
PRESLMAYR
RECHTSANWÄLTE

PRESLMAYR
RECHTSANWÄLTE

Datenschutz und Datensicherheit für „kleine“ Elektrizitätsunternehmen

Dr. Gerald Trieb, LL.M.

Rechtsanwalt und Partner
Preslmayr Rechtsanwälte Wien

Vollversammlung der Vereinigung Österreichischer Elektrizitätswerke, Wörgl, 20.5.2016

TAGLaw

Worum geht es bei Datenschutz und Datensicherheit?

PRESLMAYR RECHTSANWÄLTE

- **Grundrecht auf Datenschutz ist in Österreich und in Europa verankert → Es geht daher um den Schutz personenbezogener Informationen (=Daten) vor unbefugter Verwendung!**
- Personenbezogene Daten sind alle Informationen, die einer bestimmten oder bestimmbaren natürlichen (und derzeit auch: juristischen Person = Unternehmen) zuordenbar sind; mehr als nur persönliche Informationen!
- Daten, die besonderen Schutz genießen: sensible Daten und strafrechtsbezogene Daten;
- Datensicherheit (organisatorische Rahmenbedingungen im Fokus: Verpflichtung zur vertrauliche Behandlung, Schutz vor unbefugtem Zugang, Schutz vor Missbrauch, etc.)
- Wahrung der Betroffenenrechte (Recht auf Auskunft, Recht auf Löschung, etc.)
- Wahrung von Informations- , Melde- bzw. Genehmigungspflichten sowie sonstiger regulatorischer Anforderungen (Transparenz der Verarbeitung, Datenverarbeitungsregister, Datenschutzverträge)

Rechtsquellen des Datenschutzrechts

- **Europa:**
  - DERZEIT: Datenschutzrichtlinie aus 1995 – Umsetzung in nationalen Mitgliedstaaten erforderlich;
  - **AB 25.5.2018: DATENSCHUTZGRUNDVERORDNUNG (DSGVO) → Gilt unmittelbar in allen Mitgliedsstaaten**
  - **Text abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.DEU**
- **Österreich:**
  - DERZEIT:
    - Datenschutzgesetz 2000 – „DSG 2000“ (Umsetzung der EU-Richtlinie)
    - Verordnungen (Standard und Musteranwendungen-Verordnung, Datenverarbeitungsregister-Verordnung)
  - **AB 25.5.2018: direkte Anwendbarkeit der DSGVO in allen Mitgliedstaaten, aber nationale Ausführungsgesetze weiter erforderlich und möglich → DSG 2000 wird reformiert erhalten bleiben!**

Wechsel der Rechtsnormen - Auswirkungen

PRESLMAYR RECHTSANWÄLTE

Rechtsnormen bis 2018

Europarecht

Datenschutz-Richtlinie 1995/46/EG

Verpflichtung Österreichs zur Umsetzung der EU-Richtlinie in nationales Recht

Nationales Recht

DSG 2000

Unternehmen/Organisationen/Vereine

Rechtsnormen ab 2018

Datenschutz-Grundverordnung (EU) 2016/679

EU-Verordnung ist unmittelbar in Österreich anwendbar

Nationales „DSG-neu“

Unternehmen/Organisationen/Vereine

Grundrecht auf Datenschutz

- § 1 Abs 1 Satz 1 DSG 2000:

„Jeder hat, insbesondere im Hinblick auf die Achtung des Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht.“

- Ausnahmen in § 1 Abs 1 Satz 2 DSG: Daten sind
  - öffentlich („allgemeine Verfügbarkeit“) oder
  - anonym (Rückführbarkeit auf Person ist nicht mehr möglich!)
- **Daher: Jede Art der Datenverarbeitung ist grundsätzlich verboten!**
- **Außer es liegt eine Ausnahme vor → Rechtsgrundlage!**
- „Alles, was nicht ausdrücklich verboten ist, ist erlaubt!“ ist im Datenschutzrecht nicht zutreffend!

Rechtsgrundlagen (§ 8f. DSG 2000, Art 6, 9 DSGVO)

PRESLMAYR RECHTSANWÄLTE

- Weitere Ausnahmen vom Grundrecht = Rechtsgrundlagen für die zulässige Verwendung von Daten (am Beispiel von Smart Meter):
  - Verwendung steht im lebenswichtigen Interesse des Betroffenen;
  - Zustimmung des Betroffenen liegt vor (Auslesung und Übermittlung von Viertelstundenwerten);
  - Gesetzliche Verpflichtung oder Ermächtigung liegt vor (Speicherung von Messwerten im Zähler, Auslesung der Tagesverbrauchswerte zur Darstellung im Web-Portal und zur Übermittlung an den Lieferanten);
  - berechtigte Interessen des Auftraggebers überwiegen (Rechtsverfolgung und Rechtsverteidigung, Achtung: nicht bei Smart Meter Daten – Beweisverwertungsverbot!!!);
  - Verwendung ist zur Vertragserfüllung mit dem Betroffenen erforderlich oder für eine Anbahnung zum Vertragsabschluss (tageszeitabhängige Verrechnung im Liefervertrag vereinbart → Übermittlung von Viertelstundenwerten zulässig);

Grundsätze der Verwendung (§ 6 DSG 2000/ Art 5 DSGVO)

P) **Daten dürfen nur verwendet werden**

- nach **Treu und Glauben** und auf rechtmäßige Weise;
- für **festgelegte, eindeutige und rechtmäßige Zwecke**; keine Weiterverwendung der Daten in mit diesen Zwecken unvereinbarer Weise (**Zweckbindungsgrundsatz**);
- soweit für den Zweck der Datenanwendung **wesentlich**;
- so sie sachlich **richtig** sind und auf dem aktuellen Stand gehalten werden (Ausnahme: „historische“ Daten) und
- solange sie in personenbezogener Form zur Erreichung des Zwecks, für den sie ermittelt wurden, erforderlich sind; sie sind daher zumindest sobald wie möglich zu anonymisieren, sonst zu löschen. **(Speicherbegrenzung)**!
- NEU nach DSGVO: **Integrität und Vertraulichkeit** (Datensicherheit) und **Rechenschaftspflicht** → **DOKUMENTATION!!!**

Vom DSG 2000 zur DSGVO

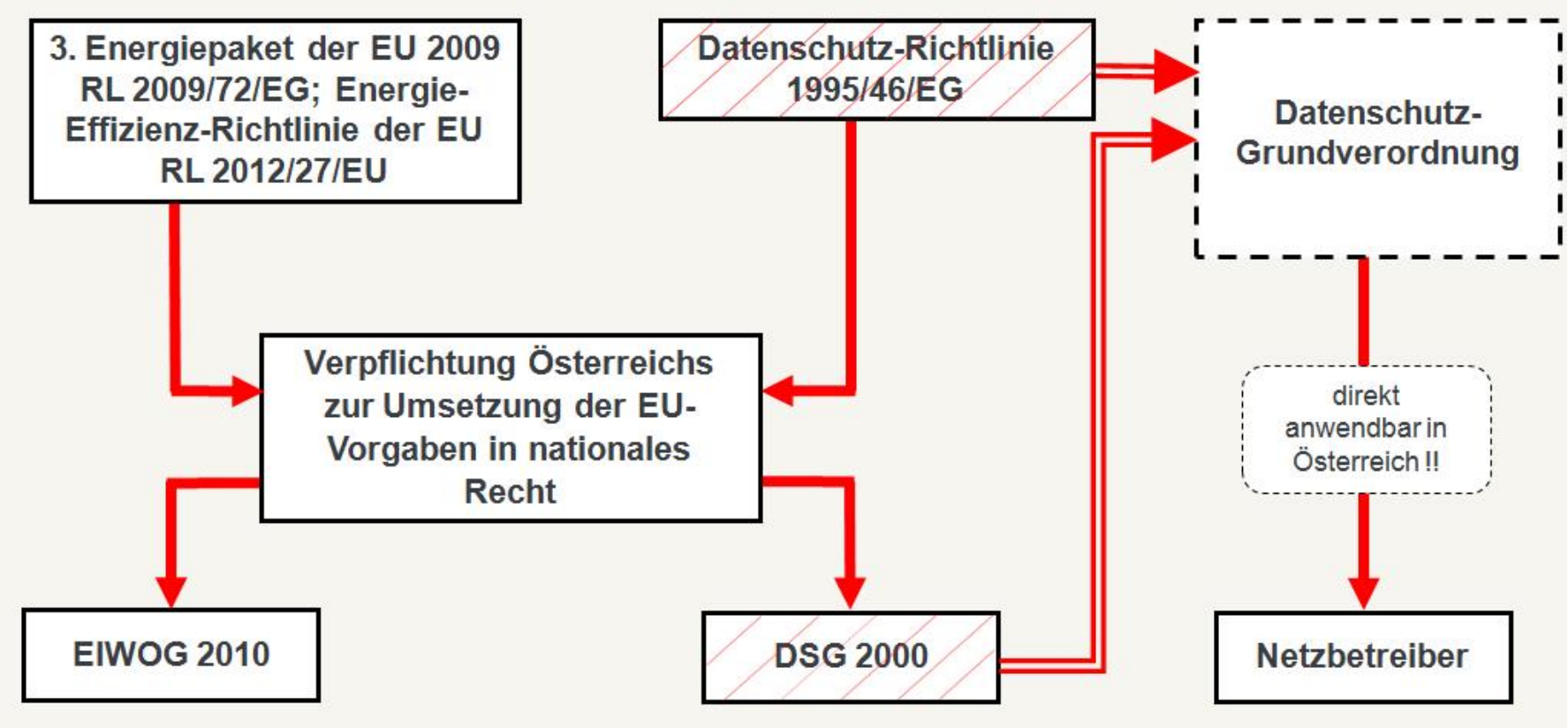
- Regulierung → **Selbstverantwortung**
  - Weitgehender Entfall von Melde- und Genehmigungspflichten
  - Verzeichnis von Verfahrenstätigkeiten
  - Datenschutz-Folgenabschätzung
- Behauptung → **Nachweis und Dokumentation**
  - Rechenschaftspflicht (Umkehr der Beweislast)
  - Höhere Anforderungen an Verträge mit Dienstleistern
- Best Practice → absolutes Must
  - Festschreibung bereits anzuwendender Grundsätze in der Verodnung (zB.: privacy by design and by default)
  - **Strafen:**
    - vom „Kavaliersdelikt“ zur finanziellen Bedrohung für das gesamte Unternehmen
    - Heute: max. EUR 25.000,00
    - **DSGVO: max. EUR 20 Mio oder 4 % vom globalen Umsatz**

Fit bis 2018:
10-Punkte-Fahrplan für die Datenschutz-Reform

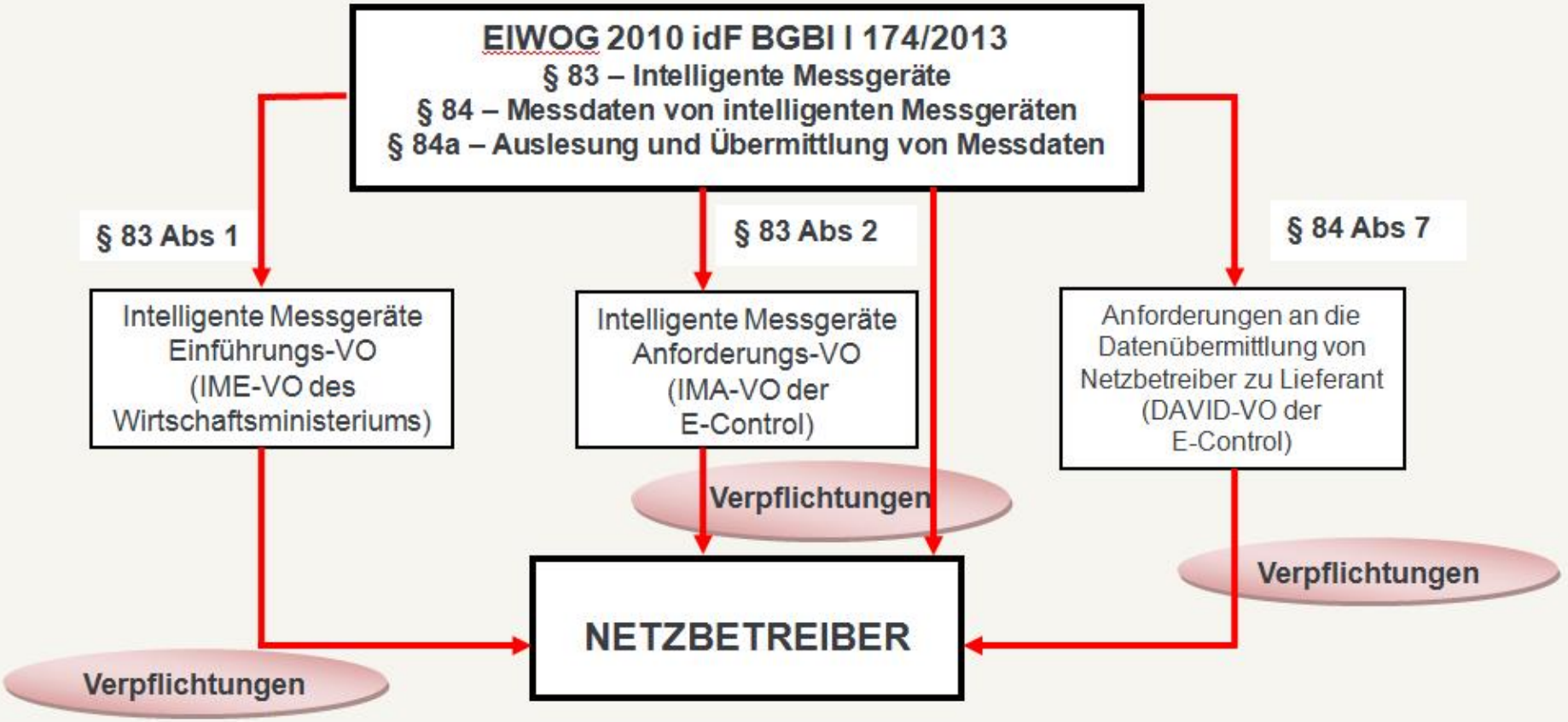
PRESLMAYR RECHTSANWÄLTE

1. **Projektverantwortlichen / Datenschutzbeauftragten bestellen, Projektstart**
   - Prüfen ob DSB nötig und wenn möglich diesen umgehend damit betrauen oder einbinden; interne/externe Mitwirkende definieren, Projektumfang, Budget und Zeithorizont definieren.
2. **Verfahrensverzeichnis / internationaler Datenverkehr**
   - Status Quo der Verarbeitungstätigkeiten/Datenanwendungen erheben und eine Dokumentation erstellen; Datensicherheitsmaßnahmen prüfen; Internationalen Datenverkehr „abarbeiten".
3. **Informationspflicht; Zustimmung; Grundprinzipien und Rechtsgrundlagen**
   - Erfüllung der Infopflichten vorbereiten; Zustimmungen prüfen; Grundprinzipien und Rechtsgrundlagen pro Anwendung prüfen.
4. **Betroffenenrechte**
   - Auskunftsrecht, Löschungsrecht, Datenportabilität, Verständigungspflichten. Sicherstellen, dass allen Betroffenenrechten zeitgerecht und ordnungsgemäß entsprochen werden kann.
5. **Dienstleister – Verträge**
   - Dienstleister identifizieren, Dienstleisterverträge abschließen bzw. überprüfen.
6. **Policies**
   - IT-Policies überarbeiten; eventuell auch Vorliegen von Betriebsvereinbarungen prüfen
7. **Datenmissbrauch – data breach notification duty!**
   - Organisation darauf vorbereiten unverzüglich Behörde und Betroffene über Datenschutzverletzungen informieren zu können. Musterschreiben; Notfallkontakte; Ernstfall üben.
8. **Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen**
   - Anwendbarkeit prüfen; technische und organisatorische Maßnahmen umsetzen
9. **Datenschutz-Folgenabschätzung**
   - Prüfen, ob erforderlich; wenn ja, durchführen. Eventuell ist eine Konsultation Aufsichtsbehörde notwendig.
10. **Schulung**
    - Schulung der Belegschaft in allen Ebenen und Geschäftsbereichen zur Awarenessbildung und Prävention unbedingt erforderlich!

Maßgeblich: Energiewirtschaftsrecht und Datenschutzrecht

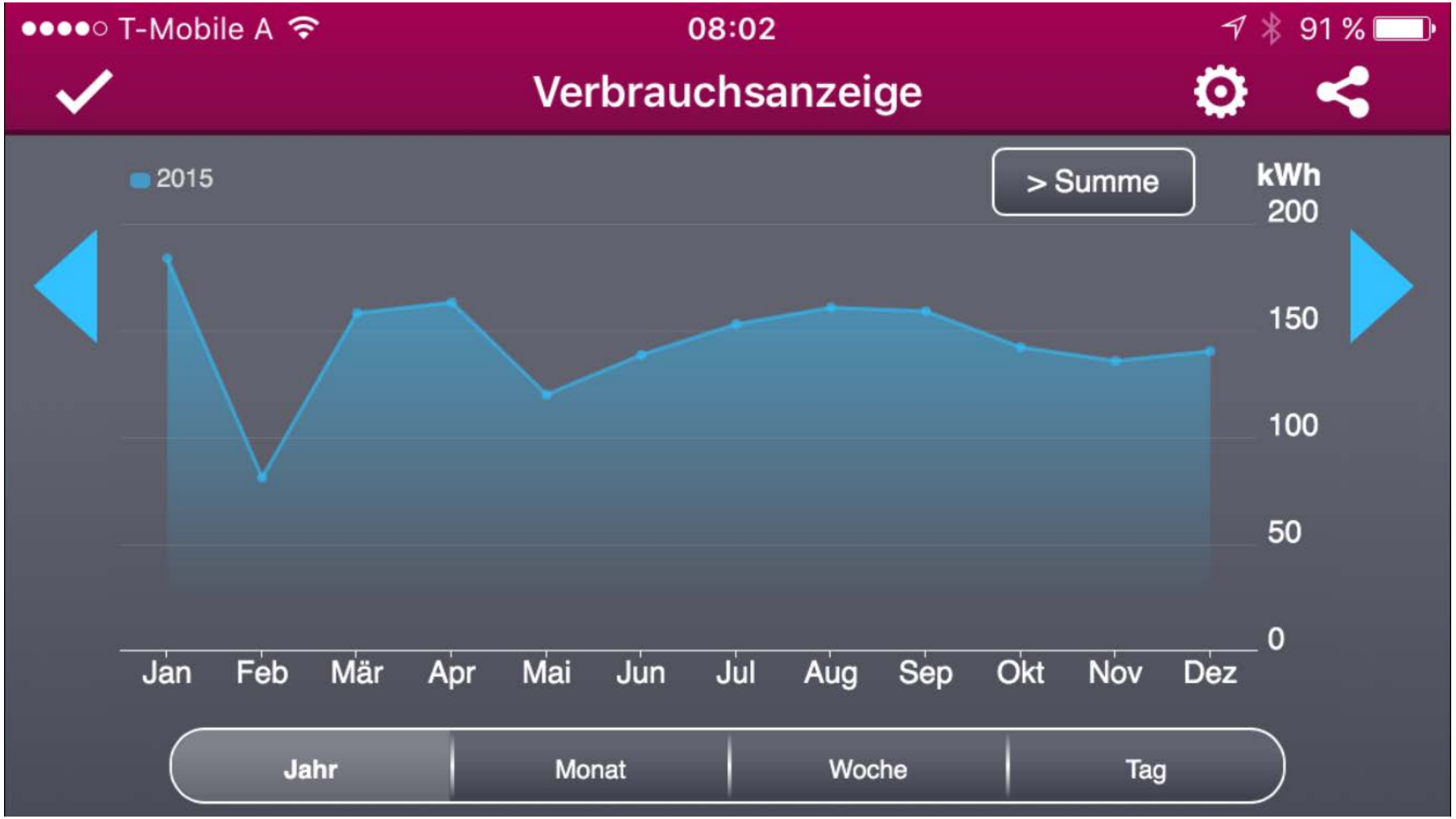


Umsetzung in Österreich im Energiewirtschaftsrecht



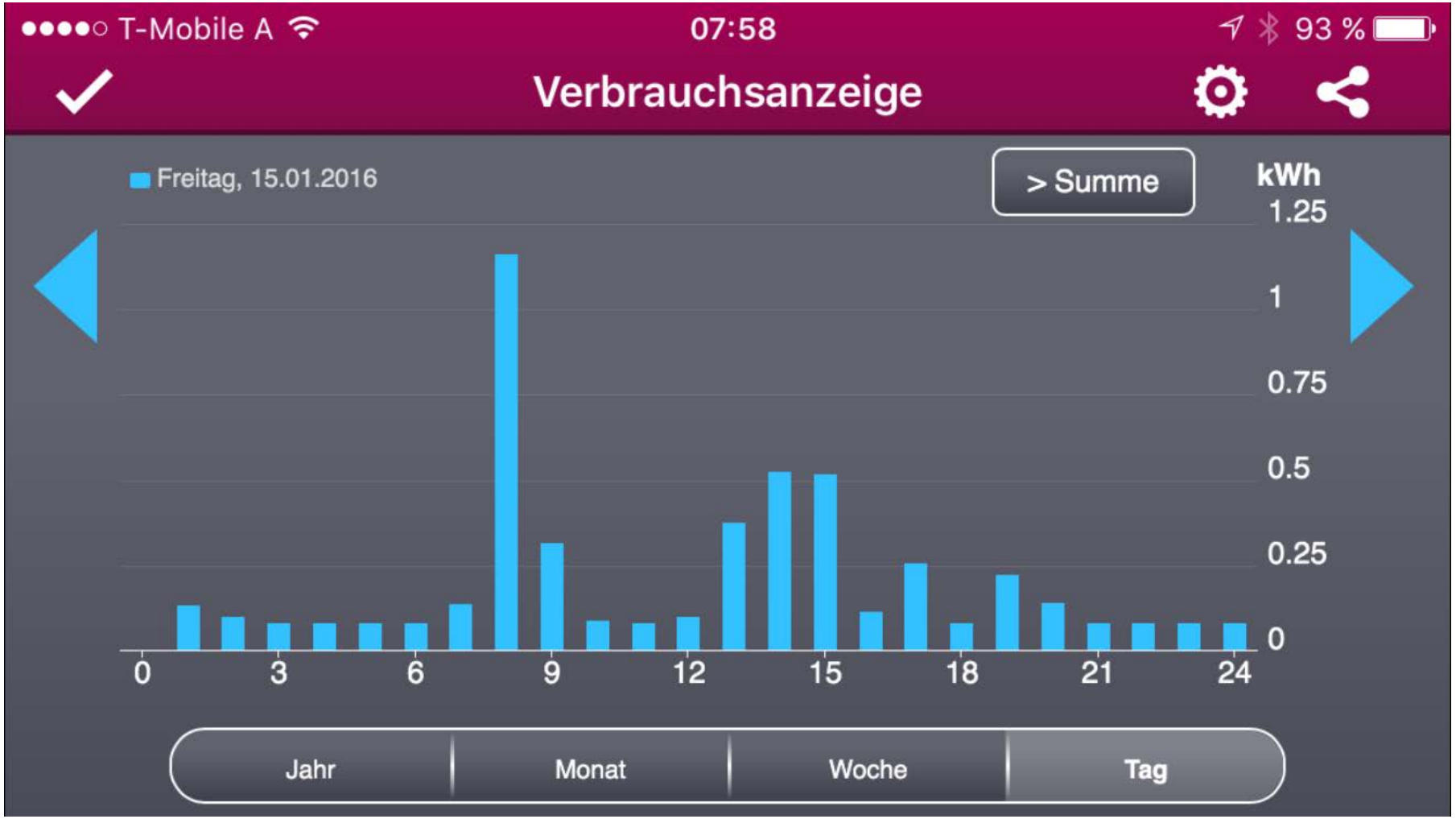
- „Herkömmlicher“ Ferraris-Zähler liefert keine Information darüber, zu welcher Tages- oder Jahreszeit wie viel Strom an einem bestimmten Zählpunkt verbraucht wird; Jahresstromverbrauch ist personenbezogenes Datum, aber nicht „heikel“;
- **Anders: Smart Meter-Daten = sehr „heikle“ Daten!**
  - Verbrauchserfassung alle 15 Minuten und Erfassung eines Tagesverbrauchswerts; Speicherung für 60 Tage im Zähler;
  - Tägliche Auslesung der Tagesverbrauchswerte zur Darstellung im Web-Portal und zur monatlichen Übermittlung an den Lieferanten (Information);
  - Auslesung von Viertelstundenwerten nur bei Zustimmung oder vertraglicher Erforderlichkeit;
  - Übermittlung an Lieferanten nur bei Zustimmung oder vertraglicher Erforderlichkeit;
  - Entsprechung von Betroffenenrechten – es sind alle vorhandenen Daten zu beauskunften ;
  - Sicherer Zugang zu Web-Portal muss sichergestellt werden;
  - Durchführung von Datenschutz-Folgenabschätzung.

Detaillierte Stromverbrauchsinformation



Detaillierte Stromverbrauchsinformation

Detaillierte Stromverbrauchsinformation



PRESLMAYR RECHTSANWÄLTE

Datenverarbeitung in Österreich → Grundsatz der Meldepflicht im DVR

Meldung vor Aufnahme der Verarbeitung an DSB erforderlich!

Vollbetrieb ab Meldung zulässig, außer es werden sensible Daten (z.B. Gesundheitsdaten), oder Daten über die Kreditwürdigkeit verarbeitet – Vollbetrieb erst nach Vorabkontrolle durch DSB ab Registrierung im DVR zulässig!

Keine Meldepflicht, wenn zB:

- Nur indirekt personenbezogene Daten
- Nur veröffentlichte Daten
- Persönliche/familiäre Tätigkeiten
- Publizistische Tätigkeit
- Standardanwendung (STMVO)

Entfall mit Anwendbarkeit von DSGVO sehr wahrscheinlich, Aber Durchführung ist eine Vorbereitung auf die DSGVO (Verfahrensverzeichnis, Datenschutzfolgenabschätzung);

P) **Beispiele für meldepflichtige Datenanwendungen:**

- Smart Metering;
- Lieferantenwechsel;
- Videoüberwachung (z.B. Überwachung eines Gebäudes wegen Einbruchs- und/oder Sachbeschädigungsgefahr)
  - Nur wenn verhältnismäßig, d.h. keine anderen Maßnahmen für Zweckerreichung ausreichend (zB.: Wachdienst, Kontrollfahrten), möglichst wenig Kameras, möglichst wenig öffentlicher Raum im Bild
  - Nur zum Schutz des überwachten Objekts
  - Besondere Kennzeichnungspflicht
  - **Vorabkontrollpflichtig**, d.h. keine Inbetriebnahme ohne Genehmigung der DSB zulässig (strafrechtsrelevante Daten!);

- Energieeffizienzmaßnahmen gemäß § § 10, 27 Energieeffizienzgesetz (EEffG), § 17 EEffG-Richtlinienverordnung;

  → Dokumentation von gesetzten bzw. initiierten Energieeffizienz-Maßnahmen und Weiterleitung dieser Maßnahmen an die nationale Energieeffizienz-Monitoringstelle.

Datensicherheit gemäß § 14 DSG

- **Aufgabenverteilung** bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ist ausdrücklich festzulegen,
- die Verwendung von Daten ist an das Vorliegen **gültiger Aufträge** der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
- jeder **Mitarbeiter** ist über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu **belehren**,
- **Zutrittsberechtigung** zu den Räumlichkeiten des Auftraggebers oder Dienstleisters ist zu regeln,
- **Zugriffsberechtigung** auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte ist zu regeln,
- **Berechtigung zum Betrieb der Datenverarbeitungsgeräte** ist festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
- **Protokollführung**, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,
- **Dokumentation** über die nach Z 1 bis 7 getroffenen Maßnahmen führen, um die Kontrolle und Beweissicherung zu erleichtern.
- Berücksichtigung des Standes der Technik erforderlich, aber Kosten/Nutzen-Abwägung unter Berücksichtigung des Risikos zulässig!

Datensicherheit - Art 32 DSGVO

PRESLMAYR RECHTSANWÄLTE

- Keine starren Vorgaben!
- Bewegliches System je nach
  - Vorhandensein technischer und organisatorischer Mittel;
  - Art der Verarbeitung;
  - Ergebnis der Prognoseentscheidung über die Gefährlichkeit einer Datenoffenlegung der Daten für Betroffenen;
- Geeignete Maßnahmen
  - Technisch / Privacy by Design
    - Pseudonymisierung (Artikel 4 Abs 3b) und
    - Verschlüsselung der Daten;
  - Sicherstellung der Systemintegrität (ISO27001 Zertifizierung, COBIT, ITIL, ITSM)
- Test der Maßnahmen erforderlich;
- Nachweis über die Einhaltung
  - Genehmigte Verhaltensregeln;
  - Zertifizierung, dass DSGVO eingehalten ist.
- Strafrahmen bei Nichteinhaltung: EUR 10 Mio oder 2 % des globalen Umsatzes;

NIS-RL - Ziele

- **Richtlinie zur Gewährleistung einer hohen gemeinsamen Netz - und Informationssicherheit in der Union**

- Ziele:
  - EU-weit soll ein **hohes Niveau an Netzwerk- und Informationssicherheit** erreicht werden durch;
  - (1) Stärkung der **Zusammenarbeit zwischen den MS und eine strategische Koordination und**
  - (2) die Verpflichtung zur Einführung eines angemessenen **IT-Risikomanagements** und der **Meldung signifikanter Störfälle;**

- **(1) Betreiber wesentlicher Dienste**
  - **Öffentliche oder private Einrichtung;**
  - aus dem Bereich **Energie,** Transport, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser und digitale Infrastrukturen (zB Internet Exchange Points).
  - **Anhang II:** Sektor Energie - Teilsektor Elektrizität:
    - Elektrizitätsunternehmen, die die Funktion "Versorgung" im Sinne des wahrnehmen ;
    - Verteilernetzbetreiber;
    - Übertragungsnetzbetreiber.

- **Kriterien:**
  - Dienst ist wesentlich für die **Aufrechterhaltung kritischer sozialer oder wirtschaftlicher Aktivitäten (Liste);**
  - Dieser Dienst hängt von **Netzwerk- und Informationssystemen ab;**
  - Ein **Störfall hätte signifikante Auswirkungen auf die weitere** Verfügbarkeit dieses Dienstes.

NIS-RL III – Verpflichtungen

- **Pflicht angemessene technische und organisatorische Sicherheitsmaßnahmen zur Risikobewältigung zu** ergreifen

  - **Betreiber wesentlicher Dienste: NIS-Behörde kann**
    - **die** Einhaltung der Sicherheitsanforderungen **jederzeit mittels Audits prüfen;**
    - **Belege für die Umsetzung** der Sicherheitsmaßnahmen **verlangen;**
    - **Verbindliche Anweisungen** zur Abhilfe der festgestellten Mängel erteilen.

- **Pflicht zur Meldung von Störfällen, die gröbere** Auswirkungen auf die **Aufrechterhaltung des Dienstes** haben.

NIS-RL IV – Zeitplan

- Annahme des Textes im EU-Ministerrat am 21.4.2016

  abrufbar unter: http://data.consilium.europa.eu/doc/document/ST-5581-2016-INIT/en/pdf

  Eine deutsche Fassung noch nicht verfügbar;

- Voraussichtliches In-Krafttreten im August 2016

- 21 Monate Zeit für Mitgliedstaaten zur Umsetzung in nationale Rechtsvorschriften

PRESLMAYR
RECHTSANWÄLTE

Vielen Dank für die Aufmerksamkeit!

Fragen?

Kontakt

Dr. Gerald Trieb, LL.M.
Preslmayr Rechtsanwälte OG
Universitätsring 12
1010 Wien

E-Mail: trieb@preslmayr.at
Telefon: +43/1/5331695
Web: www.preslmayr.at

TAGLaw