Privacy-preserving technologies
2021/22 spring

Week 2: Legal status of privacy technologies (16.02.2022)
Introduction
About me

15 years as a legal counsel

10 years in legal research

10 years as a lecturer in law for non-legal students

Current position: Privacy Engineering Consultant at Cybernetica
Homework

You will find today’s lecture and the accompanying materials useful when preparing the homework assignment.

No extra homework on the topic of „Legal status of privacy technologies” 😊
Agenda

1. Applicable laws
2. Main terms and definitions
3. Data protection principles
4. Data subject rights
5. Data controller obligations
6. Transfers of personal data
Applicable laws
Current applicable laws

International law (Council of Europe)
- European Convention on Human Rights (ECHR)
  - Convention 108

Regional law (European Union)
- Charter of Fundamental Rights of the European Union (CFR)
  - General Data Protection Regulation (GDPR)
  - Data Protection Law Enforcement Directive (DPLED)

National law (Estonia)
- The Constitution of the Republic of Estonia
  - Personal Data Protection Act¹ (IKS)
Human rights: ECHR (CoE)


Entry into force: 03.09.1953

Summary:
1. the first instrument to give effect to certain of the rights stated in the Universal Declaration of Human Rights (1948) and make them binding
2. established the European Court of Human Rights, which functions on a permanent basis
3. includes the right to privacy
Human rights: CFR (EU)

Full title: Charter of Fundamental Rights of the European Union

Entry into force: 01.12.2009 (together with the Treaty of Lisbon)

Summary:
1. The Charter has equal standing with other founding Treaties of the EU
2. individuals can take an EU institutions and Member States to court for failing to uphold their rights in the Charter when implementing EU law.
3. The only act of its kind which recognizes both the right to privacy as well as the right to data protection.
Privacy or data protection?

**PRIVACY**

relates to respect for private communications, home and for family life

privacy is driven by individual control

**DATA PROTECTION**

a broader fundamental right:
1. includes the human interest in autonomy
2. protective of the full range of fundamental rights impacted by the processing of personal information

data protection is driven by fair processing

Data protection: Convention 108 (CoE)

Full title: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)

Entry into force: 01.10.1985 (for Estonia: 01.03.2022)
To be amended: as of 11.10.2023 or later (Modernised Convention 108)

Summary: the 1st binding international instrument which
1. protects the individual against abuses which may accompany the collection and processing of personal data and
2. seeks to regulate at the same time the transfrontier flow of personal data
3. a slight change of focus after amendment in future: right to data protection as a facilitator of other fundamental rights and freedoms
Data protection: GDPR (EU)


Entry into force: 24.05.2016 (applied since: 25.05.2018)

Summary: the 1st directly applicable legal act on data protection in the EU which lays down
1. rules relating to the protection of natural persons with regard to the processing of personal data and
2. rules relating to the free movement of personal data
Data protection: DPLED (EU)

Full title: Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Entry into force: 05.05.2016 (deadline for national implementing acts 06.05.2018)

Summary:
1. protects citizens' (e.g. victims, witnesses, and suspects of crime) whenever personal data is used by criminal law enforcement authorities for law enforcement purposes
2. facilitates cross-border cooperation in the fight against crime and terrorism.
Constitutional / human rights: the Constitution (Estonia)

Full title: The Constitution of the Republic of Estonia

Entry into force: 03.07.1992 (later amended to allow Estonia to join the EU)

Summary:
1. The Republic of Estonia shall not enter into international treaties that are in conflict with the Constitution. The provisions of international treaties ratified by the Riigikogu will prevail in case of conflict with law and other legal acts of Estonia.
2. Estonia may belong to the European Union, provided that the fundamental principles of the Constitution are abided by.
Data protection: IKS (Estonia)

Full title: Personal Data Protection Act¹ (in Estonian Isikuandmete kaitse seadus¹)

Entry into force: 15.01.2019

Summary:
1. functions as the national implementing law of GDPR and DPLED
2. lays out the rules for national data protection supervision (Estonian Data Protection Inspectorate)
3. defines liability for infringing data protection law
Main focus of this course: GDPR
Data protection: GDPR (EU)

GDPR does not apply:
1) in the area covered by the DPLED (criminal offences, law enforcement)
2) activities which fall outside the scope of EU law, such as activities concerning national security
3) Member States carrying out activities in relation to the common foreign and security policy of the EU
4) processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity.*

− Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities.

* GDPR applies to controllers or processors which provide the means for processing personal data for such personal or household activities (e.g. Facebook, Google providing the means for chatting between people, emailing between people etc).
Main terms and definitions
Objects

**Personal data** – any information relating to a *data subject* includes *genetic data, biometric data* and *data concerning health*, which are defined separately.

**Anonymous information** –

a) information which does not relate to an identified or identifiable natural person or

b) personal data rendered anonymous in such a manner that the *data subject* is not or no longer identifiable

GDPR and its data protection principles **do not apply to anonymous information.**
GDPR PERSONAL DATA

The EU's General Data Protection Regulation defines personal data as any information related to a person that can be used to directly or indirectly identify them, including:

- Name
- Location data
- Physical attributes
- Online identifiers (including an IP address)
- An identification number
- Health information
- Economic, cultural or social identity of a person

Source: https://searchdatamanagement.techtarget.com/answer/What-is-included-in-the-GDPR-definition-of-personal-data
Actors

Data subject – an identified or identifiable natural person

Identifiable – 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;

Controller – somebody who, alone or jointly with others, determines the purposes and means of the processing of personal data

Processor – somebody who processes personal data on behalf of the controller(s)
Actors: joint controllership – recent case law

05.06.2018 Wirtschaftsakademie C-210/16 (European Court of Justice)
Recognising the joint controllership of Facebook and an administrator of a fan page hosted on Facebook in relation to the processing of personal data of visitors to that fan page (placing a cookie on the visitor’s device)

10.07.2018 Jehovah’s witnesses C-25/17 (European Court of Justice)
Recognising the joint controllership of a religious community and its preaching members in the context of door-to-door preaching organized, coordinated and encouraged by that community

29.07.2019 Fashion ID C-40/17 (European Court of Justice)
Recognising the joint controllership of Facebook and an operator of a website who embeds on that website a social plugin causing the visitor’s browser to request content from Facebook and to transmit personal data of the visitor to Facebook
Actors: joint controllership – how to recognise?

1. **type of entity** (“natural or legal person, public authority, agency or other body”)
2. **decisive influence** (“determines”)
   - Controller decides “essential means” (whose data, which data, for how long, who can access)
   - Processor can decide “non-essential means” (choice of hard- or software, detailed security measures)
3. **pluralistic control** (“alone or jointly with others”)
   - not all controllers are required to have access to the data (Wirtschaftsakademie p 38, Jehovah’s witnesses p 75)
   - the processing by each party is inseparable, i.e. inextricably linked (processing would not be possible without both party’s participation)
4. **why and how data is processed** (“the purposes and means”)
5. **operating with personal data** (“of the processing of personal data”)
   - no need to actually have access to the data that is being processed (Wirtschaftsakademie p 38)
Activities

**Processing** – any operation or set of operations which is performed on *personal data* or on sets of *personal data*, whether or not by automated means
e.g. *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.

In other words, **anything can be processing**.
Activities

Pseudonymisation – the *processing of personal data* in such a manner that
1. the *personal data* can no longer be attributed to a *specific data subject* without the use of additional information,
2. provided that such additional information is
   – kept separately and
   – is subject to technical and organisational measures to ensure that the *personal data* are not attributed to an identified or identifiable natural person

Pseudonymised information (the output of pseudonymisation) is *still considered personal data* (information relating to identifiable natural person).
Activities

Anonymisation – not defined in GDPR. GDPR only mentions “rendering personal data anonymous” in Recital 26.

However, anonymisation or otherwise rendering personal data anonymous is still considered a type of processing because it uses personal data as input.
Processing which does not require identification

If the controller does not or no longer require(s) the identification of a data subject for the purposes of processing, it may stop doing it.

GDPR Art 11 releases the controller of the obligation to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

If the controller is able to demonstrate that it is not in a position to identify the data subject, it must inform the data subject accordingly, if possible. In such cases, certain data subject rights do not apply anymore.
Individual exercise: 1

Read the Privacy Policy of HOIA app:
https://hoia.me/en/privacy/

1. Who is the controller, who is the processor?
2. What data is being processed?
3. Does it require identification of the data subject?
Data protection principles
Data protection principles (1/3)

Personal data shall be
1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’)
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’)
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)

TBC on next slide...
Data protection principles 2/3

Personal data shall be

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’)

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’)

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).
Data protection principles (3/3)

7. The controller shall be responsible for, and be able to demonstrate compliance with all the other 6 data protection principles (‘accountability’).
Data protection principles: lawfulness (1/5)

Any processing of personal data requires a legal basis to be lawful. Such legal basis can be:

(a) the data subject’s **consent** to the processing,

(b) stipulated in **law**:
- national law
- EU law
- international law.
Data protection principles: lawfulness (2/5)

Consent – any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Consent can be withdrawn. Data subject has the right to withdraw the consent at any time. It shall be as easy to withdraw as to give consent.

When in writing, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
GDPR provides a closed list of possible grounds of law, when processing of personal data is justified:

1. contract with the data subject
2. controller’s legal obligation*
3. vital interests of the data subject or of another natural person
4. controller’s public interest task or exercise of official authority vested in the controller*
5. purposes of the legitimate interests pursued by the controller or by a third party, exceptions:
   - public authorities in the performance of their tasks
   - when overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data

* requires specification in EU or national law
Data protection principles: lawfulness (4/5)

Processing of special categories of personal data is prohibited.

Special categories of personal data covers:
- revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,
- genetic data, biometric data for the purpose of uniquely identifying a natural person,
- data concerning health
- data concerning a natural person's sex life or sexual orientation
Exceptions to the prohibition to process special categories of personal data:

a) data subject has given explicit consent (may be prohibited by law)
b) in the field of employment and social security and social protection law
c) to protect the vital interests of the data subject or of another natural person
d) in the course of legitimate activities of a not-for-profit body with a political, philosophical, religious or trade union aim
e) personal data is manifestly made public by the data subject
f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
g) for reasons of substantial public interest
h) for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
i) for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health etc
j) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
Individual exercise 2

Read the Privacy Policy of HOIA app: [https://hoia.me/en/privacy/](https://hoia.me/en/privacy/)

1. Which processing operations does it cover?
2. What is the legal basis of processing?
Data subject rights
Data subject rights

1) Right to receive information (GDPR Art 12-14)
2) Right of access by the data subject (GDPR Art 15)
3) Right to rectification (GDPR Art 16)
4) Right to erasure (‘right to be forgotten’) (GDPR Art 17)
5) Right to restriction of processing (GDPR Art 18)
6) Right to data portability (GDPR Art 20)
   - applies only if data is provided under a consent or contract
7) Right to object (GDPR Art 21)
   - applies only in case of controller’s public interest task/exercise of official authority, for
   purposes of the legitimate interests, scientific/historical research or statistical purposes
8) Right not to be subject to a decision based solely on automated processing, including profiling (GDPR Art 22)
Data controller obligations
Controller’s obligations (1/4)

As we saw above, the controller is responsible for ensuring and demonstrating compliance with all data protection principles (data protection principle of accountability):

1. lawfulness, fairness and transparency
2. purpose limitation
3. data minimisation
4. accuracy
5. storage limitation
6. integrity and confidentiality

How does the GDPR nudge the controller into doing that?
Controller’s obligations (2/4)

Obligation to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR (GDPR Art 24)
– This is where privacy-preserving technologies come to play!

Obligation to abide by principles of data protection by design and by default (GDPR Art 25) – key to implementing data protection principles:
1. Data protection by design – implement appropriate technical and organisational measures designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing
2. Data protection by default – ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. In particular, personal data must not be made accessible without the individual's intervention to an indefinite number of natural persons.
Controller’s obligations (3/4)

Obligation to **ensure a level of security appropriate to the risks** presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed (GDPR Art 32).
− This is were privacy-preserving technologies come to play!

Obligation to **notify a personal data breach to the supervisory authority** without undue delay (max 72h, where feasible) after having become aware of it, unless it is unlikely to result in a risk to the rights and freedoms of natural persons. Notification of data subjects required only in case of high risk!

**Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data which is being processed.
Controller’s obligations (4/4)

Obligation to carry out a **data protection impact assessment** prior to the processing, if a type of processing is likely to result in a high risk to the rights and freedoms of natural persons (e.g. due to using new technologies), account has to be taken of the nature, scope, context and purposes of the processing (GDPR Art 35).

Must contain:
(a) a systematic description of the envisaged processing operations and the purposes of the processing,
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes,
(c) an assessment of the risks to the rights and freedoms of data subjects,
(d) the measures envisaged to address the risks.
Transfer of personal data
Definition of transfer

The term „transfer“ is not defined in GDPR.


The EDPB Guideline referred above is used as basis for this section of the lecture. NB! Please seek out for an updated version in the future.
The purpose of GDPR rules on transfer (GDPR Chapter V) is to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data are transferred outside the EU or to international organisations (United Nations, Red Cross etc).

When personal data is transferred and made accessible to entities outside the EU territory, the overarching legal framework provided within the EU no longer applies. Therefore, the transferred personal data has to be protected in other ways.
Ways of protection outside the EU territory

A transfer of personal data to a third country or an international organisation may take place where:

1. **adequacy decision by the European Commission** – the Commission has decided that the third country or the international organisation in question ensures an adequate level of protection;

2. **appropriate safeguards** – the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available (see the next slide for details);

3. **derogations for specific situations**
   - data subject consent, contract with or in the interest of the data subject, important reasons of public interest, legal claims, vital interests of the data subject or others, transfer from a publicly available registry, ad hoc transfer for compelling legitimate interest (informing the national supervisory authority and the data subject).
Appropriate safeguards

The appropriate safeguards may be provided for by:

a) a legally binding and enforceable instrument between public authorities or bodies,
b) binding corporate rules (GDPR Art 47),
c) standard data protection clauses adopted by the European Commission or by a national supervisory authority and approved by the European Commission (GDPR Art 93(2)),
d) an approved code of conduct (GDPR Art 40),
e) an approved certification mechanism (GDPR Art 42),
f) subject to authorization from the national supervisory authority (GDPR Art 46(3)(b)):
   - contractual clauses between EU controller/processor and non-EU controller/processor/recipient
   - provisions to be inserted into administrative arrangements between public authorities or bodies
Thank you!

cybernetica
CyberneticaAS
cybernetica_ee
Cybernetica

Triin Siil
triin.siil@cyber.ee
cyber.ee