risikomanagement ist in allen EVU zu regeln. Mehrere Aufgaben und Rollen gemäss Kapitel 8.2 «Rollen und Funktionen» können in einem EVU je nach Unternehmensgrösse auch durch eine einzige Person oder Dritte wahrgenommen werden. Die Gesamtverantwortung für das Risikomanagement trägt in allen Fällen die Geschäftsleitung (das geschäftsführende Organ) des EVU.

8. Umsetzungsempfehlungen Data Governance

(1) Die Data Governance legt Mechanismen und Regelungen zur Definition, Umsetzung, Pflege sowie nachhaltigen Weiterentwicklung der Data Policy fest. Dazu werden die erforderlichen Governance-Aufgaben, -Rollen, -Gremien und -Prozesse definiert.

(2) Die angeführten organisatorischen Strukturen und Massnahmen sind Empfehlungen, welche eine nachhaltige Umsetzung der Data Policy in einem Unternehmen sicherstellen sollen.

8.1 Aufgaben der Data Governance

(1) Die Unternehmen sind für die Umsetzung einer auf ihre Bedürfnisse angepassten Data Policy und deren Aktualisierungen verantwortlich. Sie berücksichtigen die nachfolgend beschriebenen Aufgaben. Das Datenschutzgesetz geht dabei von einer prozessorientierten Sichtweise aus.

(2) **Strategisches Datenmanagement**
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 das Datenqualitätsmanagement und das Data Reporting.

(3) **Dateninventarisierung**
Zur Sicherstellung des erforderlichen Datenschutzes und der notwendigen Datensicherheit wird ein umfassendes Dateninventar (Ist-Bestand) aufgebaut und gepflegt. Siehe dazu Kapitel 5.5 «Datenbearbeitung».

(4) **Datenqualitätsmanagement**
Unter Datenqualitätsmanagement wird die Summe aller organisatorischen, technischen und betrieblichen Massnahmen zur Sicherstellung der aus regulatorischer und unternehmerischer Sicht notwendigen Datenqualität verstanden. Dazu werden geeignete Prozesse, Messgrössen, Instrumente und eine angemessene Organisation eingesetzt.

(5) **Data Reporting**
Data Reporting umfasst die Erstellung und den Versand der erforderlichen regulatorischen Datenreports sowie die Datenauskunft gegenüber betroffenen Bedarfsträgern. Die Unternehmen sind auch für die Datenauskunft und das Data Reporting mit adäquater Qualität gegenüber Daten-Nutzungsberechtigten, Behörden und Regulatoren verantwortlich. Diese Aufgabe enthält ebenfalls die allfällige Auskunftspflicht gegenüber Behörden und weiteren Auskunftsberechtigen.

8.2 Rollen und Funktionen

(1) Je nach Form und Grösse der Organisation kann eine Person mehrere Rollen wahrnehmen oder solche werden durch Dritte ausgeführt, wobei die Verantwortung immer beim EVU bleibt. In kleineren

Unternehmen kann die Geschäftsführung entsprechende Funktionen übernehmen. Bei Grossunternehmen können diese Rollen Einzelpersonen zugewiesen werden. Eine adäquate Gewaltenteilung ist immer sicherzustellen.

(2) Für die Wahrnehmung der Aufgaben aus den Bereichen Daten-Nutzung, Data Compliance und Data Governance wird die Einführung nachfolgender Rollen empfohlen:

Kürzel	Rollen- bzw. Funktionsbezeichnung	Beschreibung Aufgaben
DPC	Data Protection Consultant / Datenschutz-Berater gemäss Art. 10 DSG	– Zuständig und verantwortlich für Schulung und Beratung des EVU (Verantwortlichen) sowie Mitwirkung bei der Anwendung der Datenschutzvorschriften sowie Datenschutz Folgen-Abschätzungen (DSFA) Weitere mögliche Aufgaben können sein: – Erstellung und Pflege des Verzeichnisses der Datenbearbeitung – Aufbau und Entwicklung der Datenschutzorganisation im Unternehmen – Verfassen einer Unternehmensrichtlinie zum Datenschutz – Prüfung der Produkte und Leistungen des Unternehmens im Hinblick auf Datenschutz – Abschluss von Auftragsvereinbarungen (Aufträge zur Datenbearbeitung) bei externen Dienstleistern – Prüfung der Rechtmässigkeit von Überwachungstätigkeiten – Erstellung einer Richtlinie für die E-Mail- und Internet-Nutzung im Unternehmen – Erstellung weiterer Richtlinien für den Umgang mit personenbezogenen Daten im Unternehmen – Sicherstellung des technisch-organisatorischen Datenschutzes (TOM) – Antworten auf Auskunftsverlangen von Betroffenen oder Aufsichtsbehörden hinsichtlich Bearbeitung/Speicherung personenbezogener Daten – Meldepflichten gemäss DSG Art. 24
CISO	Chief Information Security Officer / Chef Informationssicherheit	Zuständig für die Informationssicherheit einer Organisation. Mögliche Aufgaben können sein: – Überwachung der Umsetzung von aus den Revisionsberichten resultierenden Empfehlungen – Beratung von Fachbereichen bei Digitalisierungsvorhaben und Mitgestaltung von modernen Lösungsansätzen in Projekten – Überwachung der Sicherheitslage und Beurteilung von Risikoanalysen – Definition von Datensicherheitsstandards und Überwachung der Einhaltung – Unterstützung der operativen Bereiche bei deren Aufgaben und systematische Überwachung der durchgeführten Aktivitäten – Meldepflichten bei kritischen Cyber Security Vorfällen: Gemäss NCSC/VBS (Stand 01.22 noch in Vernehmlassung)

Kürzel	Rollen- bzw. Funktions-bezeichnung	Beschreibung Aufgaben
CSO	Chief Security Officer / Chef Sicherheit / Sicherheits-Chef	Zuständig und verantwortlich für alle Belange der physischen Sicherheit (Gebäude, Schlüssel, Zutritte …). Mögliche Aufgaben können sein: – Im Tagesgeschäft Durchsetzung der Sicherheitsvorgaben – Sicherstellen, dass geeignete technische, physikalische und verfahrenstechnische Kontrollen eingeführt sind – Erstellung von Vorgaben, Bereitstellen von Ressourcen, Unterstützung und Überprüfung, dass Informationen angemessen und innerhalb ihres Zuständigkeitsbereichs physisch geschützt sind – Information über von Arbeitnehmern/Lieferanten gemachte Empfehlungen – Information über tatsächliche oder vermutete Verstösse gegen die Richtlinien (Sicherheitsvorfälle) – Überprüfung der Einhaltung der Sicherheitspolitik und gelegentliche interne Audits
CO	Compliance Officer	– Identifikation und Bewertung von Risiken der Nichteinhaltung von Vorschriften durch das Unternehmen – Bewertung von Risiken von gerichtlichen, administrativen oder disziplinarischen Sanktionen, erheblichen finanziellen Verlusten oder Reputationsschäden, die sich aus der Nichteinhaltung spezifischer (legislativer oder regulatorischer) Bestimmungen, beruflicher und ethischer Standards oder Anweisungen des Exekutivorgans ergeben – Informations-, Schulungs- und Beratungsfunktion für die Mitarbeitenden aller Hierarchiestufen

Tabelle 5 Übersicht von Data Policy relevanten Rollen und Funktionen

(3) Die Gesamtverantwortung für die Definition, Umsetzung, Pflege sowie nachhaltige Weiterentwicklung der Data Policy Regelungen liegt bei der Unternehmensführung. Es wird empfohlen, die Mitarbeitenden periodisch angemessen zu schulen.

(4) Das Unternehmen ist bei einem Zwischenfall verpflichtet, nachzuweisen, dass die entsprechenden Vorkehrungen getroffen wurden.

(5) Anhand der nachfolgenden Abbildung werden das Zusammenspiel von Informationssicherheit und Datenschutz illustriert:

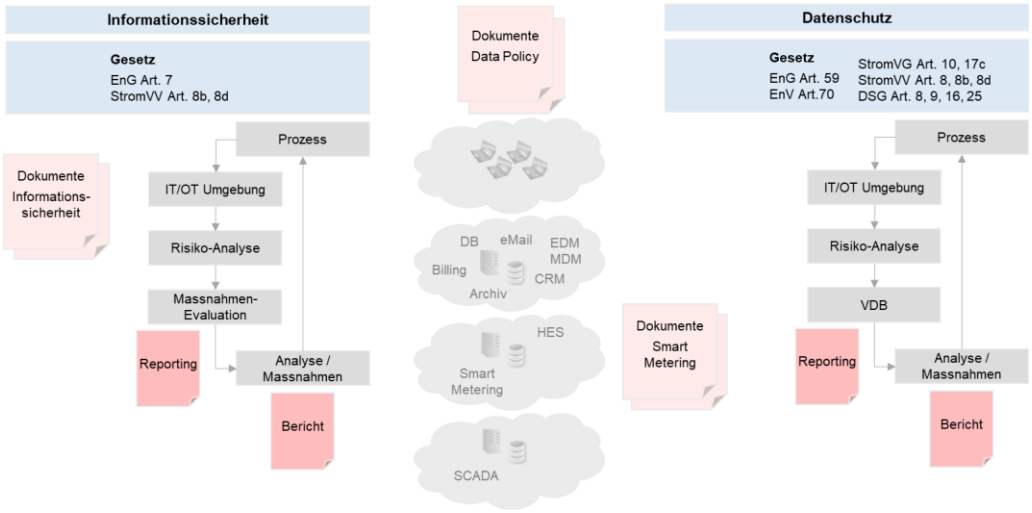


Abbildung 8 Zusammenspiel Informationssicherheit und Datenschutz

- Der CISO analysiert die Anforderungen an die Informationssicherheit und definiert Massnahmen. Für die Aufrechterhaltung des sich verändernden Sicherheitsniveaus ist ein Qualitätssicherungsprozess definiert
- Der DPC analysiert die Informationsflüsse in der Firma, führt eine Risikoanalyse durch und definiert die Grundsätze für den Zugriff und die Verwendung von Daten. Er gewährleistet, dass die VDB-Tabelle ausgefüllt wird
- Ein geeignetes Datenschutz-Managementsystem stellt u.a. die kontinuierliche Verbesserung, eine angemessene Organisation und ein regelmässiges Reporting an die Unternehmensführung sicher

8.3 Verzeichnis der Bearbeitungstätigkeiten

(1) Das im gleichnamigen Anhang beschriebene Verzeichnis der Bearbeitungstätigkeiten (VDB) kann als mögliche Grundlage für das Verzeichnis/Register gemäss Kapitel 5.5 «Datenbearbeitung» dienen.

(2) Das VDB gibt Auskunft über alle wesentlichen Aspekte der Datenbearbeitung (im Sinne einer Minimalanforderung) für alle aufgelisteten Datenklassen des Unternehmens: von der Erhebung, über die Bearbeitung, zur Weitergabe bis zur Löschung.

(3) Die im VDB enthaltenen Informationen sind des Weiteren für die Bearbeitung des Themas IT- & Cyber-Security von Nutzen.

(4) Das Verzeichnis ist ein zentrales Hilfsmittel zur Umsetzung der Data Policy, umfasst Geschäfts- und IT-Aspekte und bedingt eine bereichsübergreifende Herangehensweise, Bearbeitung und Pflege.

(5) Das VDB dient als Ausgangspunkt für die Festlegung und Umsetzung von organisatorischen und technischen Sicherheitsmassnahmen. Dazu können unterstützend Standards wie die ISO/IEC-27000-Reihe oder weitere Best Practice Regularien verwendet werden. Siehe auch Bericht «Data Policy in der Energiebranche», Kapitel 6.2.1. mit heute verfügbaren Best-Practices und Standards für den Aufbau, die Umsetzung und Pflege eines Informationssicherheitsmanagements (ISMS) oder Privacy Information Management System (PIMS).

(6) Die empfohlene VDB-Struktur ist im Anhang «Data Governance - Verzeichnis der Bearbeitungstätigkeiten» ersichtlich.

9. Anhang Data Compliance - Datenmodelle und Anwendungen

Datenmodell

(1) Von Kunden eines EVU werden folgende Daten verwaltet und bearbeitet (nicht abschliessend):

- Kundendaten (bspw. in der Rolle Vertragspartner, Rechnungsempfänger, Eigentümer)
  - Name, Vorname, Firmenname
  - Adresse, Zustelladresse
  - Gebäude
- Vertragsdaten
  - Stromlieferverträge, Netzanschlussverträge und Netznutzungsverträge mit Gültigkeitsdauer
  - Verbrauchsgruppen / Verbrauchstypen
  - Produkt, Preiselemente, Rechnungsperioden
  - Rechnungsadresse
  - Allenfalls Informationen bezüglich Inkassos
  - Allenfalls Prognosedaten
- Messdaten
  - Abrechnungsdaten / Verbrauchsdaten (Wirkenergie, Blindenergie, Leistung)
  - Wenn vorhanden Lastgangdaten (mit 15 Minutenauflösung)
  - Allenfalls lokale Strom- oder Spannungswerte
- Anlagedaten
  - Anschlussleistung, Sicherungsgrössen, Nullung, Zugang …
  - Angaben von grossen Verbrauchern (Boiler, Wärmepumpen, Speicher, Waschmaschine …)
  - Angaben von Produktionsanlagen (Technologie, Leistung …)
  - Zähler, Rundsteuerempfänger mit verwendeten Kommandos

(2) Die Dokumentation der eigenen Anlagen und die Verträge eines EVU mit Dritten umfasst (nicht abschliessend):

- Dokumentation der Anlagen (Asset-Daten)
- GIS-Daten
- Messdaten aus dem Netz (Netzqualität, …)
- Vertragsdaten mit Lieferanten und Dienstleistern
- Allenfalls SCADA Daten

(3) Personenbezogene Daten sind gemäss Datenschutzgesetz adäquat bezüglich Vertraulichkeit und Integrität zu schützen. Als personenbezogene Daten gelten (nicht abschliessend):

- Kundendaten
  - Name, Vorname

    - Adresse
- Vertragsdaten
    - Verbrauchsgruppen / Verbrauchstypen
    - Informationen bezüglich Inkassos
    - Prognosedaten
- Messdaten
    - Lastgangdaten (maximal mit 15 min-Auflösung)
- Anlagedaten
    - Rundsteuerempfänger mit verwendeten Kommandos
    - Generelle Steuerungsdaten

(4) Daten für den Netzbetrieb sind u.a. nötig, um die Versorgungssicherheit zu garantieren. Deren Integrität und Verfügbarkeit ist wichtig. Zu schützende Daten sind (nicht abschliessend):

- Messdaten beim Kunden
    - Lastgangdaten (maximal mit 15 min-Auflösung)
    - Lokale Strom- oder Spannungswerte
- Anlagedaten beim Kunden
    - Angaben von grossen Verbrauchern (Boiler, Wärmepumpen, Speicher, Waschmaschine, …)
    - Angaben von Produktionsanlagen (Technologie, Leistung, …)
- Netzbetreiberdaten
    - Dokumentation der Anlagen (Asset-Daten)
    - Messdaten aus dem Netz (Netzqualität, …)
    - SCADA Daten

10. Anhang Data Compliance - Daten aus Netzbetrieb und Grundversorgung

Beschreibung einer vereinfachten Anwendungslandschaft eines EVU

(1) Kundenbezogene Daten werden in der Regel in einem Abrechnungssystem erfasst und gepflegt. Vielfach werden mit einem mobilen Zählerauslesungssystem die Abrechnungsdaten durch einen Mitarbeiter vor Ort aus dem Zähler ausgelesen und ins Abrechnungssystem übertragen.

Die Zählerfernauslesung (sowohl herkömmlich als auch über ein Smart Metering System / iMS) ist oftmals an einen Dienstleister ausgelagert. Dasselbe gilt für das Energiedatenmanagement-System. Diese Systeme sind in der Regel über Fileschnittstellen miteinander gekoppelt.
Für die Lastbewirtschaftung wird heute in vielen Fällen eine klassische Rundsteueranlage eingesetzt, welche durch das EVU beschafft und mit Unterstützung des Herstellers betrieben wird. Im Zusammenhang mit einem Smart Meter Rollout werden diese teilweise durch Smart Metering basiertes Lastmanagement ersetzt.
Die Dokumentation der Anlagen erfolgt in einem Anlagendokumentationssystem, welches teilweise vom selben Hersteller stammt wie das Abrechnungssystem. Die weitere Dokumentation ist in der Regel filebasiert abgelegt oder nur auf Papier vorhanden.

(2) Nachfolgend findet sich eine beispielhafte Übersicht von Datenschutzanforderungen, welche während verschiedenen Datenbearbeitungsschritten einzuhalten sind:

Datentypen									
kWh / DC	**HES**	**MDM**	**Regelsysteme**	**EDM**	**Marktpartner**	**Profiling**	**Billing**	**Portal**
Lastgangdaten	Lastgangdaten	Lastgangdaten	Zähler-Nr.	Lastgangdaten	Lastgangdaten	Lastgangdaten	Zähler stände	Zählerstände
Zählerstände	Zählerstände	Zählerstände	Lastschaltgerät-Nr.	MeteringCode	MeteringCode	Metering Code	Zählervorschübe	Lastgangdaten
Zähler-Nr.	Zähler-Nr.	Zähler-Nr.	Steuerdaten				Lastgangsummen	MeteringCode
Zähler-Typ	Zähler-Typ	Zähler-Typ					MeteringCode	Adressdaten
	MeteringCode	MeteringCode					Adressdaten	Rechnungsdaten
		Adressdaten					keine LG-Daten!	

Prozess-schritt	Anforderung an Datenschutz							
Daten Erhebung	Daten Auslesung	Plausibilisierung Validierung Abrechnung Zuordnung Mappingt-Tabelle	Netzsteuerung Voraussetzung: Schaltung über Gruppen	Bilanzmanagement Abrechnung	Bilanzmanagement	Profiling	Verrechnung	Visualisierung
pseudonymisierte Daten (über Zähler-Nr.)	pseudonymisierte Daten (über Zähler -Nr.)	nicht pseudonymisierte Daten	anonymisierte Daten	pseudonymisierte Daten (über MC)	pseudonymisierte Daten (über MC)	nicht pseudonymisierte Daten	nicht pseudonymisierte Daten	nicht pseudonymisierte Daten
personenbezogene Daten	personenbezogene Daten	personenbezogene Daten	nicht personenbezogene Daten	personenbezogene Daten	personenbezogene Daten	personenbezogene Daten	personenbezogene Daten	personenbezogene Daten
				kein Zugriff auf Mapping-Tabelle	kein Zugriff auf Mapping-Tabelle	Einverständnis Kunde vorausgesetzt	keine Lastgänge im Billing-System	

Abbildung 9 Beispielhafte Übersicht von Datenschutzanforderungen für Daten aus Netzbetrieb und Grundversorgung

11. Anhang Data Governance - Verzeichnis der Bearbeitungstätigkeiten

(1) Eine Vorlage für ein Verzeichnis der Bearbeitungstätigkeiten (VDB) kann folgendermassen aufgebaut sein. Sie entspricht den minimalen Anforderungen gemäss DSG Art. 12 und umfasst ebenfalls Daten im Rahmen der Auftragsdatenbearbeitung. Die Teile 1/3 bis 3/3 bilden eine zusammenhängende Tabelle.

Verzeichnis der Bearbeitungstätigkeiten des Verantwortlichen

Name und Anschrift Verantwortlicher	Gesetzlicher Vertreter (= Geschäftsführung)	Vertreter in der EU (Art. 27 Abs. 1 i.V.m. Art. 3 Abs. 2 DSGVO)		Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten) des Datenschutzbeauftragten

Nr.	Bezeichnung der Bearbeitungstätigkeit	Verantwortlicher Fachbereich	EU Personen-daten beinhaltend	Name des Verantwortlichen	Ort der Bearbeitung	Zwecke der Bearbeitungen

Datum:
Unterschrift:

Tabelle 6 Vorlage für Verzeichnis der Bearbeitungstätigkeiten – Teil 1/3

Zuständige Aufsichtsbehörde	Regelungen zur Datensicherheit	Regelungen zur Datenlöschung
EDÖB ...	Weisung Informationssicherheit ...	

Kategorie betroffener Personen	Kategorie personenbezogener Daten	Kategorien von Empfängern

Tabelle 7 Vorlage für Verzeichnis der Bearbeitungstätigkeiten – Teil 2/3

Sachverhalte zu Drittstaatenübermittlungen	ev. Joint Controller
Data Transfer Agreement ...	

Datenübermittlungen in Drittländer		Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien	Allgemeine Beschreibung der technischen und organisatorischen Massnahmen (TOMs)
Übermittlung	Namen der Drittländer		

Tabelle 8 Vorlage für Verzeichnis der Bearbeitungstätigkeiten – Teil 3/3

(2) Nachfolgend finden sich Erklärungen und Hinweise zu den in der VDB verwendeten Kategorien:

Details → Kategorie ↓	**Mögliche Ausprägungen**	**Mögliche Fragestellungen**	**Bemerkungen**
Vertreter in der EU			Für den Fall, dass Daten im EU-Raum gesammelt und/oder bearbeitet werden.
Bezeichnung der Bearbeitungstätigkeit	Metering, HRM, Marketing	Welche Daten werden bearbeitet? Wo werden Daten bearbeitet? Zu welchem Zweck werden Daten bearbeitet?	Generische Kategorisierungen sind möglich, jedoch keine "Pauschalisierungen"
Kategorien von Bearbeitungen vgl. Kapitel 3 (3)			
Verantwortliche Rechtseinheit oder Fachbereich			
EU Personendaten beinhaltend	Ja / nein		ggfs. Relevanz für Entscheid Anwendbarkeit EU-DSGVO
Name des Verantwortlichen	Name Vorname		
Ort der Bearbeitung	Territorium & Anbieter	Wo stehen bspw. die Server? Werden Cloud-basierte Services genutzt?	Relevanz für Entscheid Anwendbarkeit DSG oder EU-DSGVO

Details → Kategorie ↓	Mögliche Ausprägungen	Mögliche Fragestellungen	Bemerkungen
Zwecke der Bearbeitungen	Produktion, Personalmanagement, …	Begründung, warum Daten bearbeitet werden	Wichtig, da diese die sog. Zweckbindung definieren
Kategorie betroffener Personen	Mitarbeitende, Kunden, Bewerber, Interessenten, …		
Kategorie personenbezogener Daten	Personendaten, besonders schützenswerte Personendaten, Profiling	Welche Inhalte werden bearbeitet und wie?	Ableitung des erforderlichen Schutzes resp. Relevanz für Schutz (bei Profiling)
Kategorien von Empfängern (öffentlich, intern, extern)	Dritte, Behörden, …	Wem werden Daten weitergegeben?	Bspw. Information in AGB, Verträgen
Datenübermittlungen in Drittländer oder internationale Organisationen / woher	Deutschland, …	Wohin resp. an wen im Ausland und ggf. welches Land werden Daten übermittelt?	Prüfung der Angemessenheit gemäss Liste EDÖB
Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien	Mögliche Fristen: 12 Monate 5 Jahre 10 Jahre Spezialfristen	Wie lange müssen / sollen bestimmte Daten aufbewahrt werden bis zur Löschung?	Löschung kann verlangt werden resp. die Löschung hat gesetzlich zu erfolgen. Dies bedingt Anpassungen in der Informatik.

Beschreibung der technischen und organisatorischen Massnahmen (TOM)

Die TOMs sind zentraler Teil der Dokumentation zum Datenschutz und sind wesentlich für das VDB, die Auftragsbearbeitung und die entsprechenden Verträge, sowie für Informations- und Transparenzpflichten. Sie können insbesondere folgende Bereiche umfassen:

1. **Pseudonymisierung**
   Vorgang, bei dem persönliche Daten durch z.B. Zahlenfolgen ersetzt werden, so dass diese nicht mehr zuordenbar sind. Siehe Beispiel Messpunkt in Kapitel 3 Definitionen.
2. **Verschlüsselung**
   Schutz der Daten vor unberechtigtem Zugang und Zugriff z.B. Datenübertragung.
3. **Gewährleistung der Vertraulichkeit**
   Regelung über Zutritt und Zugang, Art wie gewährleistet wird, dass nur Berechtigte Zugang zu Räumen, Servern usw. haben.
4. **Gewährleistung der Integrität**
   Verfahren zur Sicherstellung, dass bearbeitete Daten richtig, unverfälscht und echt sind. Steuerung von Änderungen, Löschungen usw.
5. **Gewährleistung der Verfügbarkeit**
   Massnahmen, die sicherstellen, dass z.B. bei einem Stromausfall die Verfügbarkeit der Daten, Systeme usw. gegeben ist.

Beschreibung der technischen und organisatorischen Massnahmen (TOM)
6. **Gewährleistung der Belastbarkeit der Systeme** Summe der Massnahmen zur Sicherstellung, dass Systeme gegen Unfälle, Eindringlinge oder sonstige angemessen geschützt sind.
7. **Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall** Massnahmen und Techniken, welche sicherstellen, dass in einem Schadensfall Daten, Systeme usw. wieder verfügbar sind (inkl. richtigem Inhalt).
8. **Verfahren regelmässiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen** Wie wird vorgegangen, um die getroffenen Massnahmen regelmässig zu prüfen, anzupassen, zu erneuern ...
9. **Schriftliche Dokumentation von sonstigen Massnahmen** Schulungen von Mitarbeitenden, Regelungen und Weisungen, Zertifizierungen, usw.

Tabelle 9 Kategorien, Erklärungen und Hinweise zum Verzeichnis der Bearbeitungstätigkeiten

(3) Diese Basisversion kann im Sinne eines ICT-Repository mit weiteren Tabellen ergänzt werden. Bspw. durch Tabellen, die Systeme, Sicherheitsaspekte, Zugriffsberechtigungen, Auskunftsberechtigungen usw. abbilden.

12. Anhang FAQ DSGVO

Diese FAQ's stellen Grundsätze dar, welche jedoch nicht als verbindliche Rechtsauskunft zu verstehen sind. In Einzelfällen oder gewissen Konstellationen sind erhebliche Abweichungen möglich.

Frage 1: Ist die DSGVO anwendbar, wenn Mitarbeitende aus dem Home-Office im Ausland Daten des EVU's bearbeiten, unabhängig davon, ob die Daten auf einem Server beim EVU, einem Rechenzentrum in der Schweiz, in der EU oder lokal (auf dem Endgerät) bearbeitet werden?

Antwort 1:
Im Grundsatz ist auch der Zugriff und die Einsichtnahme auf Daten eine Datenbearbeitung, wodurch sich streng rechtlich für diesen Prozess eine Anwendbarkeit der DSGVO ergibt.

Frage 2: Ist die DSGVO anwendbar, wenn ich einen in der EU angesiedelten Dienstleister für bspw. Support Dienstleistungen nutze und der Datenzugriff aus der EU erfolgt?

Antwort 2: Im Grundsatz ist auch der Zugriff und die Einsichtnahme auf Daten eine Datenbearbeitung, wodurch sich streng rechtlich für diesen Prozess eine Anwendbarkeit der DSGVO ergibt.

Frage 3: Ist die DSGVO anwendbar, wenn Daten des EVU's bei einem Data Center Anbieter in der EU gespeichert werden?

Antwort 3: Im Grundsatz ist auch die Speicherung von Daten eine Datenbearbeitung, wodurch sich streng rechtlich für diesen Prozess eine Anwendbarkeit der DSGVO ergibt.

Frage 4: Ist die DSGVO anwendbar, wenn ich Strom an Endkunden auf Schweizerischem Territorium liefere (bspw. Ferienwohnung oder -haus) und der Kunde stammt aus der EU?

Antwort 4: Nein, die Daten stammen von Personen aus der Schweiz oder unter einem Vertragsverhältnis unter Schweizer Recht.

Frage 5: Ist die DSGVO anwendbar, wenn Personen aus der EU meinen Onlineshop oder meine Homepage in der Schweiz nutzen?

Antwort 5: Grundsätzlich nein. Abweichungen sind möglich, speziell wenn diese bspw. von nachfolgenden Faktoren abhängen: wird eine Domain-Name Endung verwendet, welche nicht .ch ist, werden Sprachen verwendet, welche nicht zu den Landessprachen gehören (inkl. Englisch), können Preise auch in € umgerechnet werden oder werden direkt in € angezeigt.

Frage 6: Ist die DSGVO anwendbar, wenn ein EVU aktiv Daten von Personen aus der EU sammelt (bspw. Web-Site Crawling) oder einen Wettbewerb mit der Zielgruppe Personen aus der EU durchführt?

Antwort 6: Ja, hier werden gezielt Daten von Personen aus der EU bearbeitet resp. gesammelt. Der Hauptzweck ist nicht die Erfüllung einer vertraglichen Verpflichtung, sondern die gezielte Erhebung von Daten (Marktortprinzip). Der Ort der Bearbeitung wird dadurch irrelevant.

Frage 7: Ist die DSGVO anwendbar, wenn sich in meinem Newsletter-Versand (digital oder physisch) auch vereinzelte Personen mit Wohnort in der EU befinden?

Antwort 7: Grundsätzlich nein. Es gilt die Annahme, dass die Personendaten von der entsprechenden Person selbst erfasst wurden und bei der Erhebung die Information und Transparenz gegeben war. Weiter zielt die Aktivität mit dem Newsletter und der Inhalt NICHT primär auf Personen oder sonstige Bezüge zur EU ab und stellt somit eine geringfügige Menge an Newsletter-Kunden dar.

Frage 8: Wenn eine bestimmte Datenbearbeitung unter der DSGVO erfolgt, müssen dann alle anderen Datenbearbeitungen auch DSGVO konform erfolgen?

Antwort 8: Nein. Die spezifische Datenbearbeitung ist unter Einhaltung der DSGVO durchzuführen, was jedoch nicht zu einer Unterstellung aller Prozesse des gesamten EVU führt.

Frage 9: Wenn ein EVU entweder die DSGVO oder das DSG Schweiz einhält, ist dann automatisch die jeweils andere Gesetzgebung mit abgedeckt?

Antwort 9: Nein. Obwohl die beiden Datenschutzgesetzgebungen sehr ähnlich sind, weisen sie in einigen Bereichen auch Unterschiede auf.

Frage 10: Ist das EVU der DSGVO unterstellt, wenn Waren und/oder Dienstleistungen aus der EU bezogen resp. beansprucht werden?

Antwort 10: Nein. Beim Bezug von Waren und Dienstleistungen steht üblicherweise nicht die Datenbearbeitung im Zentrum, es sei denn, Daten und Informationen selbst stellen die Waren und Dienstleistungen dar (bspw. Einkauf von Adressdaten von Personen aus der EU). Der Kauf von physischen Gegenständen (bspw. Kopierpapier) in der EU stellt somit keine Unterstellung unter die DSGVO dar.

13. Leitfaden zu den wichtigsten Umsetzungspunkten der Data Policy

Nachfolgend werden stichwortartig die wichtigsten Aspekte und Vorschläge zur Umsetzung der Data Policy festgehalten:

(1) Allgemeine Vorbereitungen

- ✓ Ressourcenplanung für die Umsetzung
  - Die Umsetzung der unternehmensweiten Data Policy ist ein Projekt, welches mehrere Jahre dauert
  - die entsprechenden Ressourcen sind bereit zu stellen
- ✓ Kulturänderung
  - Ein Bewusstsein über die Wichtigkeit des Themas in der Unternehmung ist erforderlich.
  - Chefsache: Der Veränderungsprozess ist von der Geschäftsführung / Unternehmensleitung zu initiieren und aktiv mitzutragen
  - Die Verantwortung der Umsetzung ist nicht an die Mitarbeitenden delegierbar
- ✓ Im Klaren sein, was der Unterschied zwischen Datenschutz und Datensicherheit ist (Kapitel 7.1 und 7.2)
  - Datenschutz und Datensicherheit werden durch die Digitalisierung im Unternehmen immer wichtiger und können nicht voneinander getrennt betrachtet werden

(2) Rechtliche Grundlagen (Kapitel 5)

- ✓ Sicherstellung der Einhaltung der Vorgaben StromVG
  - informatorisches Unbundling gemäss StromVG Art. 10 Abs. 2 (Kapitel 6.1)
  - Massnahmen zur Abgrenzung von Netzbetrieb und übrigen Organisationseinheiten (insb. Energieverkauf) implementiert?
  - Abschottung des Informationszugangs für MA innerhalb des VNBs gewährleistet?
- ✓ StromVV Art. 8d
  - Profile
  - 15 Min Messintervall
  - Pseudonymisierung
  - Zustimmung
  - Kantonale Bestimmungen (klären, ob ggf. kantonale Bestimmungen strengere Vorgaben machen als jene des Bundes)
- ✓ Untersteht das Unternehmen dem DSG und/oder der DSGVO?
  - Eine Orientierungshilfe findet sich im Anhang FAQ DSGVO der Data Policy

(3) Umsetzung Data Nutzung und Data Compliance

- ✓ Datenschutzanalyse durchführen (Kapitel 7.1)
  - Need-to-know Prinzip (Kapitel 3 (6))
  - Verzeichnis der Datenbearbeitungstätigkeiten erstellen (Kapitel 8.3 und Anhang Data Governance - Verzeichnis der Bearbeitungstätigkeiten)
    - Prozessmodelle mit einbeziehen, wenn vorhanden (siehe VSE Bericht Data-Policy)
    - Lebenszyklus der Daten (Kapitel 4)
    - Es ist unerheblich, ob die Daten in digitaler oder physischer Form vorliegen
  - personenbezogene Daten identifizieren
  - weitere kritische Unternehmensdaten identifizieren (unterliegen dem Geschäftsgeheimnis, GIS-Daten, SCADA-Daten…, Kapitel 7.5)
- ✓ Datensicherheit: Risikoanalyse durchführen (Kapitel 7.2)

- Vertraulichkeit: Welche Daten darf ich nach aussen geben?
- Integrität: Kann ich sicherstellen, dass die Daten korrekt sind?
- Verfügbarkeit: Habe ich die Daten dann verfügbar, wenn ich sie benötige?
- Authentifizierung: Ist sichergestellt, dass die Identität eines Benutzers gegenüber einem System nachgewiesen ist?
- Autorisierung: Wer darf im Unternehmen welche Daten sehen?
- Nachverfolgung: Ist sichergestellt, dass Änderungen an Daten nachvollziehbar bleiben?

✓ Einbezug von Dritten (Kapitel 6.4)
- Auslagerung an Service-Anbieter
- Nutzung von Cloud-Services (z.B. Office 365)
- Eine Auslagerung an Dritte entbindet das EVU nicht von der Verantwortung

✓ Schutzbedarf der Daten festlegen (Kapitel 7.6)
- auf Basis des Verzeichnisses der Datenbearbeitungstätigkeiten
- Daten für Dokumentation der Anlagen und Verträge im EVU

✓ Massnahmen aus Datenschutz-/Risikoanalysen umsetzen (Anhang, Beschreibung TOM)
- technische und organisatorische Massnahmen zur Risikominimierung einleiten
- die Umsetzung der TOM wird mehrere Jahre in Anspruch nehmen

✓ Zustimmung der Kunden, falls eine weitergehende Datenverarbeitung durchgeführt wird, z.B. (Kapitel 6.2, 6.3):
- Datenauflösung kleiner als 15 Minuten
- Datenauslesung der Feldgeräte häufiger als 1x pro Tag
- Echtzeitdatenauslesung
- Visualisierung 15 Minuten Daten in einem Kundenportal
- Datenweitergabe an Dritte

✓ Daten Löschung (Kapitel 7.3)
- Recht auf vergessen
- nach 12 Monaten, wenn nicht für Abrechnung verwendet
- nach 5 Jahren, wenn für Abrechnung verwendet
- nach 10 Jahren die eigentliche Rechnung an die Kunden
- für weiterführende Anwendung Einstimmung der Kunden einholen
- welche Daten müssen anonymisiert werden?
- Archivierung: Sicherstellen, dass Daten auch im Archiv/Backup gelöscht werden

(4) Umsetzung Data Governance (Kapitel 8)

✓ Rollen / Funktionen (Kapitel 8.2)
- Gesamtverantwortung liegt bei der Unternehmensführung
- Datenschutzberater (DPC, Data Protection Consultant) Leitfaden
  - regelmässige und systematische Prüfung von strommarktrelevanten Regularien und Gesetzen, insbesondere DSG, DSVGO, Übergangsfristen, Umgang mit Daten von juristischen Personen
- Mitarbeiter haften bei einer Datenschutzverletzung persönlich gemäss DSG
- Chef Informationssicherheit (CISO; Chief Information Security Officer)
- Sicherheits-Chef (CSO, Chief Security Officer)
- Compliance Officer (CO)
- Die Rollen können bestehenden Mitarbeitenden zugewiesen werden, auch Mehrfachzuweisungen oder Auslagerung an Dritte sind möglich. Einschränkung: Eine Rolle darf sich nicht selbst kontrollieren

✓ periodische Schulung aller Mitarbeitenden (Awareness der Mitarbeitenden)

✓ Ansprechstelle definieren für Meldungen von Datenschutz- und Datensicherheitsvorfällen

14. Glossar

Abkürzung	Beschreibung
AAA	Authentication / Authorization / Accounting
AG	Arbeitsgruppe
AGB	Allgemeine Geschäftsbedingungen
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
CRM	Customer-Relationship-Management
CO	Compliance Officer
CSO	Chief Security Officer
DB	Datenbank
DPC (früher DPO)	Data Protection Consultant / Datenschutz-Berater gemäss Art. 10 DSG (früher Data Protection Officer genannt)
DSG	Bundesgesetz über den Datenschutz
EDM	Energiedatenmanagement
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EnG	Energiegesetz
EnV	Energieverordnung
ERP	Enterprise-Resource-Planning
EU	Europäische Union
EU DS-GVO	Datenschutz-Grundverordnung der Europäischen Union (nachfolgend: DSGVO)
EVU	Energieversorgungsunternehmen
GeBüV	Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (Geschäftsbücherverordnung)
GIS	Geoinformationssystem
HES	Head-End-System
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
iMG	intelligentes Messgerät
iMS	intelligentes Messsystem. Betrifft die ganze Messkette ab iMG (Smart Meter) bis Head End System unabhängig der Übermittlungstechnologie durch Datenkonzentrator oder Gateway.
ISO	International Organisation for Standardisation
IT	Informationstechnologie / Information Technology
LeV	Leitungsverordnung
MDM	Meter Data Management
OT	Operational Technology
SCADA	Supervisory Control and Data Acquisition
StromVG	Stromversorgungsgesetz
StromVV	Stromversorgungsverordnung

Abkürzung	Beschreibung
TOM	Technische und organisatorische Massnahmen
VDB	Verzeichnis der Bearbeitungstätigkeiten
VGSD	Verordnung zum Bundesgesetz über den Datenschutz
VNB	Verteilnetzbetreiber
VSE	Verband Schweizerischer Elektrizitätsunternehmen
ZFA	Zählerfernauslesung