BECCLE

BERGEN CENTER FOR COMPETITION LAW AND ECONOMICS

Graduate AI Ethics
"Privacy and the law. The GDPR"

Associate professor Malgorzata Cyndecka, PhD

www.beccle.no
post@beccle.uib.no

UNIVERSITY OF BERGEN

NHH

What shall we focus on?

- The objectives of Regulation (EU) 2016/679 (GDPR)
- Notion of personal data, special categories of personal data, processing of personal data
- Material and territorial scope of application of the GDPR
- Who is who?
- Principles relating to processing of personal data
- Legal basis for processing of personal data
- Rights of data subjects
- The GDPR as a risk-based legal framework
- Enforcement and interpretation.

General Data Protection Regulation – EU/EEA

(EEA = EU + Norway, Iceland and Liechtenstein)

- Repealed Data Protection Directive of 1995
- Regulation v Directive
- The Norwegian personopplysningsloven
- Rules on the protection of natural persons with regard to the processing of personal data AND and rules relating to the free movement of personal data (GDPR Art. 1)
  - "serve mankind"
  - "the right to the protection of personal data is not an absolute right"
  - "balanced against other fundamental rights, in accordance with the principle of proportionality (GDPR Recital 4).

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;* (GDPR Art. 4(1))

- **Any information – relating to – identified or identifiable – natural person**
- How to *express* personal data?
- Identified or that may merely be identified?
  - Registration number of a car?
- **Anonymous** data not covered by the GDPR, but… AI's potential.

Special categories of personal data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. (GDPR Art. 9(1))

- Race?
- Genetic, biometric, health data – defined by the GDPR
- Previously referred to as **"sensitive".**

Why important to distinguish special categories of personal data from «ordinary» personal data?

- **Higher risk** for **negative consequences**, thus much stricter requirements and responsibility when processing such personal data
  - For example, processing requires an **additional legal basis**
- **"Explicit" and "inferred" special categories of personal data – AI's potential.**

Processing of personal data

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*. (GDPR Art. 4(2))

- **NB! ALSO collection, erasure or destruction.**

Material scope – what is covered by the GDPR?

The processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system *(Art. 2(1)).*

> ***Filing system*** **-** *any* ***structured set*** *of personal data which are* ***accessible according to specific criteria****, whether centralised, decentralised or dispersed on a functional or geographical basis* (Art. 4(6)).
>
> **Can you search for specific data according to certain criteria or not?**

Processing of personal data NOT covered by the GDPR

- In the course of activities such as national security, common foreign and security policy
- Law enforcement activities (e.g. police when investigating, detecting or prosecuting criminal offences)
- EU institutions are covered by own Regulation (EC) No 45/2001
- Activities covered by e-Commerce Directive
- **By a natural person in the course of a purely personal or household activity.**

Territorial scope – where does the GDPR apply? (GDPR Art. 3)

1. **Controller or a processor established in the EU/EEA, regardless of whether the processing takes place in the EU/EEA**

2. The processing of personal data of **data subjects who are in the EU/EEA** by a **controller or processor not established in the EU/EEA**, where the controller or processor:

(a) offers goods or services (payment not required) **data subjects in the EU/EEA**

(b) monitors their behaviour that takes place in the EU/EEA

TARGETING CRITERION!

3. EU/EEA Member States' embassies and consulates located outside the EU/EEA.

Who is who?

THE MOST IMPORTANT ACTORS

(THERE ARE MORE)

Controller

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****;*

This may also be decided by Union or Member State law.

- **Responsible for compliance with the GDPR**
  - Liability, fines etc.
- **Must demonstrate such compliance (document!)**
- Joint controllers
  - Facebook "like" buttons.

Processor

a natural or legal person, public authority, agency or other body which ***processes personal data on behalf of the controller*** (GDPR Art. 4(8)).

- A **separate entity**
- Agreement between the controller and the processor.

Data subject

- **(EVERY) natural person in the EU/EEA**
- The GDPR's territorial scope
- *Paradox?*
- Still, right to know about being data subject
- Rights of data subjects – **KNOW YOUR RIGHTS!**

Principles relating to processing of personal data

- **Pillars or foundations of data protection**
- **Every processing** of personal data must comply with those principles
- Decide on how **the GDPR should be interpreted**
- **Not precise and leave room for interpretation**
- Often must be **balanced against each other**.

Principles relating to processing of personal data

GDPR Art. 5(1) – data protection principles:

a) **Lawfulness, fairness and transparency**

b) **Purpose limitation**

c) **Data minimisation**

d) **Accuracy**

e) **Storage limitation**

f) **Integrity and confidentiality**

GDPR Art. 5(2)

- **Accountability.**

Processing of personal data shall be

- **Lawful**
  - The GDPR (in particular, legal basis) as well as EU law and national law
- **Fair**
  - Data subject's expectations, non-discrimination, power (im-)balance, ethical
- **Transparent**
  - Not surprising, information, trust, compliance with the GDPR.

Processing of personal data shall comply with the principles of

- **Purpose limitation**
  - Specified, explicit and legitimate purposes
  - Crucial to other principles and processing
  - Repurposing is limited
- **Data minimisation**
  - Adequate, relevant and limited to what is necessary
  - Quality and quantity
- **Accuracy**
  - Accurate, updated, quality – erase or rectify.

Processing of personal data shall comply with the principles of

- **Storage limitation**
  - As a rule, no longer than necessary for the given purpose
  - Longer if solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
- **Integrity and confidentiality**
  - Security
- **Accountability**
  - The controller responsible for and able to demonstrate compliance.

Every processing of personal data requires a legal basis

GDPR Art. 6(1) – «ordinary» personal data

a) **Consent**

Processing necessary for:

b) Contract

c) Controller's legal obligation

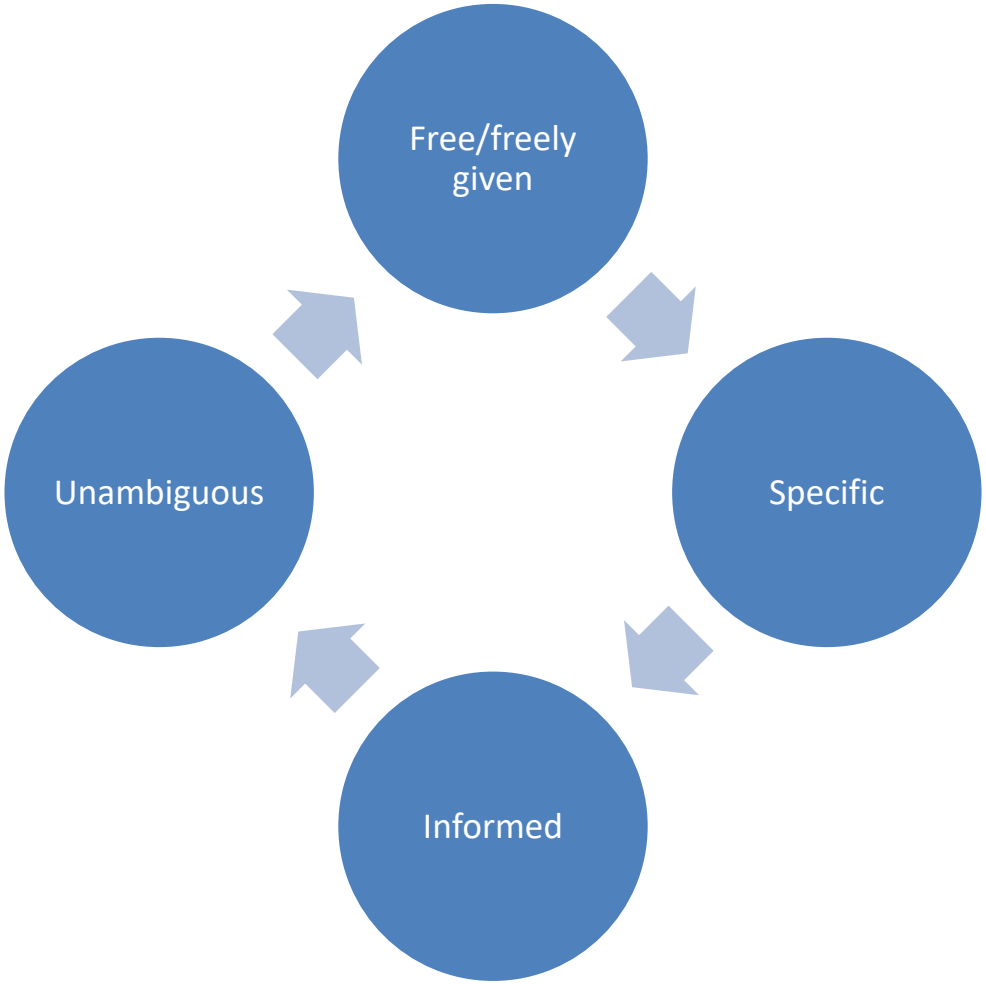
d) Protect vital interests

e) Task in public interest or exercise of official authority

f) Legitimate interest

If **special categories of personal data**, in addition a legal basis under GDPR Art. 9(2)! e.g. explicit consent.

Elements of valid consent



Rights of data subjects

- Right to **information** when our personal data are collected from us or from other source (GDPR Art. 13 and 14)
- Right of **access** (GDPR Art. 15)
- Right to **rectification** (GDPR Art. 16)
- Right to **erasure («right to be forgotten»)** (GDPR Art. 17)
- Right to **restriction** of processing (GDPR Art. 18)
- Right to **data portability** (GDPR Art. 20)
- Right to **object** (GDPR Art. 21)
- **Right not to be subject to a decisions based solely on automated processing (GDPR Art. 22) - AI**

A risk-based approach to data protection

- **NO requirement of NO RISK, but...**
- The **controller** must assess, mitigate and reduce risk to an acceptable level
- **Before the processing and underway**
- Implement **appropriate technical and organisational measures**
- **Data protection by design and default**
- If the processing poses **high risk: carry out a Data protection impact assessment (DPIA)**
- Data protection authority (in Norway: Datatilsynet).

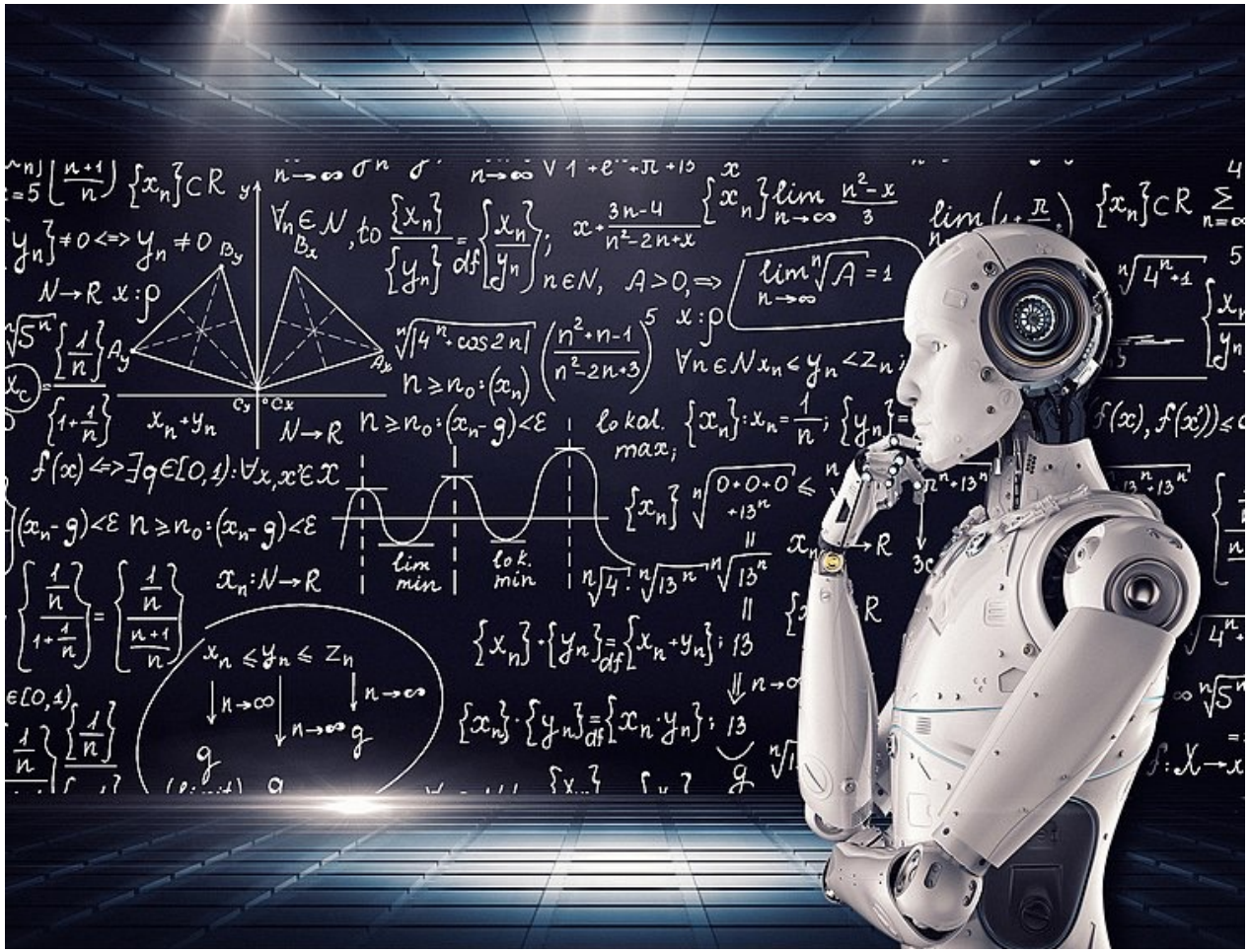
Enforcement of the GDPR and its interpretation

- **Data protection authorities in EU/EEA Member States**
- Tasks from monitoring, advising, promoting awareness and understanding the risks to handling of complaints, investigation, issuing warnings and imposing administrative fines
- **Fines: in case of an undertaking (company) up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher**
- Cross-border processing – lead supervisory authority
- **European Data Protection Board (EDPB)** – general guidance, opinions, binding decisions.

Would you like to more know about the relation between the GDPR and AI?

- **The impact of the GDPR on artificial intelligence**, Study by Panel for the Future of Science and Technology for the European Parliament, June 2020, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530
- AI is GDPR compliant, but …
- The GDPR provisions are vague and open-ended
- AI gets more complex
- The GDPR does not hinder AI, but we need more guidance to avoid risks and costs
- Datatilsynet: Sandbox for responsible AI: https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/ (see also ICO, CNIL).

Thank you for your attention!



Source:
https://www.flickr.com/photos/152824664@N07/30212411048/ Author: mikemacmarketing