Data Protection and Smart Grid Communication

– The European Perspective –

Frank Pallas
Karlsruhe Institute of Technology
Center for Applied Legal Studies (ZAR)

Karlsruhe Institute of Technology

Europe is different.

Regulatory Approach

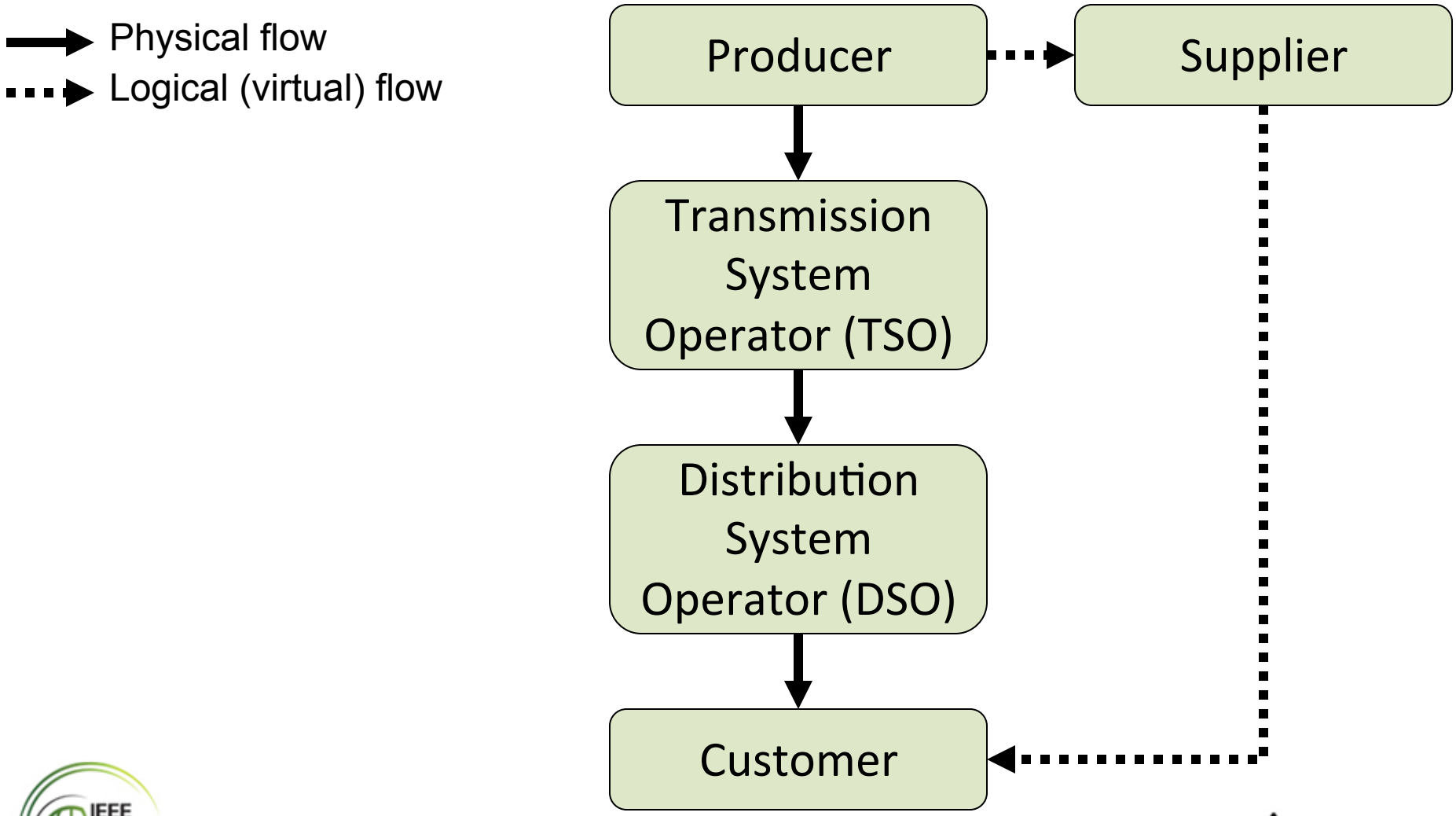
and

Privacy / Data Protection

EU Givens

~~„The Utility“~~

EU Givens: Energy Regulation



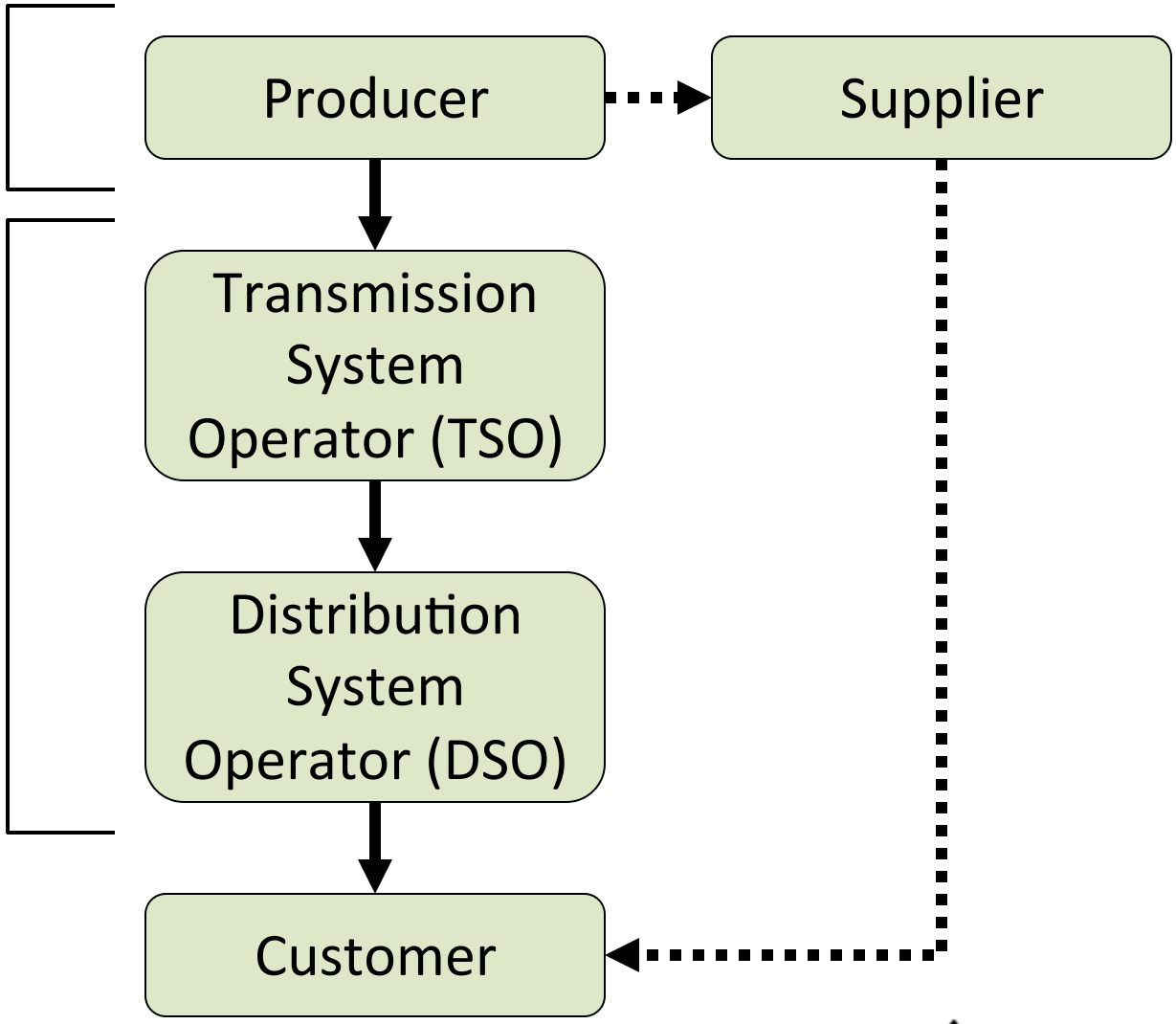
EU Givens: Energy Regulation

Market-driven

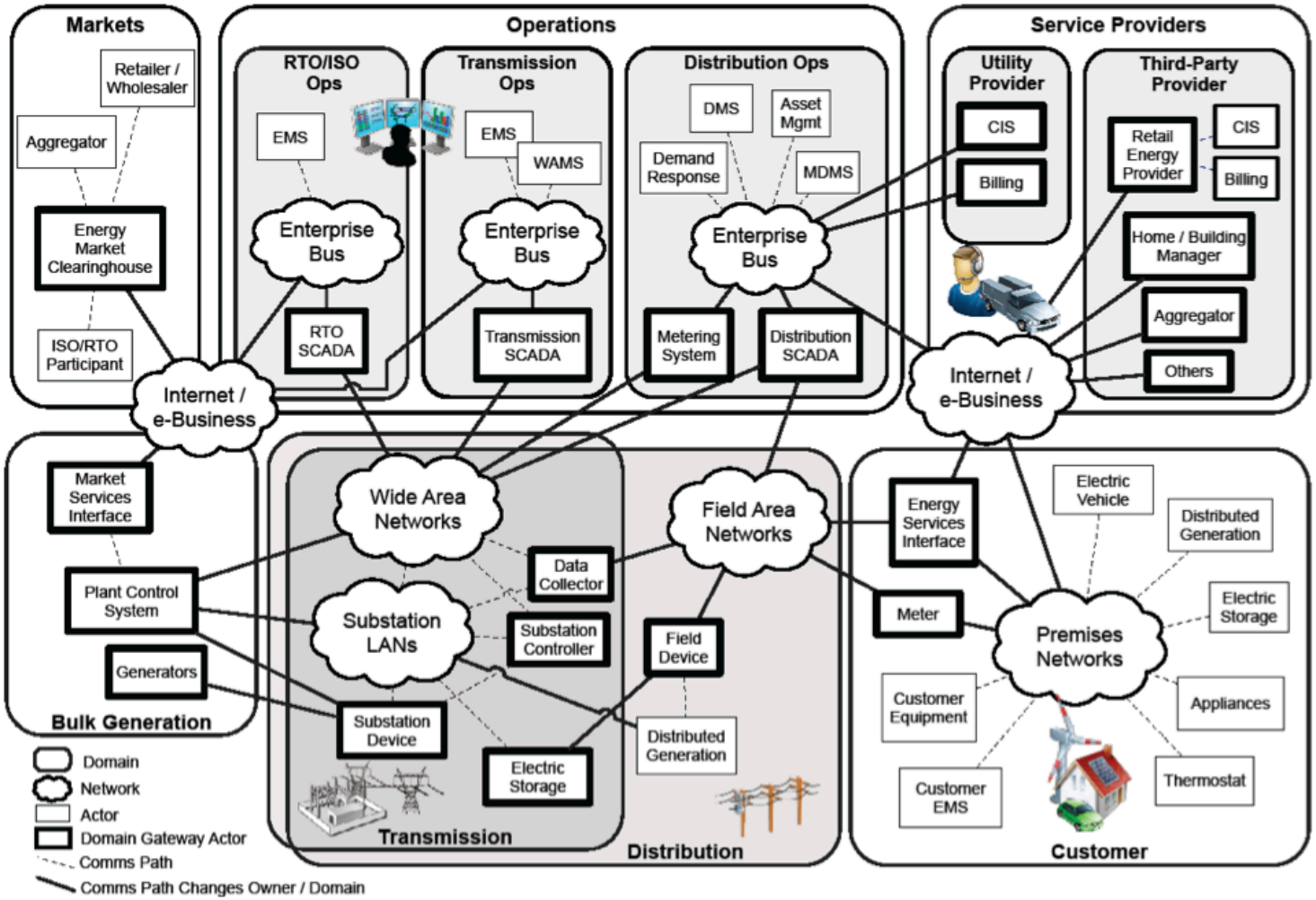
„Local Natural Monopolies“

➔ Strict Regulation

➔ Unbundling (incl. Information)

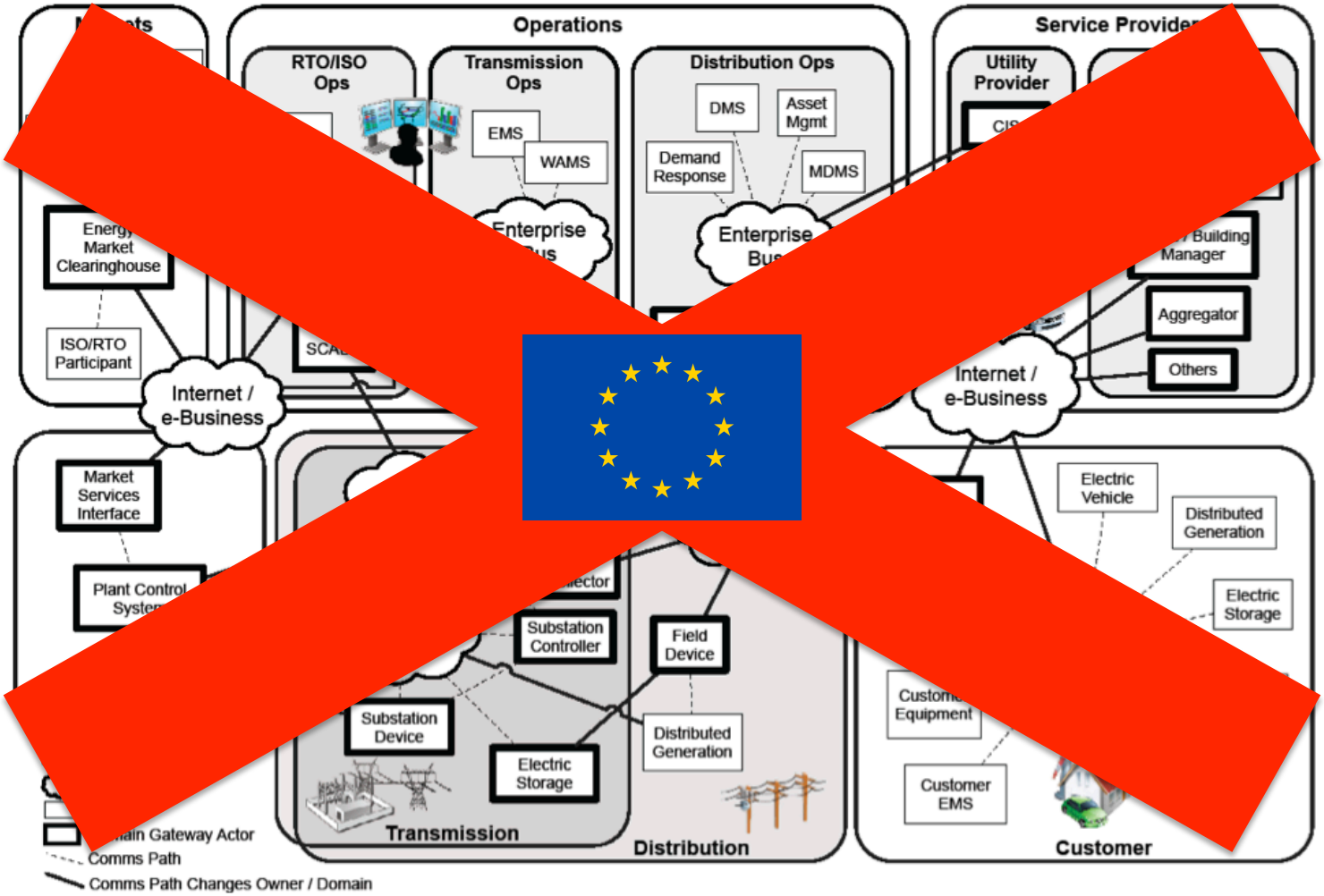


Domains vs. Unbundled Actors



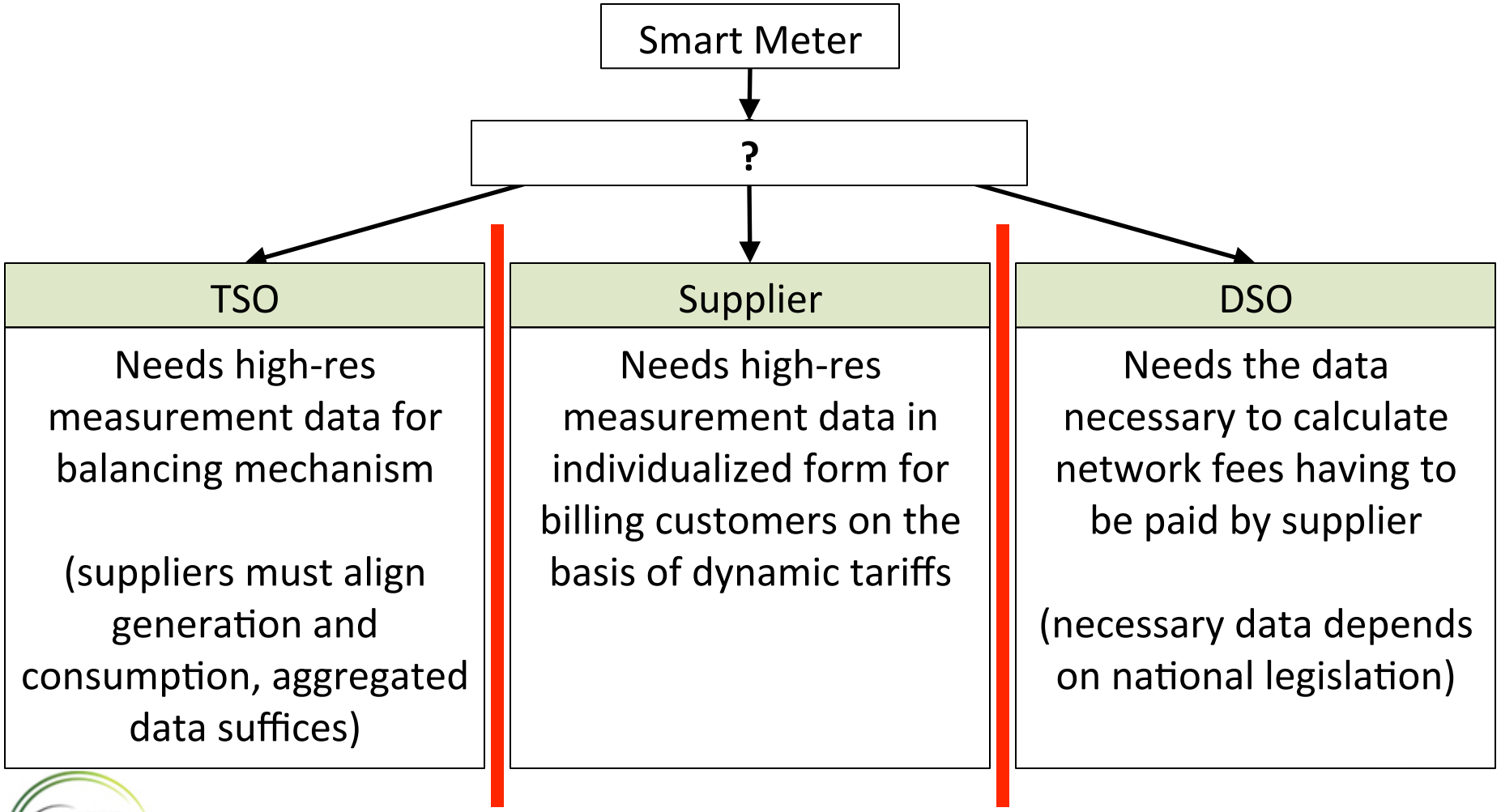
Source: NISTIR 7628 – Smart Grid Cyber Security Strategy and Requirements – „September Draft 2009“

Domains vs. Unbundled Actors



Source: NISTIR 7628 – Smart Grid Cyber Security Strategy and Requirements – „September Draft 2009“

„Informational Unbundling“



EU Givens

EU Givens: Data Protection („Privacy“)

Any collection, processing and use of
„personal data“...

... requires a **legitimation** for doing so, ...

... must serve well-specified and explicitly stated **purposes** and ...

... must be confined to the essential **minimum amount** of personal data.

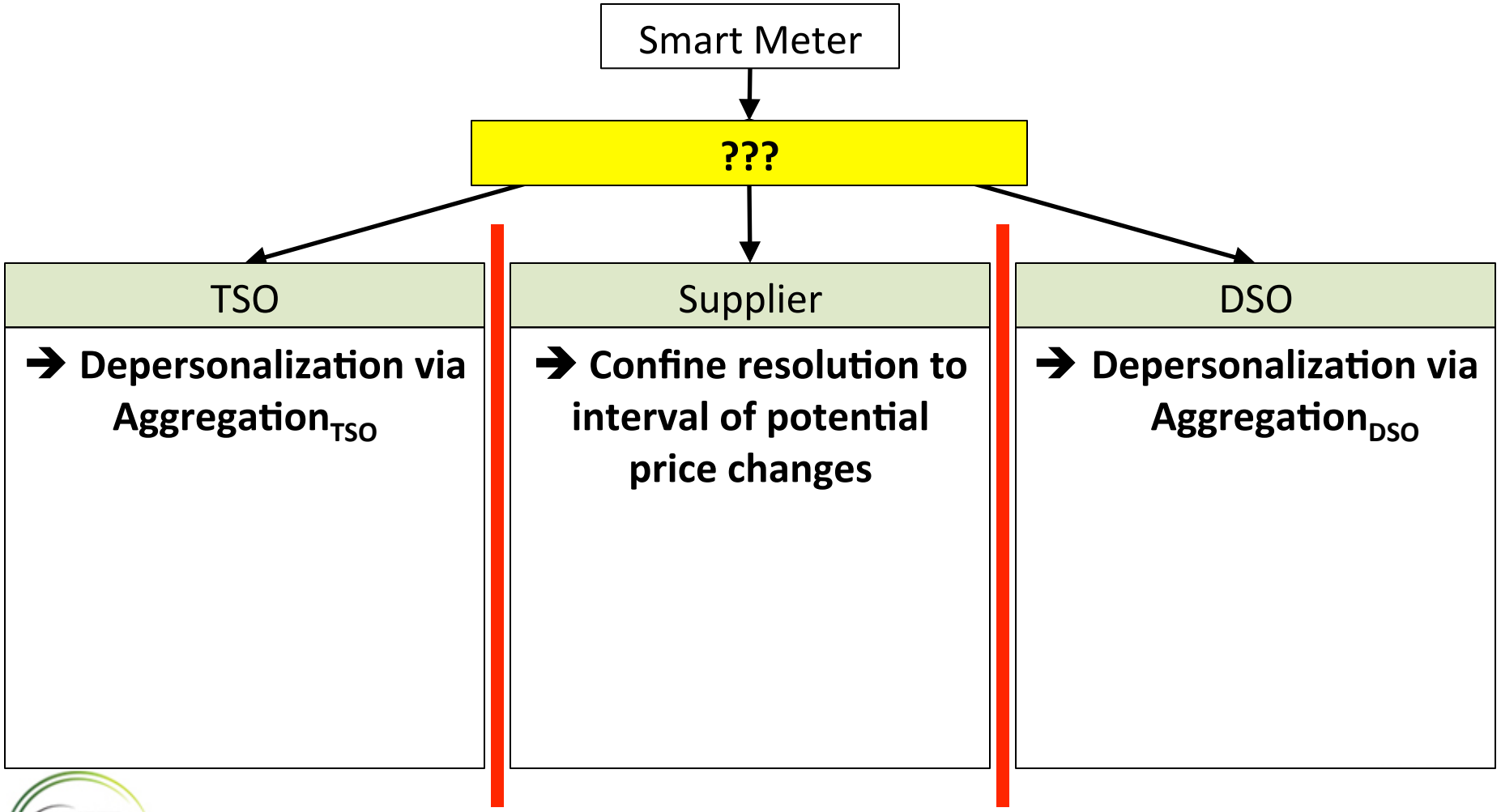
„Data Needs“ and Data Protection

TSO	Supplier	DSO
Legitimation: No contract; legal obligation inconsistent across EU	**Legitimation:** Contract with customer	**Legitimation:** No contract; legal obligation inconsistent across EU
Data minimization: Sum-values per supplier and/or DSO suffice under most legislations ➔ **Depersonalization via Aggregation$_{TSO}$**	**Data minimization:** ➔ **Confine resolution to interval of potential price changes**	**Data minimization:** Sum-values per supplier suffice under most legislations ➔ **Depersonalization via Aggregation$_{DSO}$**
Purpose limitation: --	**Purpose limitation:** May use for billing etc.; other purposes (targeted advertising) require separate legitimation (i.e. customer consent)	**Purpose limitation:** --

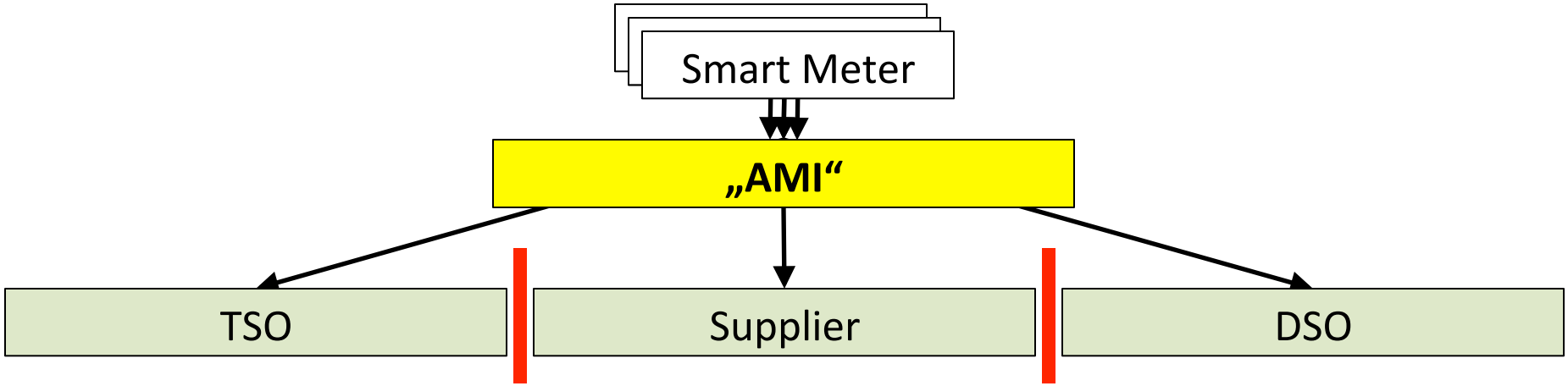
Implication

Any SG communication architecture that is to be deployed within the EU must provide different „restricted data views“ to different market roles, depending on different legitimating bases

„Data Needs“ and Data Protection

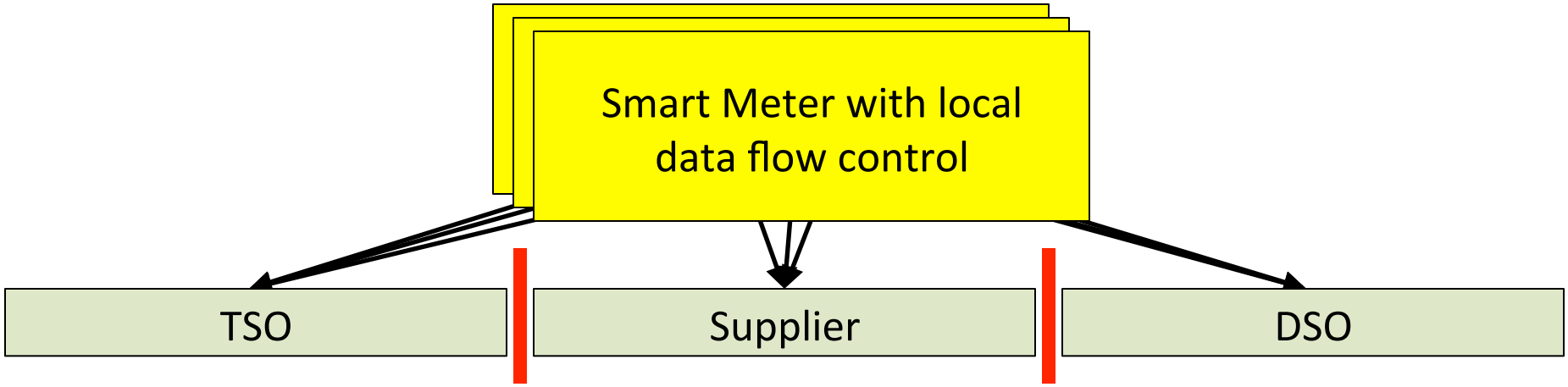


Approach 1: Central Database („AMI“)

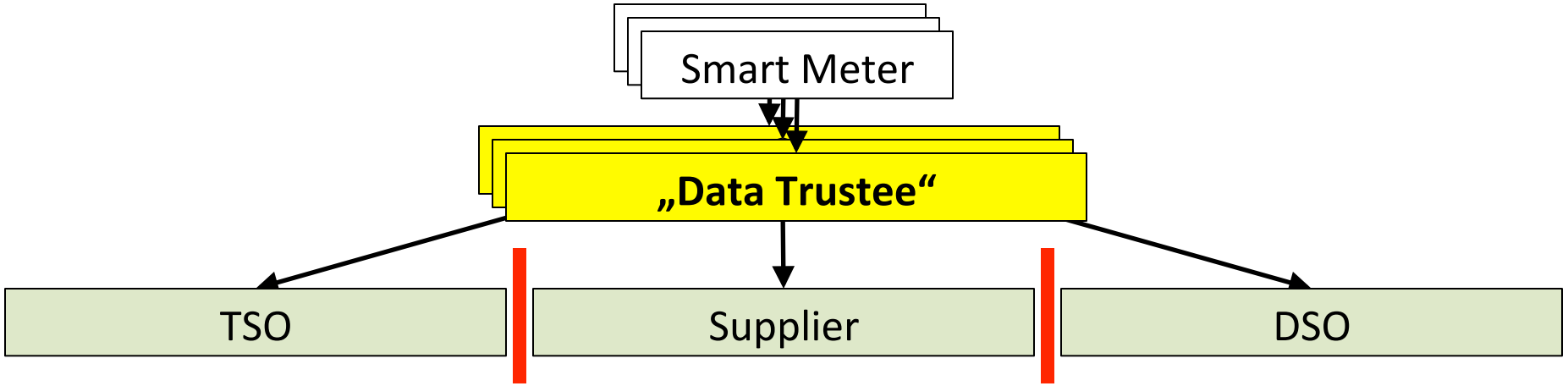


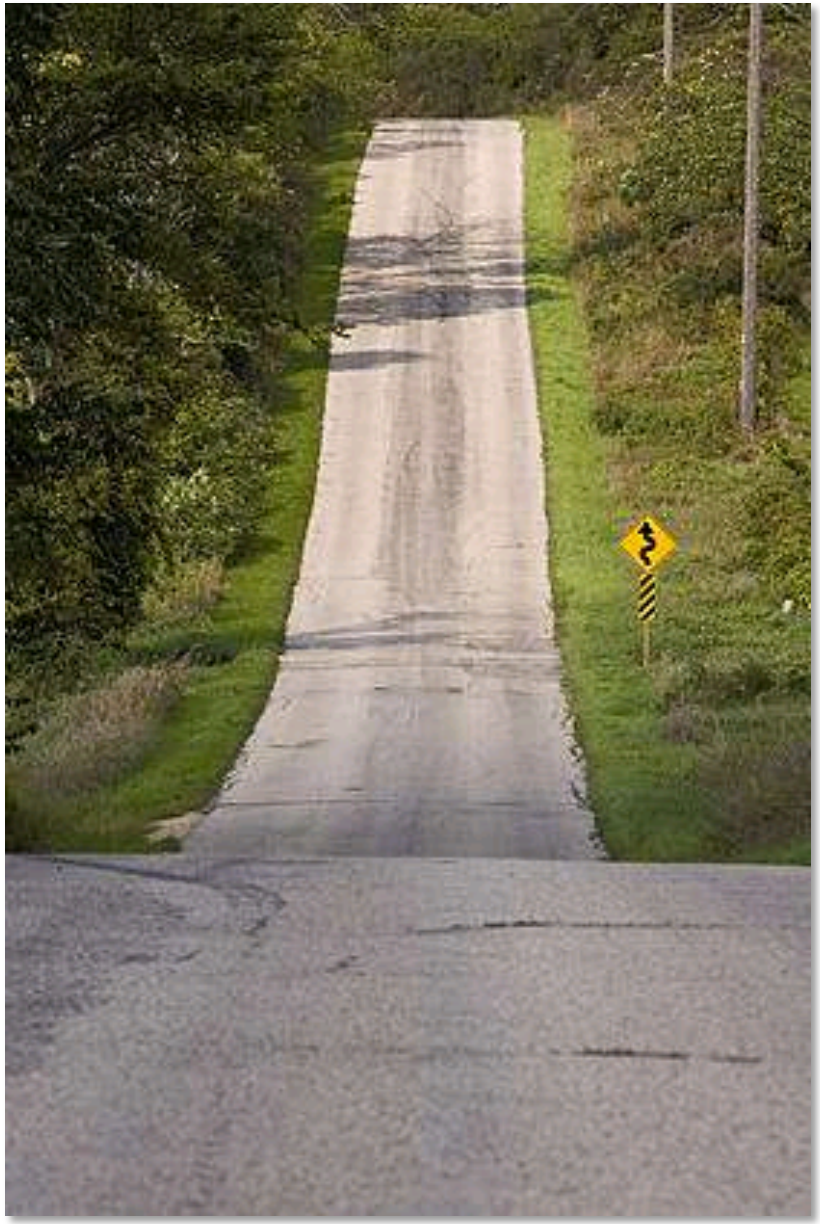
- ➔ Who should operate?
  State / DSO / TSO?
- ➔ No choice, customer is forced to „trust“
- ➔ Conflicts with idea of „informational self-determination“
- ➔ More or less attitude against centralized, inescapable databases across Europe (UK vs. D)

Approach 2: Acces Control at User Side



Approach 3: Customer-selectable „Data Trustees“





SEE THE PAPER

Europe is different.

And don‘t underestimate the implications arising from regulatory givens.

Contact

Frank Pallas

Karlsruhe Institute of Technology (KIT), Center for Applied Legal Studies (ZAR)

Research Group „Energy Information Law and New Legal Informatics“

http://compliance.zar.kit.edu

frank.pallas@kit.edu

This work was supported by the German Federal Ministry of Economics and Technology (EEnergy, Meregio, Grant 01ME08003).The authors are responsible for the content of the presentation.

Backup slides