WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

EFMD EQUIS ACCREDITED

Technical aspects vs. Innovation challenges of Enabling and Enhancing Privacy

Axel Polleres

(Thanks for their contributions to: Sabrina Kirrane, Erwin Filtz, Sushant Agarwal, Javier Fernandez,…)

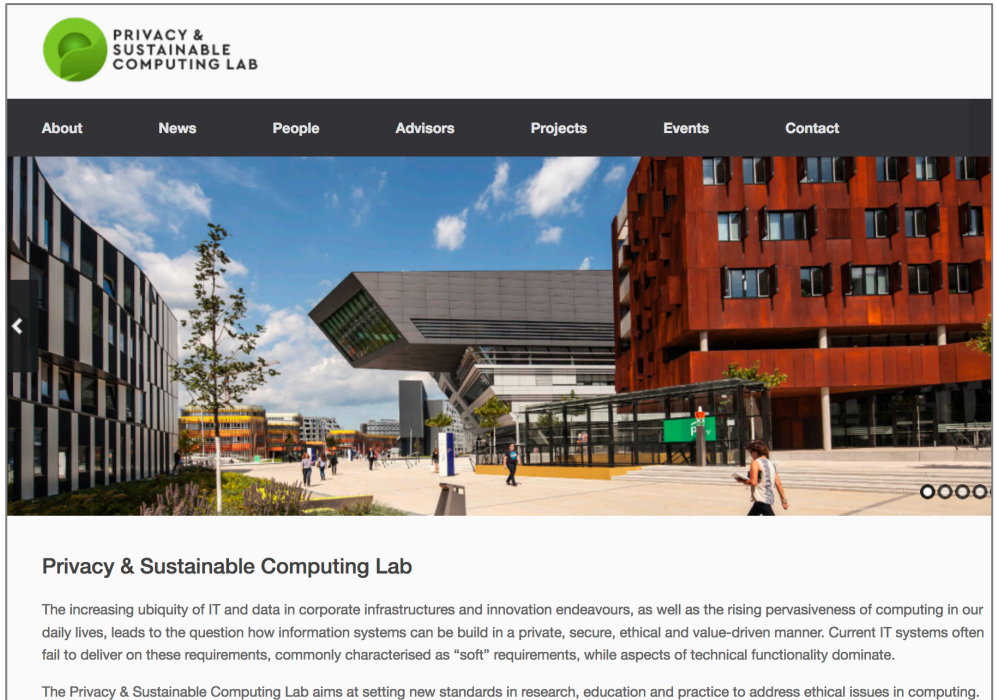
http://polleres.net

Twitter: @AxelPolleres

Where I am coming from, collaborators…

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

- **Privacy & Sustainable Computing Lab**
- http://www.privacylab.at/
- Launched September 2016, launch event with various important stakeholders: technologists, standardization, activists…
- Goal: setting new standards in research, education and practice to address ethical issues in computing.



Dr. Sabrina Kirrane (Lab Director)

Prof. Sarah Spiekermann (co-founder)

Prof. Axel Polleres (co-founder)

EFMD EQUIS ACCREDITED

Privacy in the EU: all about the upcoming GDPR, various national and European research efforts…

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Draft of the regulation
7/22/2012

Revisions in the draft
3/12/2013

Discussions in the EU Council
5/19/2014

Trilogue starts
6/24/2015

EU Council finalises the chapters
8/6/2015

Trilogue agrees
12/17/2015

Comes into force
5/15/2018

2013 | 2014 | 2015 | 2016 | 2017 | 2018

bmvit
Bundesministerium für Verkehr, Innovation und Technologie

Horizon 2020
European Union funding for Research & Innovation

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

ULD

TenForce
The Pragmatic Company

cbased®

the answer company™
THOMSON REUTERS®

W3C®

CeR ICT

Deutsche Telekom

ERCIM
European Research Consortium for Informatics and Mathematics

Technische Universität Berlin

proximus

EFMD EQUIS ACCREDITED

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

TU WIEN

Main technical challenges (prioritized from our point of view)

1. Informed Consent & Policies
2. Transparency, Deletion
3. Subjectivity
4. Anonymization

Last, but not least, and for all these challenges:
Protection vs. Innovation?

Consent & Policies

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

GDPR requirements:

Article #	Title	Description
7	Conditions for consent	Controllers should be able to demonstrate the 'freely given' consent from data subjects and should provide the right to withdraw consent any time

Opt-in, consent declarations

- Demonstrate consent
- Freely given
- Clearly distinguishable
- Withdraw consent at any time

Discussion:

- How to guarantee opt-in has been understood? Policy templates, "Privacy Icons"
- Research proposes that **opt-out, interactive processes,** and **partial consent** are more intuitive than opt-in by monolithic consent forms
- Giving consent online has many behavioural and UI components!
- Can I delegate consent to a personal agent?
    - How to express and execute consent **policies** in provable **machine readable form**?
    - Would that legally hold?

EFMD EQUIS ACCREDITED

Transparency, Access, Rectification, Deletion

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Article #	Title	Description
12	Transparent information, communication and modalities for the exercise of the rights of the data subject	To provide info related to processing in concise, transparent, intelligible and easily accessible form, using clear and plain language..
15	Right of access for the data subject	Right to access personal data which is collected and processed and to know which data is processed
16	Right to rectification	Right to ask controllers to rectify any inaccurate personal data regarding them
17	Right to erasure ("right to be forgotten")	Right to ask controllers to delete their personal data
18	Right to restriction of processing	Right to ask controllers to restrict processing of personal data

Trust via Transparency

- Concise, transparent, intelligible and easily accessible information about processing
- Using clear and plain language
- Standardized icons (machine-readable)

Discussion:

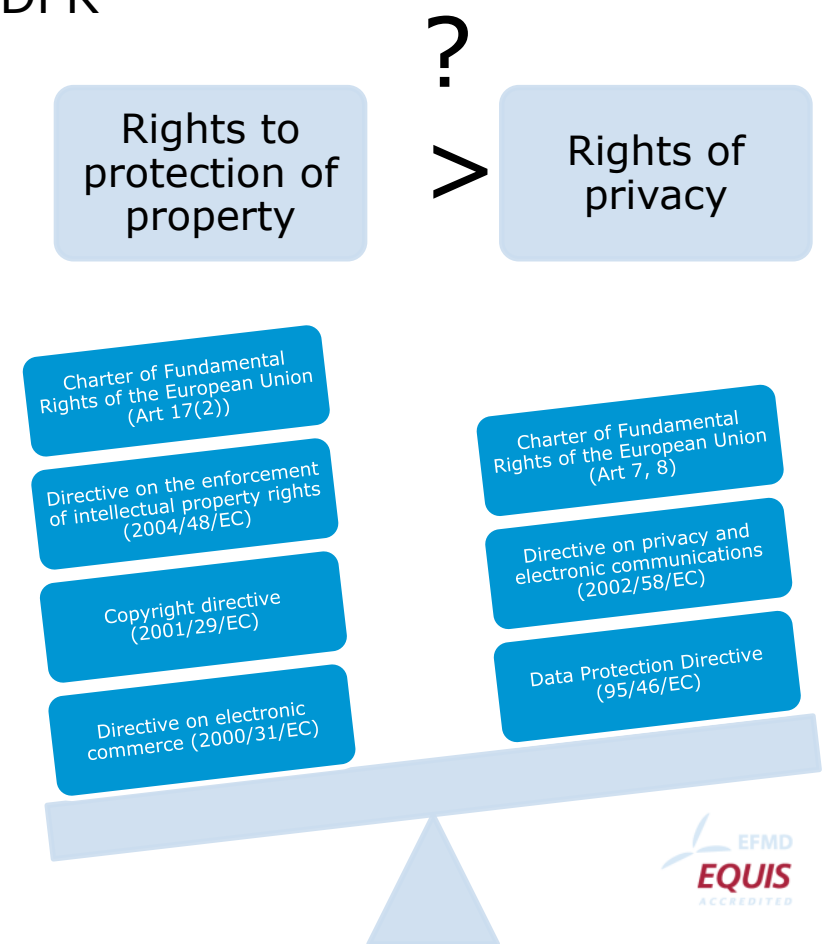
- Develop agreed models to present transparency data in a standardized manner, allowing the user to access the data collected about them in an integrated manner (e.g. Linked Data, PROV, extensions…)
- Open questions in terms of deletes (e.g. feasibility of Hard deletes in cloud environments) vs. transparency demands.
- Protocols to store transparency information *(Blockchain is not the only option!)*

EFMD EQUIS ACCREDITED

Subjectivity

- Ambiguity/Room for interpretation in the GDPR
- e.g. conflicting(national) laws with the GDPR
- Different national interpretations

Discussion:
- Metrics for e.g. understandability of privacy terms
- Standardization?
- *Investigate/analyze case law*



Anonymization for Innovation?

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

Having regard to the opinion of the Committee of the Regions ([2]),

Which K should we use for K-Anonymity? K-Anonymity is not enough!
Best practices and industry strength tools needed!

The GDPR does not apply to anonymous data where the data subject is no longer identifiable.

The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

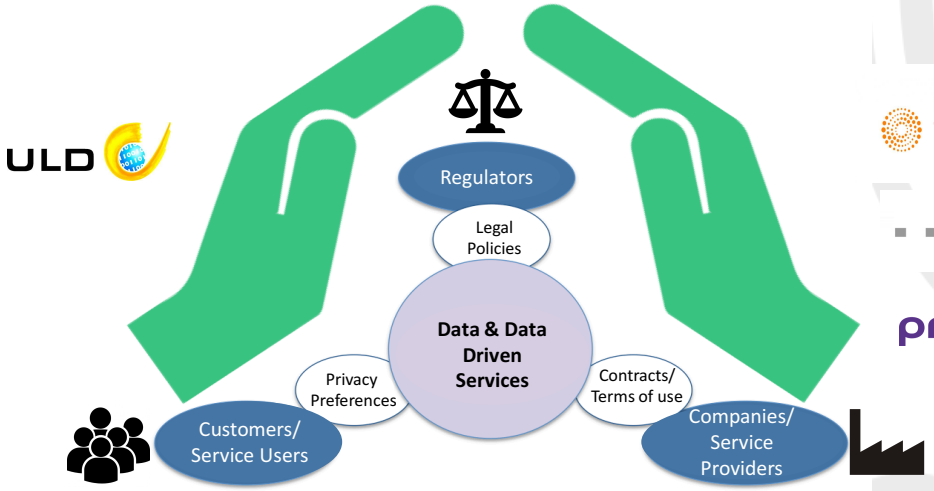
EFMD EQUIS ACCREDITED

Our current solution approach: The SPECIAL project

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

SPECIAL

Scalable policy-aware linked data architecture for privacy, transparency and compliance



ULD

the answer company™ THOMSON REUTERS®

Deutsche Telekom

proximus

W3C® ERCIM European Research Consortium for Informatics and Mathematics WU WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS TenForce The Pragmatic Company CeRICT Technische Universität Berlin

https://www.specialprivacy.eu/

Horizon 2020
European Union funding
for Research & Innovation

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 731601

EFMD EQUIS ACCREDITED

Our current solution approach: The SPECIAL project

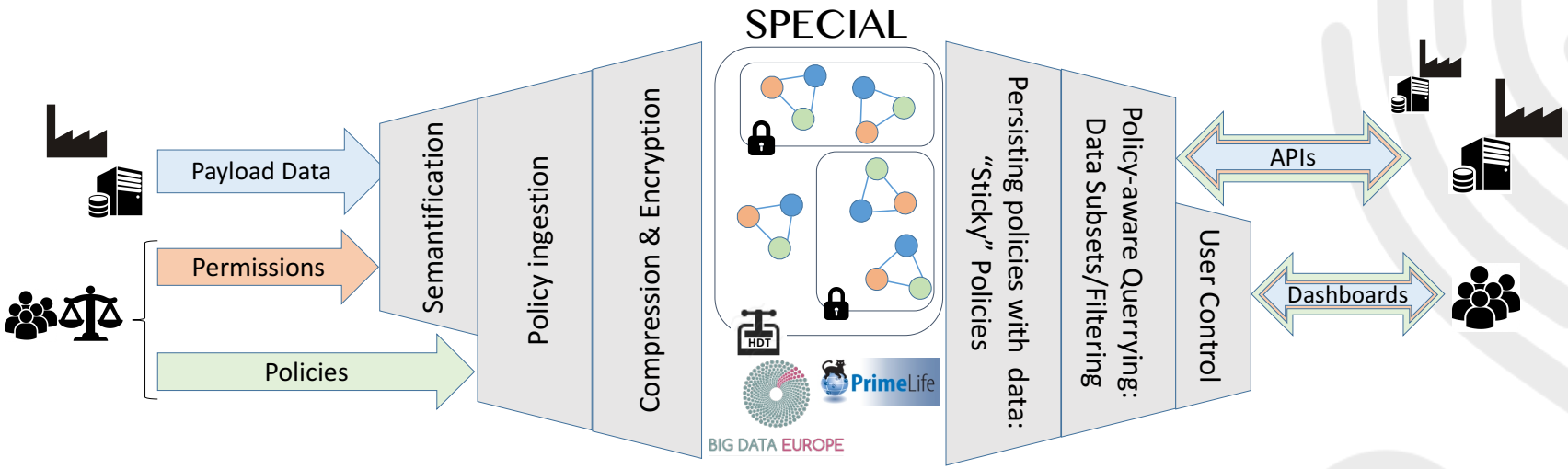
WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Objectives

- Policy management framework
  - Gives **users control** of their personal data
  - Represents **access/usage policies** and **legislative requirements** in a **machine readable format**
- Transparency and compliance framework
  - Provides information on how data is **processed** and with whom it is **shared**
  - Allows data subjects to take **corrective action**
- Scalable policy-aware Linked Data architecture
  - Build on top of the Big Data Europe (BDE) platform **scalability and elasticity mechanisms**
  - Extended BDE with **robust policy, transparency** and **compliance protocols**

EFMD EQUIS ACCREDITED

SPECIAL Technical components:



- **Big Data Europe** scalability and elasticity
- **PrimeLife** policy languages, access control policies, release policies and data handling policies

Technical aspects vs. Innovation challenges

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

- Summary and input for discussion:
  - **Technical support** for privacy should be understood as an innovation driver/asset, not an obstacle!
    - Many opportunities for tools and algorithmic support
    - E.g.
      - formalizing and reasoning about Policies + data analytics about case law (=**Rules + Data Science**)
      - **UI**s, **Standards**, Best Practices
      - **Linked Data** for Privacy!
  - Take the enterprise view of Big Data analysis into account!
  - **Harmonization** on Privacy law alone is not enough, but also on the **national interpretations** and conflicting laws!

- Thank you!

EFMD EQUIS ACCREDITED