PRESLMAYR
RECHTSANWÄLTE

Privacy Targeted Contract Stipulations in Public Tenders as a Practical Solution for Local DSOs

Dr. Gerald Trieb, LL.M.

Attorney at Law and Partner
Preslmayr Attorneys at Law, Vienna

Presentation at the European Utility Week 2015, Vienna, November 4, 2015

References in Smart Metering

2009 - Assessment of the "permissibility of the use of smart meter-data under data protection law" on behalf of Association of Austrian Electricity Industry before the introduction of the "new" Austrian Energy Act (ElWOG):

since then continuous consultancy in their project groups, e.g. for the development of

–a draft law for a novelty of the "smart meter"- regulations in the ElWOG (before its amendment in 2013) or

–a pattern for a notification regarding the processing of smart meter-data to the Austrian Data Protection Authority (DPA).

Continuous consultancy for different network operators with the conception and implementation of smart metering-pilot projects from a privacy point of view (including their notification with the DPA),:

–Preparation of the Roll-out and

–implementation of privacy targeted contract stipulations in tender documents for the procurement of smart meter – components

Continuous participation in national and international expert committee's:

- Task Force „Smart Grids" of the European Commission since 2010;
- Expert's committee in the Ministry of Economy to discuss specific issues for the implementation of Smart Metering in summer/autumn 2012;
- Platform "Smart Sustainable Infrastructures" at the Austrian Standards Institute since spring 2012.

Continuous lecturing activities and publications:

- Steering Committee "Grids" and symposium "Smart Metering" of the Association of Austrian Electricity Industry;
- Compliance with new electricity meters, Wirtschaftsblatt, 17.12.2010;
- Smart Metering under EU-Data Protection Law, International Data Privacy Law, 2011, 121;
- Smart Metering NEW, ecolex 12/2013;
- Smart Metering - New guidelines from Europe through the upcoming data protection law; Oesterreichs Energie, June 2015
- Privacy targeted contract stipulations in public tenders for Smart Metering–components, Oesterreichs Energie, (October 2015).

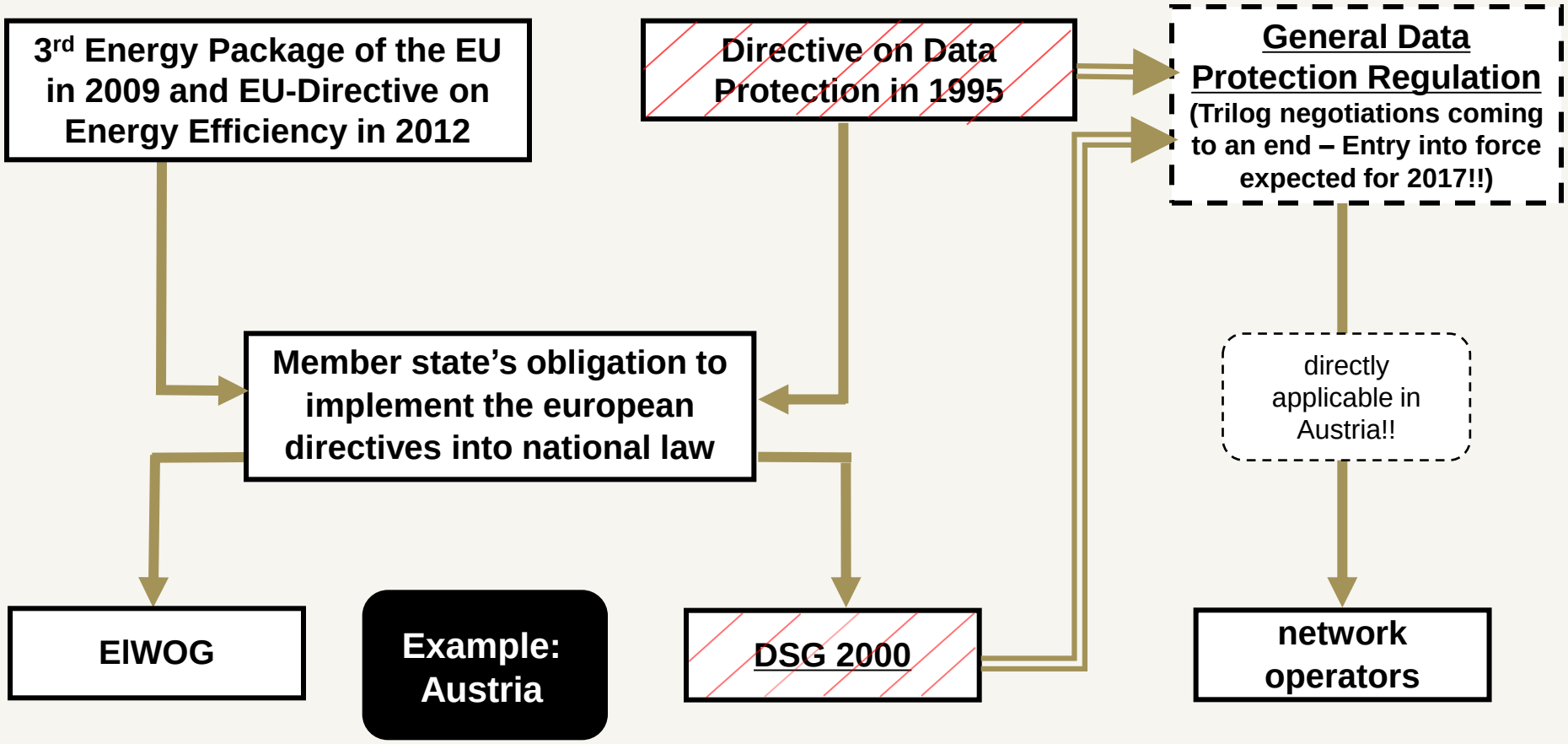
PRESLMAYR RECHTSANWÄLTE

What is this lecture about?

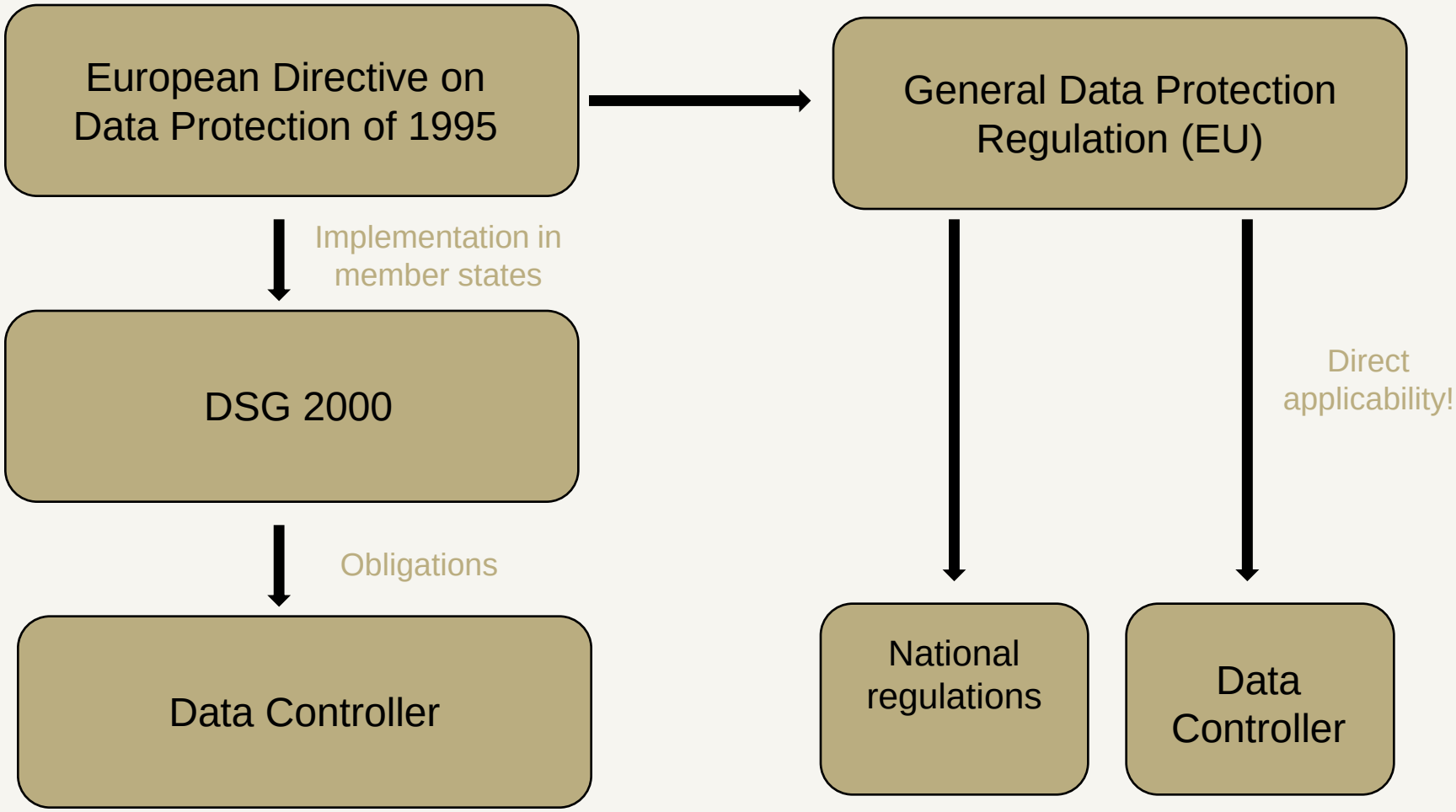
- **Data protection law – current status and future developments**
- **Data protection requirements for smart metering under European Union Law**
  - Organizational requirements
  - Data security requirements
  - Protection of data subject's rights
- **Implementation of such requirements in tender conditions**
- **Procurement procedures already started or even completed without privacy targeted stipulations - what can you (still) do?**

Legal framework for the implementation and operation of smart meters in Austria

Energy law and data protection law



Details on European and national Data Protection Law – now and in the future



The network operator is the major player – Consequences for data protection law!!!

The network operator is according to ElWOG and DSG 2000;

- responsible for the roll-out of smart meters;
- installer and operator of smart meters;
- "first" processor of the meter data;
- Addressee of data subject's rights;

Example: Austria

A network operator can be the controller according to data protection law and, as a consequence, responsible for compliance with obligations under data protection law in the source of the operation of smart meters and the use of personal data processed!

<u>Attention:</u> Obligations under data protection law concern <u>every user of data</u>, whether data usage is for own or for a third party's purpose (e.g. supplier, service provider)!

Sanctions for non-compliance – possibilities of minimization

National data protection laws (current status)

- **Administrative penalties comparatively low**
- **Data Protection Authorities are generally not very active**
- **Common other risks are:**
  - compensation (for damages),
  - claims or injunctions for omission under competition law (more likely for energy suppliers and service providers)

EU-General Data Protection Regulation

- The penalty range will increase drastically! Maximum penalties of several million EUR, or of a certain percentage (between 2 and 5%) of the group-wide sales, whichever is higher!
- Draft of the European Parliament (accepted by a large majority!): **Penalties of up to EUR 100 million or 5 % of the group-wide sales!**
- In addition, new obligations for controllers will be implemented for "complex" or “large" data applications (for example „Data Protection Impact Assessment“ (DPA), Privacy and Security Certification duties, Data Protection Supervisor (?))
- Compliance with obligations may mitigate awarded sactions; compliance measures must be considered when calculating the penalty in case of breach!

Data protection requirements – current status (Directive 95/46/EG)

Organizational and legal requirements regarding data security:

- Obligatory for data controllers and data processors (for example for operators of a „Meter Data Management Systems“)!
- Regulated in Art 17 para 2 ff.: commission of service providers and definition of their obligations and data security methods;
- **Duty to ensure proper and lawful use of data** (Art. 17 para 2 ff.) → Written contract also recommended with domestic service providers (if not mandated by law)!

Implementation in the tender documents as the basis for the procurement contract necessary!!!

Obligations of service providers

Central Statement: Use of data exclusively for the purpose of providing the commissioned services! Prohibition to use data for own purposes! (Art.17 para 3)

Example: Austria

- Observe data security measures (Art. 17 para 3);
- Employees have to be bound to treat data confidential (Art. 16);
- **Subcontracting with other service providers only with the permission of the controller;**
- **Conditions for compliance with data subject's rights (right to access, rectification and deletion) by the controllers must be given;**
- **Destroying data after the end of the contract, returning or keeping the data by order of the controller (for a given period);**
- **Provide every information to the controller necessary to control observance of these obligations by the service provider.**

Data security measures I

The aim is to protect data from accidental or unlawful destruction and loss;

- Addressed in **Art. 17;**
- Duty to ensure that data are used properly and not accessible to unauthorized persons;
  → a clear and secure authorization-concept is required in the company:
  Which employees need access to which data!

Methods must be taken in consideration of the state of the art and economic viability (!)

Data security measures II

§ 14 DSG 2000:

- **Explicit definition of the division of responsibilities in the use of data between organizational units and employees;**
- **Employees must be bound to the existence of valid instructions of authorized organizational units;**

Example: Austria

- Privacy training sessions for employees;
- Regulation of the admission authorization to the rooms of controllers or service providers as well as the access authorization on data, programs and the protection of the data carriers before the examination and use by unauthorized persons;
- Control of data usage by detailed access protocols for tracking purposes;
- Documentation of implemented security measures.

Data subject's rights (Art 12)

Data are processed in

- Smart meter (depending on local laws; in Austria: consumption is recorded in a 15-minutes-intervall without user's consent for a period 60 days!!!);
- Meter Data Management System (MDMS).

Obligation for data controller to

- Grant the data subjects the right of access to the data (information on the attributes processed, the purposes, the sources as well as any recipients of the data), respectively to have these data rectified or deleted (Art. 12);
- Have objections to data usage respected (Art. 14).

Problems in big companies:

- Which data are stored about the data subject?
- Where are they collected from?
- To whom are they transmitted?
- Who had access (internally or externally) to the data (tracking details of possible exports)?

Implementation in tender conditions I

Meter Data Management System (MDMS):

Recommendation: Implementation of data protection requirements as “must criteria” in tender conditions:

- Installation of a clear and thoughtful access and roles-concept;
- comprehensive access protocols (including automatic documentation of every reading, remote or remote-maintenance access);
- Possibility of physical deletion of data (also in back- up systems);
- Restrictions on data exports to the legally required level including its recording;
- Adaptation of the processed attributes to "use cases" (no data collection, if data are not necessary for valid processes) ;
- Possibility of anonymization and pseudonymization of data (system tests and system development with real data is not allowed according to data protection principles, since processing for such purposes does not fall under the purposes for which data were collected!);
- Exclusive commission of European sub contractors (to avoid difficulties with the international transfer of data – see: Schrems vs Facebook!);

Implementation in tender conditions II

Smart Meter:

- Data collection must be limited to legal requirements;
- Data readout options must be designed according to legal requirements (e.g.: data on daily consumption obligatory, data on consumption in an intervall of 15 minutes depending on user's consent).
- Control option for the settings of a display of the meter via a web portal mobile app to ensure user's access to and control of data to be obtained from the meter:
  - Information available via the display;
  - Readout of meter data by the network operator or by a service provider.

Data subject's rights:

- Requirement of a functionality of the system to obtain all data processed about a particular user easily in order to efficiently answer respective data subject's requests;
- Possibility of an entire deletion of a user upon his or her legitimate request (not duty or interest for controller for further storage of the user's data).

Tender procedures have already started - what can you (still) do?

1 Before the end of the tender period

- Cancellation of the tender procedure for “just cause”;
  Attention: duty to compensate for possible damages occurred for frustrated efforts of (potential) bidders;
- Rectification of the tender conditions.

After the end of tender period, before awarding the contract 2

- Tender procedures are often conducted in “negotiated procedures“, giving the contracting authority the opportunity to negotiate with the bidders;
- Limitations for negotiations and changes:
  - Taboo: the central aspects of the tendered products or services; data protection requirements are important elements, but don’t represent central aspects of the tendered service!
  - Changes to the tender conditions possible during the negotiation procedure, provided that
    - the information is announced to all bidders;
    - the circle of the potential bidders is not changed; and
    - all bidders are able to fulfil the changed requirements;
- Cancellation for “just cause” is still permissible.

Tender procedures have already started - what can you (still) do? II

3 The contract has already been awarded

- No space for rectification or modifications ;
- additional orders under certain circumstances, e.g. by way of a “direct award” of a contract without a tender procedure (be aware of value limits!) permissible.

Practical experiences 4

- Bidders are willing and able to fulfil the organizational requirements under data protection law;
  → Data protection requirements are not criticized by bidders;
- Negotiation results are still outstanding!

Data protection requirements in tender documents do not impair the procurement process while contributing to a data privacy compliance!!

PRESLMAYR
RECHTSANWÄLTE

Thank you for your attention!

Dr. Gerald Trieb, LL.M.

Attorney at Law and Partner

Preslmayr Attorneys at Law

1010 Vienna, Universitätsring 12

Tel. +43/1/5331695, Fax +43/1/5355686,

trieb@preslmayr.at

Registration for the firm's electronic newsletter 'P-News':
P-News@preslmayr.at