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

Setting of ULD

- Data Protection Authority (DPA) for both the public and private sector
- Also responsible for freedom of information

Source: en.wikipedia.org/wiki/Schleswig-Holstein

Source: www.maps-for-free.com
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

European Data Protection Directive
95/46/EC

---

<table>
<thead>
<tr>
<th>No.</th>
<th>Article</th>
<th>Relevant Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.10.95</td>
<td><strong>Article 17</strong></td>
<td><strong>Safeguards for processing</strong></td>
</tr>
<tr>
<td>1</td>
<td>Member States shall provide for the protection of the rights and freedom in respect of the processing of personal data. This protection shall be without prejudice to the obligations arising from the application of any agreements concluded between Member States which provide for a level of protection of personal data equal to that ensured in accordance with the Directive, and applicable at the time of its conclusion, and whose implementation is not impeded by the provisions contained in this Directive.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>The Member States shall provide that the controller is responsible for, inter alia, ensuring that processing is in accordance with this Directive and that the rights of the data subject are not adversely affected by the processing.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>The controller shall, in any case, provide the data subject with a statement of the envisaged safeguards in respect of the processing in question, if the data subject has not been satisfied with the answer given by the data subject.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>The safeguards referred to in paragraph 1 shall, in any case, be without prejudice to the principles of processing personal data and must be in accordance with the principles laid down in the other Articles of this Directive, and to the extent necessary, in accordance with the other legal provisions of the Member States.</td>
<td></td>
</tr>
</tbody>
</table>
1995: “Privacy-Enhancing Technologies”


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

"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)

Overview

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

- **Idea:**
  One for All and All for One

- **Objective:**
  real harmonisation

- **But:** 70 opening clauses ("variables" for Member States)

PETs – where are we after 25 years?

GDPR as "Game Changer" (?)

- **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**

Powerful toolbox if applied appropriately
Which roles do you play?

Art. 4 (7) GDPR: ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Art. 4 (8) GDPR: ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Data Protection by Design & by Default

- Art. 25 GDPR
  1. 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 […]

- Targeted at controllers

- Producers of IT systems “should be encouraged” (Rec. 78)

- 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)

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

Art. 25 Data Protection by Design and by Default

2. 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. [...]

Imbalance in power
⇒ data protection necessary

Important: Perspective of the individual

Source: beludise via Pixabay
Data protection: more than IT security

**PETs – where are we after 25 years?**

IT security: The adversary is Eve (or Mallory).

Data protection: The adversary is Bob! (Well, at least he is one of them.)

---

Protection goals: more than IT security

Confidentiality

Unlinkability

+ Data minimisation

Integrity

Intervenability

Transparency

Availability

classical IT security protection goals*)

*) From the data subject’s perspective
... 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

Overview

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

The simple "Anonymization" Proxy

... knows everything!
Multiple anonymization proxies
in a cascade

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

Anonymity with Mixes
(David Chaum 1981)
**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?**

**Usage?**

**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

Best Practice „Data minimisation“: Authentication without identification

For each purpose:
Which data are necessary?

**Complete Data:**

**Minimal data:**

Often **not** all data necessary
**Usual case: linkable information**

[Diagram showing linkable information between Driver's License, Insurance, and Cars]

**Data minimisation by attribute-based credentials**

[Diagram showing data minimisation and verification by a trustworthy third party]
Example: Attribute-based credentials
in school communication

PETs – where are we after 25 years?

Usage?

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 minimisation through
- attribute selection,
- attribute aggregation,
- unlinkability of multiple presentations

https://abc4trust.eu/soederhamn
From the Privacy Lab: “Data Track”

- User-side tool
- For transparency + exercising one’s rights
Extension for typical cloud usage

The prototype of the trace view interface of the Data Track tool.

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

Basis for exercising data subjects' rights

A redesign proposal of GenomSyntig in which users have the choice from the to access data stored locally or control their data stored in a remote service.

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

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

- Technologies:
  - Anonymisation?
  - Identity management?
  - Encryption?
  - IoT privacy?
- Terminology
- Usability?
- Awareness?

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

- 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

Challenge: Bridging the gap between technology and (data protection) law
Key escrow  Weak crypto  Sisyphos
Backdoors  Data retention
Real names  Biometrics
Politics without expertise

"One must imagine Sisyphos happy."

Who is the hero?
The fire fighter or the maintenance technician of the fire detection system?
Or the thoughtful scientist?

PETs – where are we after 25 years?
Conclusion

• 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