Lecture: Introduction to Privacy, GDPR and Ethical Data Sharing

Dr. Irene Kamara, Assistant professor cybercrime law and human rights

ENCRYPT Hackathon: Data Readiness for Privacy-Preserving Technologies 31 March 2025

About us

- Located in the Netherlands
- Interdisciplinary department with around 80 staff: law, social sciences, computer science, psychology, economics
- Research on cross-cutting topics on regulating tech, legal and ethical implications
- Education:
  - LLM law & tech
  - Bachelor on global law
  - Professional learning programs: Cybersecurity governance, AI & law, Energy law
  - Master in Cybersecurity & AI

Tilt
Tilburg Institute for Law, Technology, and Society

Do people care about their online privacy?

"A large number of respondents said they are worried about cyber-attacks and cybercrime (56%), the safety and well-being of children in the online environment (53%), and the use of personal data and information by companies or public administrations (46%)"

Special Eurobarometer 518 Digital Rights and Principles (2021)

"Over a third of respondents (39%) indicate being unaware that the rights that apply offline should also be respected online. In some EU countries, more than half of the respondents think this way, while older persons are less aware of this (e.g. 49% of those surveyed in the age group 55+)."

Special Eurobarometer 518 Digital Rights and Principles (2021)

Is there a "Privacy Paradox"?

→or else: why do people share their personal information online and don't protect their systems? (e.g. use "12345" as password?)

- "difficult to associate a specific value to their privacy and therefore, the value of protecting it"*
- people lack awareness of their rights.
- people lack awareness of collection of information.
- people lack awareness of potential harm and impact.

*https://theconversation.com/the-privacy-paradox-we-claim-we-care-about-our-data-so-why-dont-our-actions-match-143354

Tilburg Institute for Law, Technology, and Society

PROTECTION OF PERSONAL DATA & PRIVACY: 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.

3. Compliance with these rules shall be subject to control by an independent authority.

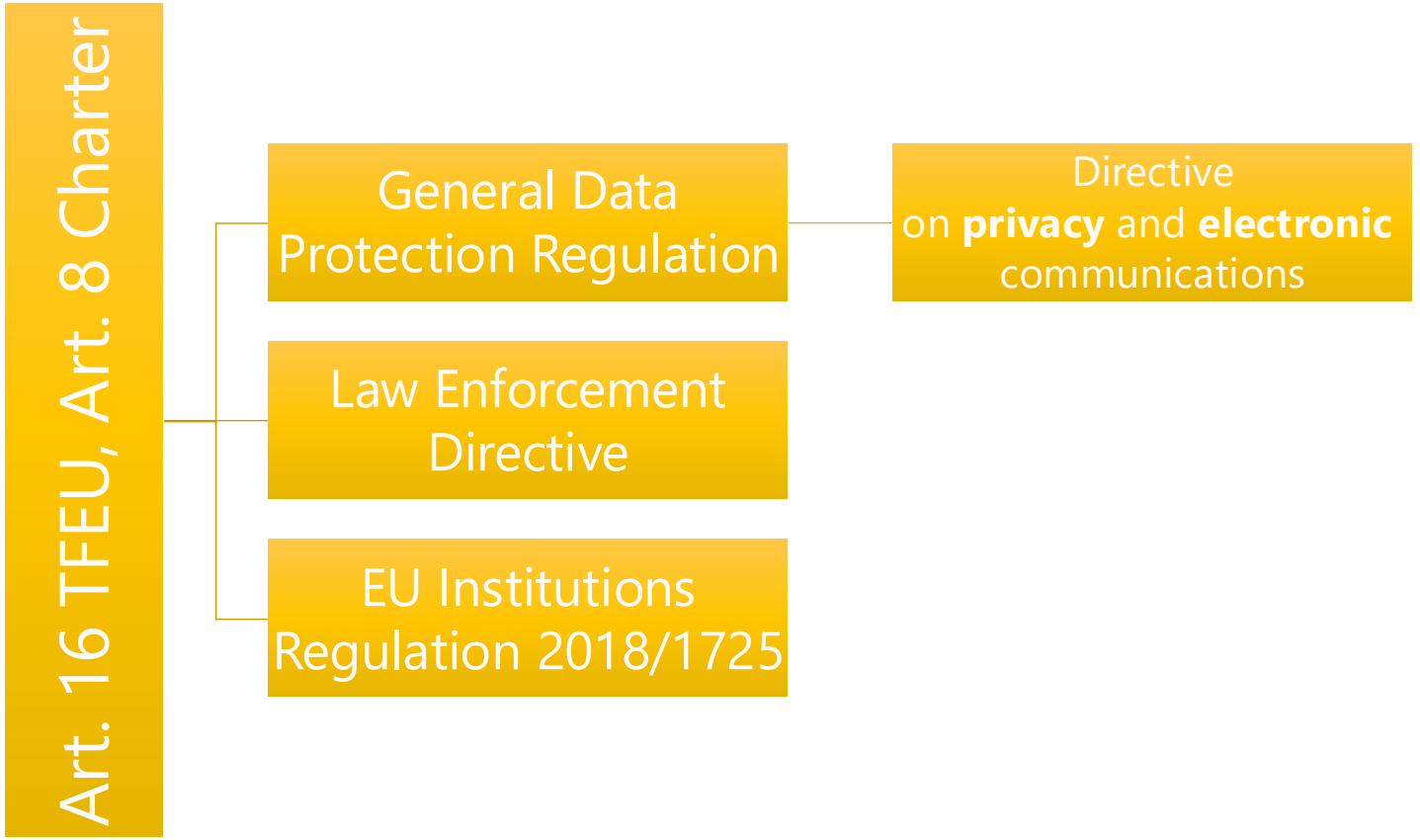
Charter fundamental rights EU

Outline

- General Data Protection Regulation: overview
- What is personal data?
- Key principle #1: purpose limitation
- Key principle #2: data minimisation
- Pseudonymisation v anonymisation
  - What is pseudonymisation in the GDPR?
  - 10 misunderstandings about anonymisation

Tilburg Institute for Law, Technology, and Society

Overview of personal data protection EU law



EU DATA PROTECTION LAW: GDPR

- Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) • **GDPR**

- **Directly applicable to all Member States**
- **99 Articles**
- **Started applying in 2018**
- **Applies to both private and public sector**
- **Persons responsible to comply: natural and legal persons**
- **Only natural persons (=individuals) protected**
- **Applies to *processing* of personal data**

KEY CONCEPTS: PERSONAL DATA

- Indirect identifiability example:
- A person can be singled-out,
- e.g. based on car registration number, national insurance number, passport number, or
- a combination of significant criteria (eg age, occupation, place of residence).

- Art. 4(1) '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

Tilburg Institute for Law, Technology, and Society

Indirect identifiability: example

A business uses Wi-Fi analytics data to count the number of visitors per hour across different retail outlets. It is not necessary to know whether an individual has visited an individual store (or multiple stores) before. This involves the business processing the Media Access Control (MAC) addresses of mobile devices that broadcast probe requests to its public Wi-Fi hotspots. MAC addresses are intended to be unique to the device (although they can be modified or spoofed using software).
If an individual can be identified from that MAC address, or other information in the possession of the network operator (the business, in this example), then the data is personal data. Additionally, even if the business does not know the name of the individual, using a MAC address (or other unique identifier) to track a device with the purpose of singling out that individual or treating them differently means the data is also personal data.

Source: ICO – UK Information Commissioner

Can you think of examples?

Personal data

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone);
- an Internet Protocol (IP) address;
- a cookie ID;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

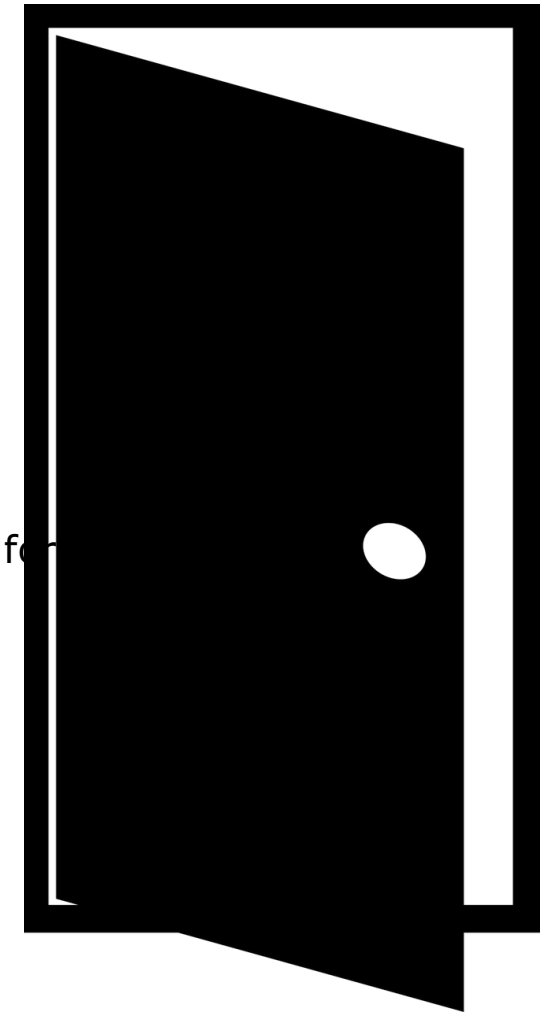
Non-personal data

- a company registration number;
- an email address such as info@company.com;
- anonymised data.

Source: European Commission

Special categories of data

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used f
identification purposes);
- health data;
- sex life; or
- sexual orientation.



Main principles

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security)
- Accountability.

Art. 5 General Data Protection Regulation

Purpose limitation principle

"Personal data shall be:
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes." art. 5(1)(b) GDPR

Purpose limitation principle: checklist

- ✓ We have clearly identified our purpose or purposes for processing.
- ✓ We have documented those purposes.
- ✓ We include details of our purposes in our privacy information for individuals.
- ✓ We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.
- ✓ If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose or we get specific consent for the new purpose.

Source: ICO

Data minimisation principle

- The principle of “data minimisation” means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it.
- The data minimisation principle is expressed in Article 5(1)(c) of the GDPR: personal data must be ”adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”

Tilburg Institute for Law, Technology, and Society

Data minimisation principle checklist

- ✓We only collect personal data we actually need for our specified purposes.
- ✓We have sufficient personal data to properly fulfil those purposes.
- ✓We periodically review the data we hold, and delete anything we don't need.

Source: ICO

GROUNDS FOR LAWFUL PROCESSING

- Consent
- Contract
- Legal obligation of controller
- Vital Interest of data subject
- Performance of a task in Public Interest
- Legitimate interest

Art. 5 General Data Protection Regulation

PERSONAL DATA, PSEUDONYMOUS AND ANONYMOUS DATA

- Truly **anonymous** data are not personal data
  - what's the consequence? GDPR does NOT apply.
- **Pseudonymous** data are personal data
- Art. 4(5): '**pseudonymisation**' means the processing of personal data in such a manner that the personal data can **no longer** be attributed to a **specific data subject without the use of additional information**, 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;

Pseudonymisation: example

A courier firm processes personal data about its drivers' mileage, journeys and driving frequency. It holds this personal data for two purposes:

- to process expenses claims for mileage; and
- to charge their customers for the service.

For both of these, identifying the individual couriers is crucial.

However, a second team within the organisation also uses the data to optimise the efficiency of the courier fleet. For this, the identification of the individual is unnecessary.

Therefore, the firm ensures that the second team can only access the data in a form that makes it not possible to identify the individual couriers. It pseudonymises this data by replacing identifiers (names, job titles, location data and driving history) with a non-identifying equivalent such as a reference number which, on its own, has no meaning.

The members of this second team can only access this pseudonymised information.

Whilst the second team cannot identify any individual, the organisation itself can, as the controller, link that material back to the identified individuals.

Source: ICO

EDPB 2025 Guidance on pseudonymisation

Three steps:

1. modify or transform the personal data.
2. keep additional information for attributing the personal data to a specific data subject separately, i.e. separate from those who are to be prevented from achieving such an attribution.
3. Apply technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf

ANONYMISATION: 10 MISUNDERSTANDINGS

1. **´Pseudonymisation is the same as anonymisation´**

--> Fact: pseudonymisation is NOT the same as anonymisation

2. **´Encryption is anonymisation´**

--> Encryption is not anonymisation, but a powerful pseudonymisation technique´ why? Because the original information needs to be accessible and decryption is possible.

Q: what if the decryption key is deleted? ¨One cannot assume that encrypted data cannot be decrypted because the decryption key is said to be "erased" or "unknown". ¨

3. **´Anonymisation of data is always possible´**

--> It is not always possible to lower the re-identification risk below a previously defined threshold whilst retaining a useful dataset for a specific processing.

https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf

ANONYMISATION: 10 MISUNDERSTANDINGS II

- **4. ´Anonymisation is forever´**
- --> Risk that some anonymisation processes could be reverted in the future. E.g. new technical developments and the availability of additional information might compromise previous anonymisation processes.
- **5. "Anonymisation always reduces the probability of re-identification of a dataset to zero"**
- --> The anonymisation process and the way it is implemented will have a direct influence on the likelihood of re-identification risks.
- **6. ´Anonymisation is a binary concept that cannot be measured´**
- --> It is possible to analyse and measure the degree of anonymization

Except for specific cases where data is highly generalised (e.g. a dataset counting the number of visitors of a website per country in a year), the re-identification risk is never zero.

Tilburg Institute for Law, Technology, and Society

ANONYMISATION: 10 MISUNDERSTANDINGS III

- **7. ´Anonymisation can be fully automated´**
- --> Automated tools can be used during the anonymisation process, however, given the importance of the context in the overall process assessment, human expert intervention is needed.
- **8. ´Anonymisation makes the data useless´**

  -->A proper anonymisation process keeps the data functional for a given purpose – but perhaps not for others (remember the GDPR principles?)

  9. ´Following an anonymisation process that others used successfully will lead our organisation to equivalent results´

  --> Anonymisation cannot be applied akin to following a recipe, because the context (nature, scope, context and purposes of the processing of the data) are likely different from one circumstance to another

  10. ´No one cares to re-identify the persons in my dataset´

  --> Personal data has a value in itself, for the individuals themselves and for third parties. Re-identification of an individual could have a serious impact for his rights and freedoms. Motivations to re-identify: unintended errors/data breach, actual interest (e.g. scientific research, journalism or criminal activity), curiosity.

Tilburg Institute for Law, Technology, and Society

…HOWEVER…

- Recent case at the Court of Justice EU: C-413/23 - EDPS v SRB
- ---> Should pseudonymised data be included within that scope **automatically**, **irrespective of the accessibility of the additional identification data**, or should the data following the pseudonymisation process be considered personal data only for those persons who can reasonably identify the data subjects?

- The Advocate General opined that:
- ´´pseudonymised data may fall outside the scope of the concept of 'personal data' but only where the risk of identification is non-existent or insignificant.´´

- Ruling is pending, but important to keep an eye on the developments!

https://curia.europa.eu/juris/document/document.jsf?text=&docid=295078&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=28933701#Footnote2

Tilburg Institute for Law, Technology, and Society

WWW.TILT.NL

i.kamara@tilburguniversity.edu

Tilburg University

Understanding Society