Privacy and Data Protection

Jens Kremer, University of Helsinki
Content

1. Privacy
2. Data Protection
3. The Regulation of Data (GDPR)
WHAT ARE YOU LOOKING AT?

Part 1: Privacy
Privacy

- To be Let Alone
- Limited Access to person
- Secrecy
- Informational Self-Determination
- Identity & Personhood
- Intimacy Relationships
Privacy as a global Human Right

- Universal Declaration of Human Rights (UDHR); 10 December 1948: Article 12
- International Covenant on Civil and Political Rights (ICCPR); 16 December 1966; Article 17
- European Convention on Human Rights (ECHR), 3. September 1966, Article 8;
Privacy as a Fundamental Right

European Convention on Human Rights (ECHR)

Article 8 – Right to respect for private and family life

- 1. Everyone has the right to respect for his private and family life, his home and his correspondence.

- 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
Rights: Scope

Art 8 (1) ECHR

• *Everyone* has
  • the *right to respect*
    • for his *private*
    • and his *family life,*
    • his *home*
    • and his *correspondence*
Right: Limitation

2. There shall be **no interference** by a public authority with the exercise of this right except such as is

- in **accordance with the law** and is
- **necessary in a democratic society**
- in the **interests** of
  - national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
In the **Scope**?

Yes → Justified through Limitation?

No → No

Yes → Violation!

Bad!
Part 2: Data Protection
EU Charter of Fundamental Rights

Article 7 Respect for private and family life

• Everyone has the right to respect for his or her private and family life, home and communications.

Article 8: Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

The Protection of Personal Data

‘personal data’

• means any information **relating to an identified or identifiable natural person** (‘data subject’);

• an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier

• or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Processing

‘processing’ means

• any operation or set of operations which is performed on personal data or on sets of personal data,

• whether or not by automated means,

• such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
The new European General Data Protection Regulation (GDPR)

Part 3: GDPR
The European Data Protection Reform

- **First GDPR draft released**
  - January 2012

- **Trialogue end and LIBE Committee vote**
  - December 2015

- **Adoption by EU Parliament and Council**
  - April 2016

- **Entered into force**
  - 4th of May 2016

- **Directly applicable in EU**
  - 25th of May 2018


**New: Unified Regulation** directly applicable in all EU Member States: *The General Data Protection Regulation*

EU Data Protection from May 2018

EU Regulation 2016/679 (GDPR)
- Applies to all processing of personal Data
- by public bodies, private entities, and individuals
- Directly in all EU Member states

EU Directive 2016/680 (Police and Criminal Justice)
- Applies to all processing of personal data
- by authorities for police and criminal justice purposes
- Implemented through national laws in EU Member States
GDPR Scope: Who does it apply to?

- Protects **rights and freedoms of natural persons**, the right to privacy and the right the protection of personal data.

- EU-wide standard for rules of personal data processing

- Applies to all **processing of personal data** (Art 2(1) GDPR)

- Does NOT apply to (Art 2(2) GDPR):
  - activity outside the **scope of Union law**
  - Member states activities regarding **defense and national sec.**
  - Purley personal or household activities (**household exemption**)
  - Police and criminal justice matters (but: Directive)
Some Terminology

**personal data**
any information relating to an *identified* or *identifiable* natural person (‘data subject’)

**processing**
any operation which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

**controller**
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

**processor**
a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

(Article 4 GDPR)
Personal Data Categories

Anonymous Data → Identifiable Personal Data → Identified Personal Data → Sensitive Data

Risk Level & Safeguards

Rights interference: Data Protection Law applies
Anonymization & Pseudonymization

• Personal data is personal when a data subject can be identified or is identifiable (with ‘reasonable’ means).
• Truly anonymized data is not personal data
• ‘pseudonymisation’: no longer directly attributable.
  • ‘Rami Miller, born 10.9.1990 has two cats and one dog’
  • → R.M. 1990, Cats: 2, Dog: 1
  • → cX2391, Cats: 2, Dog: 1.

• Pseudonymized data is always personal data!
• Pseudonymization may be a safeguard that mitigates privacy risks.
GDPR Territorial Scope: Where?

1. GDPR applies
   - EU
   - C/P

2. GDPR applies
   - EU
   - C/P
   - Offering goods or services

3. GDPR applies
   - EU
   - C/P
   - Monitoring DS

4. GDPR does not apply
   - EU
   - C/P

Controller or Processor

Data Subject
How to process personal data?

The right to **privacy** and right to **personal data protection** are Fundamental Rights in Europe.

- All personal data processing is interfering with individual rights.
- All personal data processing is therefore illegal, unless it can be justified.

**GDPR Lawful Grounds for Data Processing:**

- Individual Consent
- Contract
- Legitimate Interest of the Controller
- Public Interest
- Protecting Vital Interest
- Legal Obligation
Legal Basis: Consent (Art 7)

- Consent under the GDPR comes with new requirements:
  - Needs to be freely given, specific, informed, unambiguous
  - Genuine free choice: consent cannot be made conditional for providing a service
- Contract is not consent!
- Clear language, separate presentation, clear affirmative action (e.g. no pre-ticked box)
- Purpose – specific
- Consent can be revoked at any time
Basic Principles of Data Protection

- Fair, Lawful and Transparent Processing
- Purpose Limitation
- Data Minimization
- Data Security
- Limited Retention
- Accuracy
- Accountability
# Rights of Data Subjects

<table>
<thead>
<tr>
<th>Category</th>
<th>Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transparency and Information</strong></td>
<td>• Importance of information and communication</td>
</tr>
<tr>
<td></td>
<td>• Clear, concise, intelligible and accessible information</td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td>• Control over personal data, informational self-determination</td>
</tr>
<tr>
<td></td>
<td>• Right to obtain information about processing</td>
</tr>
<tr>
<td><strong>Rectification and Erasure</strong></td>
<td>• Data rectification</td>
</tr>
<tr>
<td></td>
<td>• ‘Right to be forgotten’</td>
</tr>
<tr>
<td><strong>Restriction</strong></td>
<td>• Right to restriction of processing</td>
</tr>
<tr>
<td><strong>Data Portability</strong></td>
<td>• Demand transfer data from one service to another</td>
</tr>
<tr>
<td></td>
<td>• Receive data in ‘structured, commonly used and machine-readable format’</td>
</tr>
<tr>
<td><strong>Object</strong></td>
<td>• Right to object processing at any time</td>
</tr>
<tr>
<td></td>
<td>• When processing is based on legitimate interest, public interest</td>
</tr>
<tr>
<td></td>
<td>• To direct marketing</td>
</tr>
<tr>
<td><strong>Profiling</strong></td>
<td>• The right to not be subjected to automated decision-making and profiling</td>
</tr>
<tr>
<td><strong>Judicial Remedy</strong></td>
<td>• Right to lodge complaints with DPAs in own Member State</td>
</tr>
<tr>
<td></td>
<td>• National Court complaints if unhappy with DPA procedure</td>
</tr>
</tbody>
</table>
Obligations of Controllers/Processors

**Controllers**

- Accountability and Responsibility
- Data Protection by Design and by Default
- Joint Controller arrangements
- Appointment of Representatives (if outside EU)
- Appointment of Processors
- Processing Records
- Cooperation with DPAs
- Data Security and data breach reporting/notification

**Processors**

- Confidentiality of processed data
- Compliance with Controller's instructions. Failure: full liability as controller
- Record keeping
- Cooperation with DPA
- Data Security
- Data Breach Reporting
Other GDPR Content

- Privacy Impact Assessments (PIAs)
- Prior Consultation with DPAs (in certain cases)
- Data Protection Officers (DPOs)
- Industry Specific Codes of Conduct
- Seals and Certification
- DPAs and One-stop Shop
Enforcement and Sanctions

Everybody needs to be compliant in May 2018.

Liabilities:

• Compensation for Data Subject damages

• Administrative Fines
  • Effective, proportionate and dissuasive fines
  • Maximum Fines: 10 Million EUR/2% or 20 Million EUR/4% of global annual turnover

• Possible criminal sanctions in Members States
Tasks/ Homework

- **Task 1:** Is your consent valid?

- **Task 2:** Access Request

- **Task 3:** Anonymisation and Pseudonymisation
  - How can personal data be anonymized?
  - Understand the difference between pseudonymisation and anonymisation.
  - Problem of re-identification of anonymized data with machine learning.