Privacy-Enhancing Technologies – where are we after 25 years?

> Marit Hansen Data Protection Commissioner Schleswig-Holstein, Germany

IFIP Summer School on Privacy and Identity Management 23 September 2020

orum



Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein





Overview



25 years ago ... a look into 1995

- Status 2020: GDPR
- Potential (of) privacy-enhancing technologies
- PETs a success story?
- Conclusion

PETs – where are we after 25 years?



www.datenschutzzentrum.de

European Data Protection Directive 95/46/EC

23. 11. 95 EN Official Journal of the European Communities

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Article 15

Automated individual decisions

Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to subgaud his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

No L 281/43

otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

Article 17 Security of processing

An end of their behalf for the purposes of driver markening, and to be expressively offered their head of the purposes of driver markening, and to be expressively offered their head of the purposes of driver markening and to be expressively offered their head of the purposes of driver markening and the purposes of driver driver drivers of the purposes of driver d

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

the processor shall act only on instructions from the controller,

the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.



1995: "Privacy-Enhancing Technologies"

John Borking et al.: Privacy-enhancing technologies – The path to anonymity", 1995

Transferring ideas from David Chaum et al. to the data protection community



PETs – where are we after 25 years?

www.datenschutzzentrum.de

"Identity Protector"



Was sind Privacy-Enhancing Technologies?

"Privacy-Enhancing Technologies (PET) are a coherent system of ICT measures that protects privacy [...]
by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system."

Borking / Raab (2001)

PETs – where are we after 25 years?



ULD

www.datenschutzzentrum.de

Overview



- 25 years ago ... a look into 1995
- Status 2020: GDPR
- Potential (of) privacy-enhancing technologies
- PETs a success story?
- Conclusion

Source: athree23 via Pixabay



General Data Protection Regulation

• Idea:

One for All and All for One

- Objective: real harmonisation
- But: 70 opening clauses ("variables" for Member States)



https://upload.wikimedia.org/wikipedia/commons/ 8/85/Unus_pro_omnibus%2C_omnes_pro_uno.jpg

PETs – where are we after 25 years?

www.datenschutzzentrum.de

Regulation (EU) 2016/679

9

GDPR as "Game Changer" (?)



Source: Astryd_MAD via Pixabay

Powerful toolbox if applied appropriately

- Market location principle (Art. 3 GDPR)
- Responsibility (Art. 24 gdpr)
- Data protection by design (Art. 25(1) GDPR)
- Data protection by default (Art. 25(2) GDPR)
- Security (Art. 32 gdpr)
- Data protection impact assessment (Art. 35 GDPR – "Rights and freedoms of natural persons")
- Certification (Art. 42+43 GDPR)
- Fines & sanctions by Data
 Protection Commissioners (Art. 83+84 GDPR)
- Courts



Which roles do you play?



www.datenschutzzentrum.de

Data Protection by Design & by Default

• Art. 25 GDPR

- Targeted at controllers
- Producers of IT systems "should be encouraged" (Rec. 78)

- Art. 25 Data Protection by Design and by Default
- Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, [...] which are designed to implement data-protection principles [...], in an effective manner [...]
- Objective: to design systems + services from early on, for the full lifecycle ...
 a) ... in a data-minimising way
 b) ... with the most data protection-friendly pre-settings



Data Protection by Design & by Default

- Art. 25 GDPR
- Targeted at controllers
- Producers of IT systems "should be encouraged" (Rec. 78)

- Art. 25 Data Protection by Design and by Default
- The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. [...]

13

14

- Objective: to design systems + services from early on, for the full lifecycle ...
 a) ... in a data-minimising way
 - b) ... with the most data protection-friendly pre-settings

PETs – where are we after 25 years?



PETs - where are we after 25 years?

ULD

Data protection: more than IT security





... more than IT security

- Availability + integrity guarantees may hinder erasure, possibly conflicting with data minimisation/unlinkability + intervenability (right to erasure, right to rectification)
 - E.g. blockchain implementation
 - E.g. redundancy by distributing various copies
 - E.g. logfiles with personal data
- Confidentiality guarantees may hinder transparency (information) + intervenability (on the basis of the right of access)
 - E.g. hidden data collection



www.datenschutzzentrum.de

Overview

17



- 25 years ago ... a look into 1995
- Status 2020: GDPR

PETs - where are we after 25 years?

- Potential (of) privacy-enhancing technologies
- PETs a success story?
- Conclusion

Source: athree23 via Pixabay





PETs – where are we after 25 years?



www.datenschutzzentrum.de



... knows everything!



Multiple anonymization proxies in a cascade

... with encryption for separation of information: No entity knows everything!



PETs – where are we after 25 years?





Real scenario: Infrastructure? Who is the operator?





- E.g. TOR or AN.ON for IP addresses
- Anonymization method: "sameness"

PETs – where are we after 25 years?



www.datenschutzzentrum.de



23

Possibilities

- For communication infrastructure
- Service for controllers (companies, authorities)
- Participation / crowd approach: everybody can provide a Mix

Obstacles

- Infrastructure who is the controller?
- Based on separation of the knowledge of multiple actors – how about legal accountability questions?
- IP address anonymization not sufficient



ATTRIBUTE-BASED CREDENTIALS

PETs - where are we after 25 years?



www.datenschutzzentrum.de

Best Practice "Data minimisation": Authentication without identification

For each purpose: Which data are necessary?

Complete Data:



Often not all data necessary

Minimal data:



Usual case: linkable information



Example: Attribute-based credentials

in school communication



PETs – where are we after 25 years?



ULD 🌈

www.datenschutzzentrum.de



Possibilities

- Whenever authentication is necessary
- If proof of attributes is sufficient

Obstacles

- Infrastructure necessary, e.g. for role-out + revocation
- If re-identification offered: additional complexity
- Different from today



DATA TRACK

PETs - where are we after 25 years?



www.datenschutzzentrum.de

From the Privacy Lab: "Data Track"





32

PrimeLife

***PRIME*



Source: A4Cloud, D-5.4 User Interface Prototypes V2, 2015 http://cloudaccountability.eu/sites/default/files/D45.4 User interface prototypes V2.pdf

Usage?

Possibilities

• For each interaction

Obstacles

- User-side security difficult
- May cause effort on the side of the controllers if data subject rights become known
- Potentially, the user becomes a controller herself

PETs – where are we after 25 years?



www.datenschutzzentrum.de

Overview



- 25 years ago ... a look into 1995
- Status 2020: GDPR
- Potential (of) privacy-enhancing technologies
- PETs a success story?
- Conclusion

Source: athree23 via Pixabay

Privacy-enhancing technologies: How mature? How usable?



www.datenschutzzentrum.de

Contact Tracing instead of data retention of location data

- Pandemics contact tracing app for the masses
- Basis: Bluetooth

- Contacts, not locations
- Changing identifiers
- Decentralised storage
- Promised:
 - Voluntary
 - Opt-in
 - No other purposes



😉 🧕 Source: Gerd Altmann via Pixabay

• Corona-Warn-App: Open Source, documents on Github: e.g. https://github.com/corona-warn-app



Overview



• 25 years ago ... a look into 1995

- Status 2020: GDPR
- Potential (of) privacy-enhancing technologies
- PETs a success story?
- Conclusion

PETs – where are we after 25 years?

www.datenschutzzentrum.de

Challenge: Bridging the gap between technology and (data protection) law



Source: Free-Photos via Pixabay



www.datenschutzzentrum.de

Who is the hero?



Source: skeeze via Pixabay

PETs – where are we after 25 years?



Conclusion



Source: congerdesign via Pixabay

- Data protection by design and by default
 - Demanded by the GDPR
 - Thereby to be demanded by controllers
- Success stories are rare
- Privacy-enhancing technologies alone not sufficient
- Ongoing work
- Needed: framework + help
- And: visibility of good solutions

PETs – where are we after 25 years?