



DSGVO und neues DSG – Auswirkungen auf die Schweiz und die Energiebranche



Fachtagung Data Policy – Herausforderung «Daten-Policy für die Energiebranche»
Olten, 15. November 2018

Thomas Steiner

Dr. iur., LL.M., Rechtsanwalt, VISCHER AG



Inhalt

- I. Einleitung
- II. DSGVO: Neuerungen, Mythen und Bedeutung für Schweizer Unternehmen
- III. Nutzung von Daten aus intelligenten Mess-, Steuer- oder Regelsystemen: Dreistufiger Rechtsrahmen
- IV. Stand der Datenschutzrevision in der Schweiz
- V. Auswirkungen für die Datennutzung in der Energiebranche: Gestärktes Vertrauen und mehr Privatsphäre oder innovationshemmende Bürokratie?



Rückblick: Sechs Monate DSGVO – Viel Verunsicherung, einige Verfahren, kein Weltuntergang



Sechs Monate DSGVO: Viel Verunsicherung, einige Verfahren – kein Weltuntergang

- Verunsicherung aufgrund von Mythen und Missverständnissen
- Ärgernis zu Beginn: E-Mail-Flut und Klick-Plage (aufgrund von Missverständnissen)
- Abmahnungswelle: Bisher ausgeblieben
- Erste Beschwerden von Konsumentenverbänden (Max Schrems mit Verein «Noyb») gegen Facebook, Instagram, WhatsApp, Google
- Leitlinien von Aufsichtsbehörden – nicht immer klärend
- Immerhin: Datennutzung, Datenschutz, Datensicherheit und Daten-Policy als Top-Themen auf Chefetagen

- Treiber der Datenschutzreformen (EU und Schweiz):
Angst vor Kontrollverlust bei Big Data Analytics

- Daten als Rohstoff für digitale Geschäftsmodelle – auch in der Energiebranche
- Big Data und Data Analytics auf dem Vormarsch
- Migration von Daten in die «Cloud»
- Wachsende Risiken für die Datensicherheit
- Algorithmen übernehmen Selektionen und führen automatisierte Entscheide aus

- Daten aus intelligenten Mess-,
Steuer- oder Regelsystemen

● (Personen-) Daten aus intelligenten Systemen

Personendaten

Konkrete Person ist aufgrund der Angaben **identifiziert** oder indirekt (in Kombination mit anderen Angaben) **identifizierbar**



Pseudonyme Daten

Re-Identifizierung – je nach Kontext sowie Zugriffsmöglichkeiten und -rechten des Interessenten – möglich: Abgleich mit separat gespeicherten, besonders vor unberechtigtem Zugriff geschützten Zusatzinformationen («Schlüssel»)



Pseudonymisierung ist v.a. eine Datensicherheits- und Datenminimierungsmassnahme

Anonyme Daten

Re-Identifizierung wäre nur mit **aussergewöhnlich hohem Aufwand** möglich, den kein (motivierter) Interessent vernünftigerweise auf sich nehmen würde – **Datenschutzrecht nicht anwendbar**



● Personendaten / Identifizierbarkeit



- Art. 4(1) DSGVO / Art. 4 Bst. a E-DSG: **Identifizierbarkeit**
- Messdaten aus intelligenten Systemen sind Personendaten, wenn der Kunde (Vertragspartner/natürliche Person) durch **Zuordnung** der Messdaten an eine Kundennummer, Hausnummer, Smart Meter-Gerätenummer oder andere Merkmale **und Abgleich mit** verfügbaren oder einem Interessenten vernünftigerweise zugänglichen **Referenzdaten** (z.B. Datenbank mit Name des Vertragspartners) **identifizierbar** ist*
- Es reicht nicht jede rein theoretische Möglichkeit der (Re-) Identifizierung; berücksichtigt werden Mittel, die der Verantwortliche oder ein (motivierter) Dritter **vernünftigerweise** («wahrscheinlich», «*reasonably likely*») zur Identifizierung **nutzen würde***

* vgl. Art. 4(1) und Erw. 26 DSGVO / Botschaft-BR zu Art. 4 Bst. a E-DSG; BBl 2017 6941, S. 7019.

● Anonymisierungsmethoden und Lösungsansätze



- Anonymisierungsmethoden (Auswahl)
 - **Masking**: Löschung identifizierender Informationen (z.B. Name und Vorname, Adresse, E-Mail, Telefonnummer, Kundennummer, Smart Meter-Gerätenummer)
 - **Randomization**: Vertauschung von Merkmalen und Zuordnung identifizierender Merkmale zu unterschiedlichen Gruppen unter Verwendung von Zufallsmechanismen
 - **Datenaggregation / Generalisierung**: Identifizierende Angaben so generalisieren, dass jede Person denselben Durchschnittswert einer Gruppe von Personen hat – z.B. zur Veränderung der Granularität des Datensatzes (Regionen statt Ortschaften, Altersgruppen statt Jahrgänge)
- Anonymisierung von Daten aus intelligenten Systemen: Lösungsansätze
 - Technisch anspruchsvoller: **Splitting** an der Quelle/**nahe am Datenpunkt** («edge») → **originär zwei separate Datensätze** (einmal mit anonymen Daten – einmal mit identifizierenden Merkmalen)
 - Rechtlich anspruchsvoller: **Kopie** des Datensatzes erstellen – **Datensatz anonymisieren**

● Dreistufiger Rechtsrahmen für den Umgang mit Daten aus intelligenten Mess-, Steuer- oder Regelsystemen

● Dreistufiger Rechtsrahmen

- I. Bundesgesetz über den Datenschutz (DSG)
 - Art. 17c Abs. 1 StromVG: **Einheitliche Unterstellung unter das DSG** für Datenverarbeitungen «im Zusammenhang mit intelligenten Mess-, Steuer- oder Regelsystemen»
 - Zweck der Bestimmung (möglichst einheitliche Voraussetzungen für die Entwicklung digitaler Geschäftsmodelle) spricht für **weite Auslegung** von «im Zusammenhang mit»
- II. Spezialbestimmungen für eng definierte Anwendungsbereiche (StromVV)
 - **Erlaubnistatbestände** für die Bearbeitung von (Personen-) Daten aus intelligenten Systemen
 - **Einschränkungen für die Bearbeitung und Weitergabe** von (Personen-) Daten aus intelligenten Systemen
 - **Nicht optimal auf DSG abgestimmt** (Einwilligung ist gemäss DSG nur in Ausnahmefällen notwendig – insbes. für die *Bekanntgabe* von Personendaten durch Bundesorgane; bei der Bearbeitung durch Private insbes. für die *Bekanntgabe besonders schützenswerter Personendaten*)*
 - Spezialbestimmungen zur Datensicherheit
- III. Kantonales Datenschutzrecht

* vgl. Stefan Rechsteiner/Thomas Steiner, Datenschutz bei intelligenten Mess- und Steuersystemen, in: Jusletter 11. Juni 2018, Kap. IV.3.

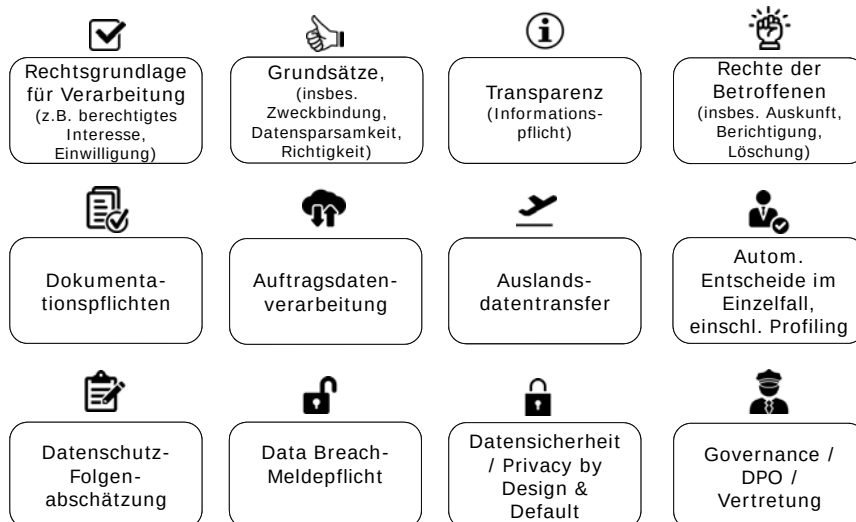
● DSGVO, neues DSG und die Energiebranche

● Und die Bedeutung der DSGVO? –
Kaum Anwendungsfälle für Schweizer
Elektrizitätsunternehmen

● Datenschutz in der EU: Die wichtigsten Neuerungen

- Stärkung der **Betroffenenrechte** (insb. Informations-, Auskunfts-, Berichtigungs-, Löschungs- und Widerspruchsrechte; Recht auf **Datenübertragbarkeit**)
- Höhere Anforderungen an die **Transparenz** (Informationspflicht bei der Beschaffung von Personendaten)
- Höhere Anforderungen an die Gültigkeit von **Einwilligungen**
- *Privacy by Design & Default* / **Datenschutzfolgenabschätzung**
- Fokus **Datensicherheit**; Meldepflichten bei *Data Breach*
- Erweiterte **Dokumentationspflichten** (und Rechenschaftspflichten)
- **Sanktionsdrohung** (künftige Unterlassung oder Einschränkung der Datenverarbeitung; Geldbussen bis EUR 20 Mio. oder, wenn höher, bis 4% des weltweiten Jahresumsatzes)

● Die DSGVO im Überblick





Relevanz der DSGVO für Schweizer Unternehmen

- Anwendung der DSGVO auf **Verarbeitungen personenbezogener Daten** durch Schweizer Unternehmen, die
 - Individuen, die sich **in der EU** befinden, (entgeltlich oder unentgeltlich) Produkte oder Dienstleistungen **anbieten** (erkennbare Ausrichtung auf den EU-Endkundenmarkt; sog. **Marktortsprinzip**); oder
 - das **in der EU stattfindende Verhalten** von Individuen **beobachten (Auswirkungsprinzip)**; z.B. Online-Tracking; anschliessendem Profiling mit Rechtswirkung oder ähnlichen Auswirkungen für Betroffene)
- Unabhängig von DSGVO-Anwendungsfällen:
 - Erwartungen von Kunden deren Datenverarbeitungen der DSGVO unterstehen
 - Vertrauen der Kunden und Mitarbeiter in Datenmanagement des Unternehmens stärken
 - Anpassung an absehbare Angleichung des DSG an die DSGVO



Klarstellung von Missverständnissen zur Anwendbarkeit auf Datenverarbeitungen von Schweizer Unternehmen

- EU-Bürgerschaft irrelevant für Anwendbarkeit der DSGVO
- Nicht die Lieferung bzw. Dienstleistungserbringung, sondern das **Angebot** von Waren oder Dienstleistungen an Individuen in der EU begründet die Anwendbarkeit der DSGVO (erkennbare Ausrichtung auf den EU-Endkundenmarkt; sog. **Marktortsprinzip**)
- Verhaltensbeobachtung begründet nur bei spürbaren und vorhersehbaren **Auswirkungen** die Anwendbarkeit der DSGVO (**Auswirkungsprinzip**; z.B. Online-Tracking mit anschliessendem Profiling und Rechtswirkung oder ähnlichen Auswirkungen für Betroffene)
- Anwendbarkeit der DSGVO nicht auf Unternehmen, sondern auf konkrete **Datenverarbeitungen**
- Grenzüberschreitendes Outsourcing (Schweiz–EU oder EU–Schweiz) alleine begründet nicht die Anwendbarkeit der DSGVO
- Klarstellung weiterer Missverständnisse: <http://blog.vischer.com/de/die-dsgvo-und-die-schweiz-10-mythen-und-missverstandnisse>



Stand der Datenschutzrevision in der Schweiz



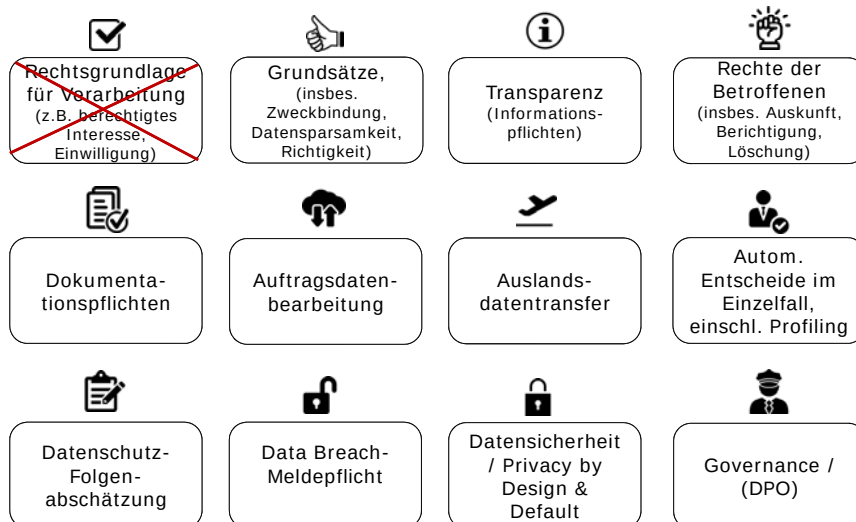
Datenschutzrevision in der Schweiz

- 15.09.2017: Totalrevision DSG – Entwurf des Bundesrates
- Sommersession 2018: NR beschliesst **Revision in Etappen** und beschliesst **Schengen-Datenschutzgesetz** (SDSG); SR stimmt in der Herbstsession 2018 zu
- SDSG gilt nur für Bearbeitung von Personendaten durch Bundesorgane bei **der Schengener Zusammenarbeit in der Strafverfolgung**
- **Totalrevision des DSG** – weitere Sitzungen der SPK-NR; Behandlung im NR auf Frühjahrssession 2019 verschoben; danach SPK-SR und SR; Inkrafttreten nicht vor 2020
- **Annäherung an den DSGVO-Standard**; «Swiss Finish» weitgehend vermieden
- Kantonale Datenschutzgesetze werden auch revidiert

● Totalrevidiertes DSG: Die wichtigsten Neuerungen

- Verzicht auf Schutz von juristischen Personen
- Stärkung der **Betroffenenrechte** (insb. Informations-, Auskunfts-, Berichtigungs-, Lösungs- und Widerspruchsrechte; aber voraussichtlich kein Recht auf Datenübertragbarkeit)
- Höhere Anforderungen an die **Transparenz** (Informationspflicht bei der Beschaffung von Personendaten)
- *Privacy by Design & Default* / **Datenschutzfolgenabschätzung**
- Fokus **Datensicherheit**; Meldepflichten bei *Data Breach*
- Erweiterte **Dokumentationspflichten** (und Rechenschaftspflichten)
- EDÖB erhält Verfügungskompetenz
- **Strafbarkeit natürlicher Personen** (bei Vorsatz; subsidiäre Strafbarkeit des Unternehmens) – keine Verwaltungssanktionen

● E-DSG im Überblick



● Wichtige Umsetzungsmassnahmen im Unternehmen

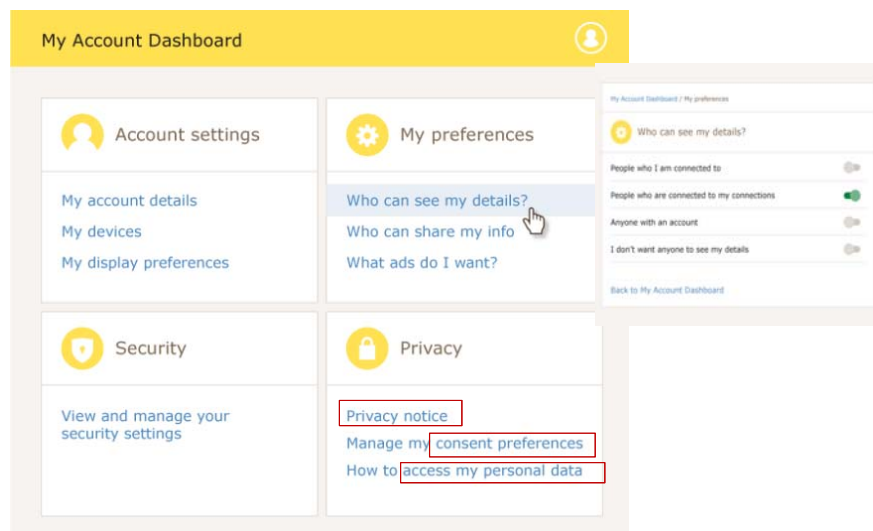
- Analyse und Dokumentation der Verarbeitungstätigkeiten (Verzeichnis / Dateninventar)
- Aussenaufttritt anpassen
 - **Informationspflicht:** Datenschutzerklärungen
 - Verträge mit Kunden (AGB)
 - **Kontrollmöglichkeiten / Betroffenenrechte** (Opt-out ausserhalb von Art. 8d StromVV) gewähren, z.B. in **Privacy Center**
 - Verträge mit externen Dienstleistern und Partnern (Verantwortlicher–Verantwortlicher / Verantwortlicher–Auftragsbearbeiter)
- Interne Richtlinien und Prozesse anpassen/implementieren
 - **Betroffenenrechte:** Verfahren betreffend Umgang mit Auskunfts-, Berichtigungs- und Löschungsbegehren
 - **Datensicherheit:** Verfahren betreffend Erkennung, Meldung und Untersuchung eines *Data Breach*; Datensicherheitskonzept
 - Richtlinie für Datenschutzfolgenabschätzung
 - **Datenschutz-Organisation:** Rollen, Zuständigkeit und Verantwortung im Unternehmen regeln (interne Datenschutzrichtlinie)

● Informationspflicht und Kontrollrechte: Privacy Center als möglicher Lösungsansatz

● Transparenz (Informationspflicht bei der Beschaffung von Personendaten)

- Art. 17 Abs. 2–4 E-DSG: Informationen, die **zur Geltendmachung der Rechte nach DSG notwendig sind und eine transparente Datenbearbeitung gewährleisten**, mindestens:
 - wer für die Bearbeitung verantwortlich ist und wie ihn die Betroffenen kontaktieren können (z.B. über Privacy Center)
 - die Bearbeitungszwecke
 - Empfänger oder Kategorien von Empfängern, denen die Personendaten bekanntgegeben werden
 - Kategorien der bearbeiteten Personendaten (wenn nicht direkt beim Betroffenen erhoben)
 - Bei Auslandsbekanntgabe: Angabe des Staates (und Garantien für die Auslandsübermittlung)
- Weitere ... (vgl. dazu als Gold-Standard: Art. 13 und 14 DSGVO)

● Privacy Center: Datenschutzerklärung, Einwilligungs-Präferenzen und Auskunftsrecht





Auswirkungen für die Datennutzung in der Energiebranche: Gestärktes Vertrauen und mehr Privatsphäre oder innovationshemmende Bürokratie?



Auswirkungen für die Datennutzung

- Positiv:
 - **Sensibilisierung der Nutzer**
 - Transparenz und Kontrollrechte: **Vertrauen in Datennutzung und neue digitale Geschäftsmodelle**
 - Datenschutz bei Produkte-Design berücksichtigen
 - Datennutzung, Datenschutz, Datensicherheit und Daten-Policy als Top-Themen auf Chefetagen
- Negativ:
 - **Allumfassendes Datenschutzrecht statt Fokus auf risikobehaftete Bearbeitungen**
 - Nutzer sind überfordert mit Informationsfülle und Optionen («Privacy Paradox»)
 - Fehlende Abstimmung mit Vorschriften zur informationellen Entflechtung gemäss Art. 10 Abs. 2 StromVG (Einschränkung der Nutzung und Weitergabe von «wirtschaftlich sensible[n] Informationen»)*
- Ambivalent: Erlaubnistatbestände in StromVV
 - Innovationsfördernde (oder hemmende?) Erlaubnistatbestände
 - **Nicht optimal auf DSGVO abgestimmt***

* vgl. Stefan Rechsteiner/Thomas Steiner, Datenschutz bei intelligenten Mess- und Steuersystemen, in: Jusletter 11. Juni 2018, Kap. IV.3 und V.

● Ihr Kontakt bei VISCHER



Thomas Steiner

Dr. iur., LL.M., Rechtsanwalt

Leiter des Praxisteam Data & Privacy

tsteiner@vischer.com

+41 58 211 34 76



Stefan Rechsteiner

Dr. iur., Rechtsanwalt

Partner, Leiter der Praxisteam

Regulatory und Energierecht

srechsteiner@vischer.com

+41 58 211 34 81

VISCHER



Herzlichen
Dank.

Zürich

Schützengasse 1
CH-8021 Zürich
Tel +41 58 211 34 00
Fax +41 58 211 34 10

Basel

Aeschenvorstadt 4
CH-4010 Basel
Tel +41 58 211 33 00
Fax +41 58 211 33 10