

EU Data Protection Law: Fundamentals of the Legal Framework

17.06.2026



Isabela Maria Rosal



isa.rosalsantos@kuleuven.be



Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Academy of European Law. Neither the European Union nor the granting authority can be held responsible for them.

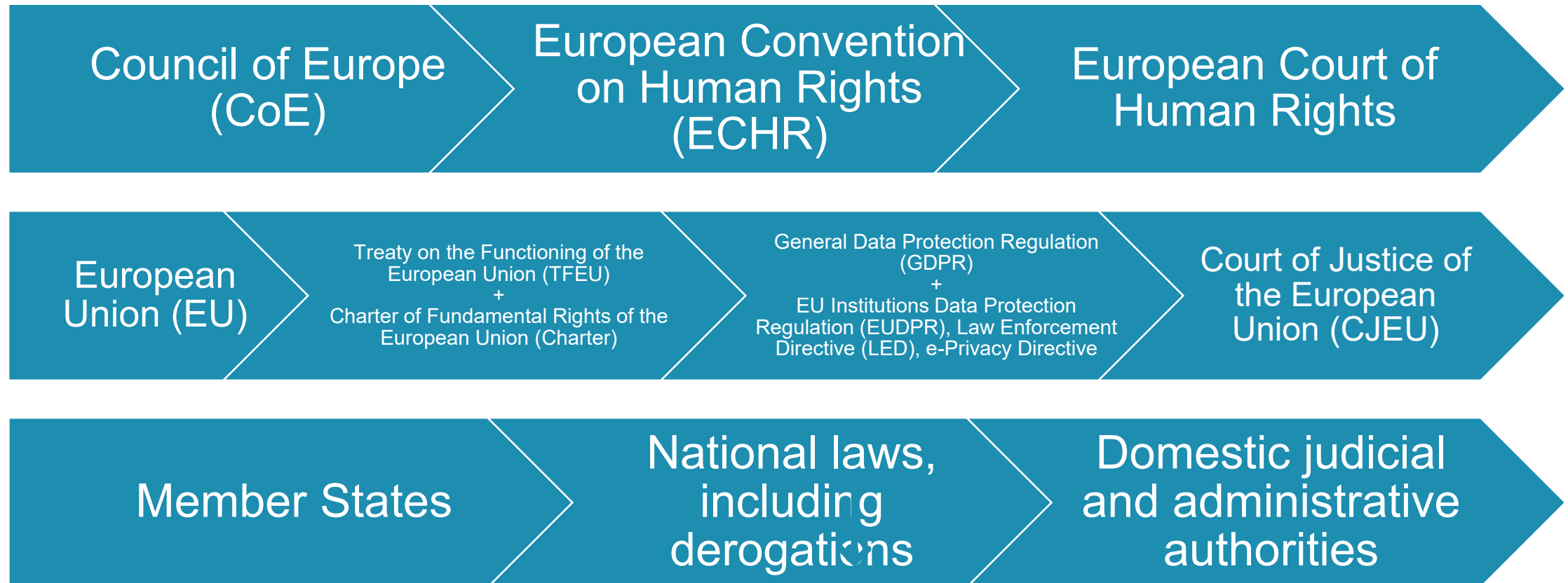
Overview of today's activity

Legal framework

GDPR: scope and key definitions

Data Protection Principles

Legal framework



Soft law: Article 29 Working Party (WP29), European Data Protection Board (EDPB), European Data Protection Supervisor (EDPS), European Union Agency for Cybersecurity (ENIS)

GDPR

Scope and key concepts



GDPR Scope

Article 2

Material scope

1. This Regulation applies to 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.
2. This Regulation does not apply to the processing of personal data:
 - (a) in the course of an activity which falls outside the scope of Union law;
 - (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
 - (c) by a natural person in the course of a purely personal or household activity;
 - (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
 - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
 - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

GDPR Scope: what is personal data?

For the purposes of this Regulation:

- (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;

BA500184



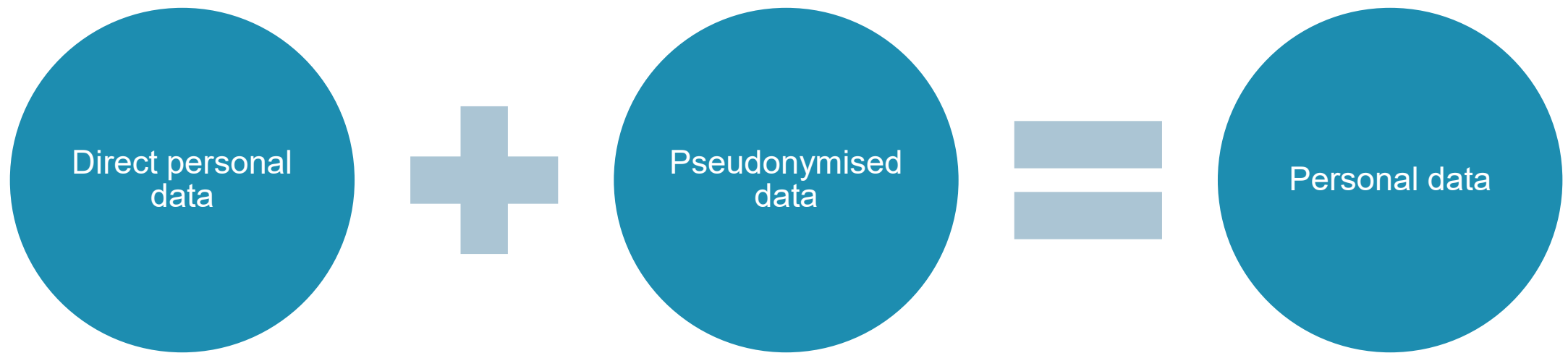
"You wear it on your wrist and it hacks—I mean, tracks—all your personal data."

GDPR Scope: what is personal data?



GDPR does **not** apply

GDPR Scope: what is personal data?



GDPR does apply

GDPR Scope: what is personal data?

Identifiability test

Recital 26 GDPR: The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. **To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.** To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. **The principles of data protection should therefore not apply to anonymous information**, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

GDPR Scope: what is personal data?

JUDGMENT OF THE COURT (Second Chamber)

19 October 2016 (*)

(Reference for a preliminary ruling — Processing of personal data — Directive 95/46/EC — Article 2(a) — Article 7(f) — Definition of 'personal data' — Internet protocol addresses — Storage of data by an online media services provider — National legislation not permitting the legitimate interest pursued by the controller to be taken into account)

In Case C-582/14,

REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 28 October 2014, received at the Court on 17 December 2014, in the proceedings

Patrick Breyer

v

Bundesrepublik Deutschland,

CJEU, Case C-582/14, Breyer v. Deutschland, 19 October 2016, ECLI:EU:C:2016:779

GDPR Scope: what is personal data?

Anonymous vs. pseudonymous data: the CJEU reaffirms the relative approach to the concept of personal data

BY [DANIELA SPAJIĆ](#) - 13 JUNE 2023

On 26 April 2023, the General Court of the European Court of Justice (CJEU) issued a judgment on the anonymisation of personal data. This blogpost discusses the decision in the case [SRB v. EDPS \(Case T-557/20\)](#), where the General Court provided another take on anonymising and pseudonymising personal data in the context of data sharing. | [SHARE THIS POST](#)

[Blog post](#) and [decision](#)

OPINION OF ADVOCATE GENERAL
SPIELMANN
delivered on 6 February 2025 (1)

Case C-413/23 P

**European Data Protection Supervisor
v
Single Resolution Board**

(Appeal – Processing of personal data – Procedure for granting compensation to creditors and shareholders following the resolution of a bank – Obligation to provide information – Article 15(1)(d) of Regulation (EU) 2018/1725 – Failure to inform those creditors and shareholders as regards the recipient of the personal data – Decision of the European Data Protection Supervisor finding an infringement of Regulation 2018/1725 in relation to the processing of pseudonymised personal data)

[Opinion](#)

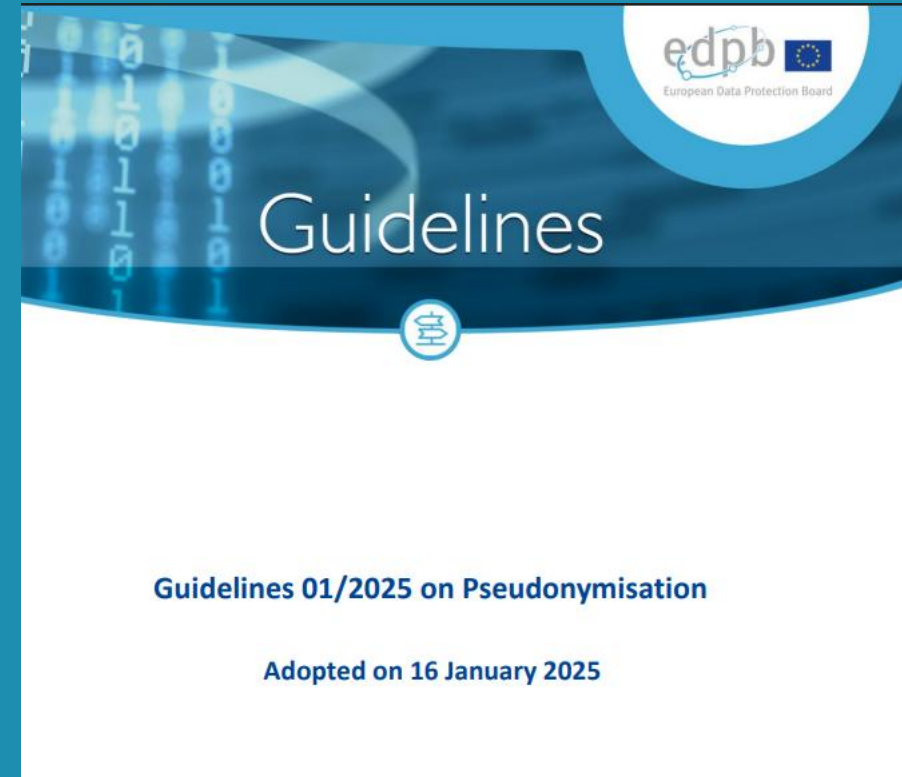
GDPR Scope: what is personal data?

[Blog post](#)

The EDPB 01/2025 Guidelines on Pseudonymisation: A Step in the Right Direction?

This post reviews EDPB 01/2025 Guidelines on Pseudonymisation. It stresses the importance of the pseudonymisation domain for risk assessment and highlights a few definitional inconsistencies. It also shows how the Guidelines can be read in the light of recent CJEU case law.

by Sophie Stalla-Bourdillon



[EDPB Guidelines](#)

GDPR scope: what is processing?

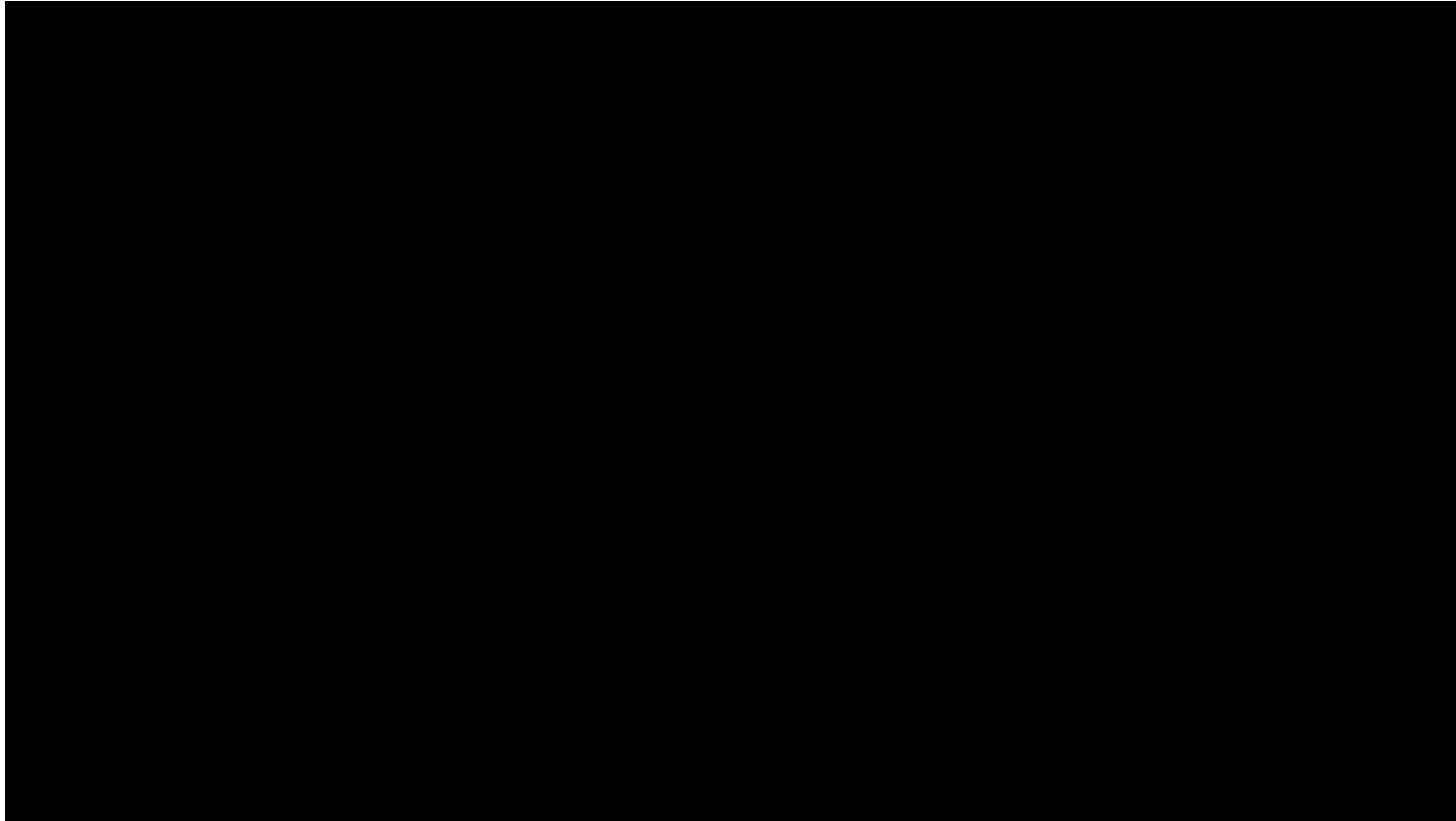
- (2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

GDPR scope: agents involved

- (7) ‘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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- (8) ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Joint controllership and the role of Data Processing Agreements

Personal data in new technologies: does the GDPR apply?



Personal data in new technologies: does the GDPR apply?

JUDGMENT OF THE COURT (Fourth Chamber)

11 December 2014 (*)

(Reference for a preliminary ruling — Directive 95/46/EC — Protection of individuals — Processing of personal data — Concept of ‘in the course of a purely personal or household activity’)

In Case C-212/13,

REQUEST for a preliminary ruling under Article 267 TFEU from the Nejvyšší správní soud (Czech Republic), made by decision of 20 March 2013, received at the Court on 19 April 2013, in the proceedings

František Ryneš

v

Úřad pro ochranu osobních údajů,

CJEU, Rynes v. Uad pro ochranu osobnich udaju,
11December 2014, ECLI:EU:C:2014:2428

JUDGMENT OF THE COURT (Third Chamber)

11 December 2019 (*)

[Text rectified by order of 13 February 2020]

(Reference for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Charter of Fundamental Rights of the European Union — Articles 7 and 8 — Directive 95/46/EC — Article 6(1)(c) and Article 7(f) — Making the processing of personal data legitimate — National legislation allowing video surveillance for the purposes of ensuring the safety and protection of individuals, property and valuables and for the pursuit of legitimate interests, without the data subject’s consent — Installation of a video surveillance system in the common parts of a residential building)

In Case C-708/18,

REQUEST for a preliminary ruling under Article 267 TFEU from Tribunalul București (Regional Court, Bucharest, Romania), made by decision of 2 October 2018, received at the Court on 6 November 2018, in the proceedings

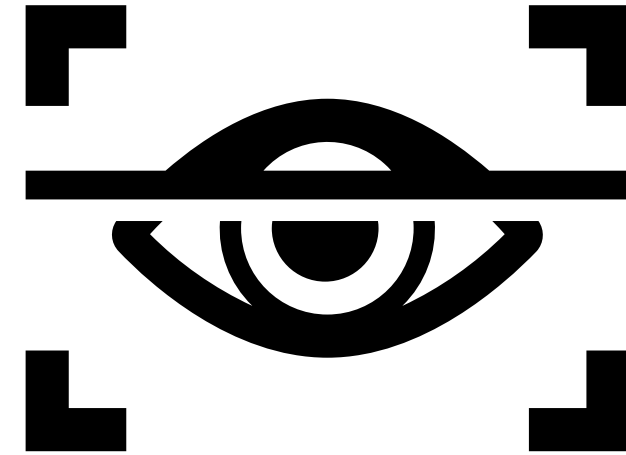
TK

v

Asociația de Proprietari bloc M5A-ScaraA,

CJEU, TK v. Asociatia de Proprietari, 11 December 2019,
ECLI:EU:C:2019:1064

Who is who? Focus on context + data processing agreement



Security company

More in the afternoon session

Principles

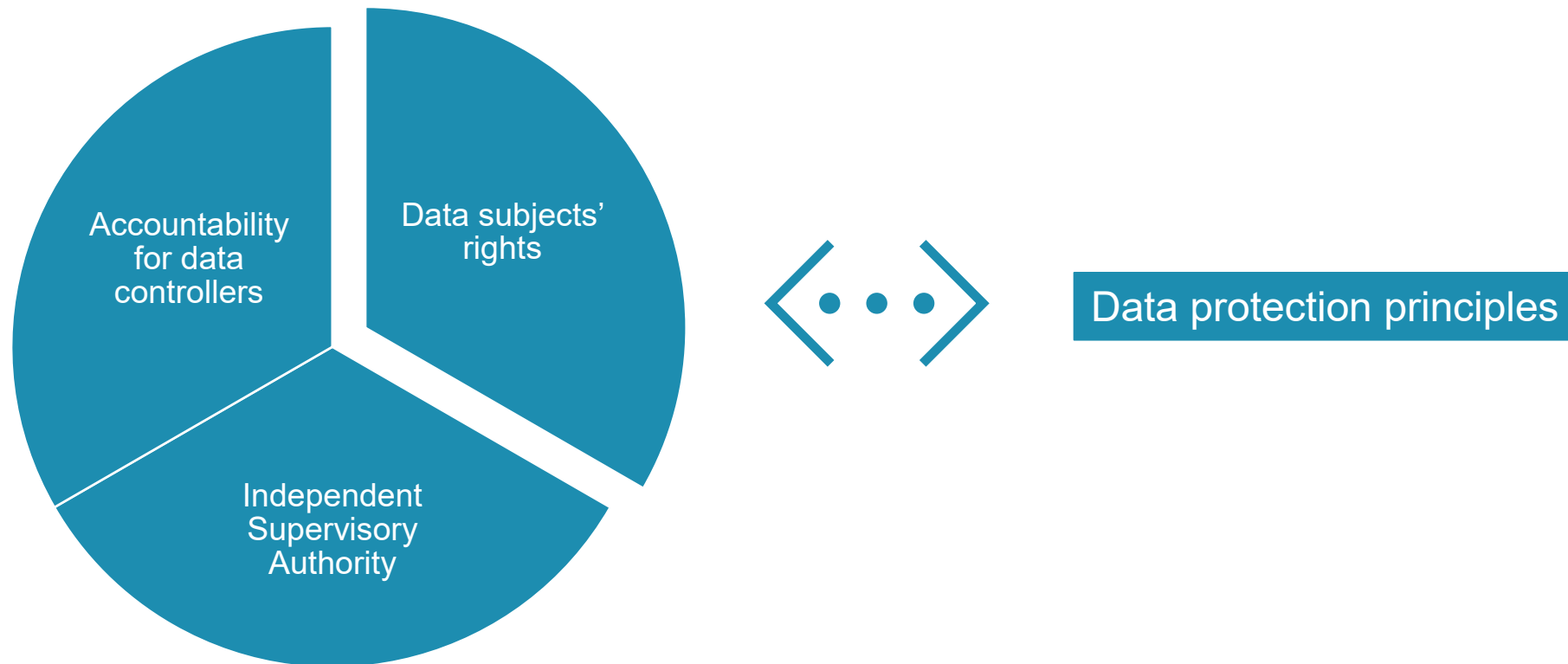


Structure of the fundamental right



Recital 11 GDPR Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

Structure of the fundamental right



Lawfulness

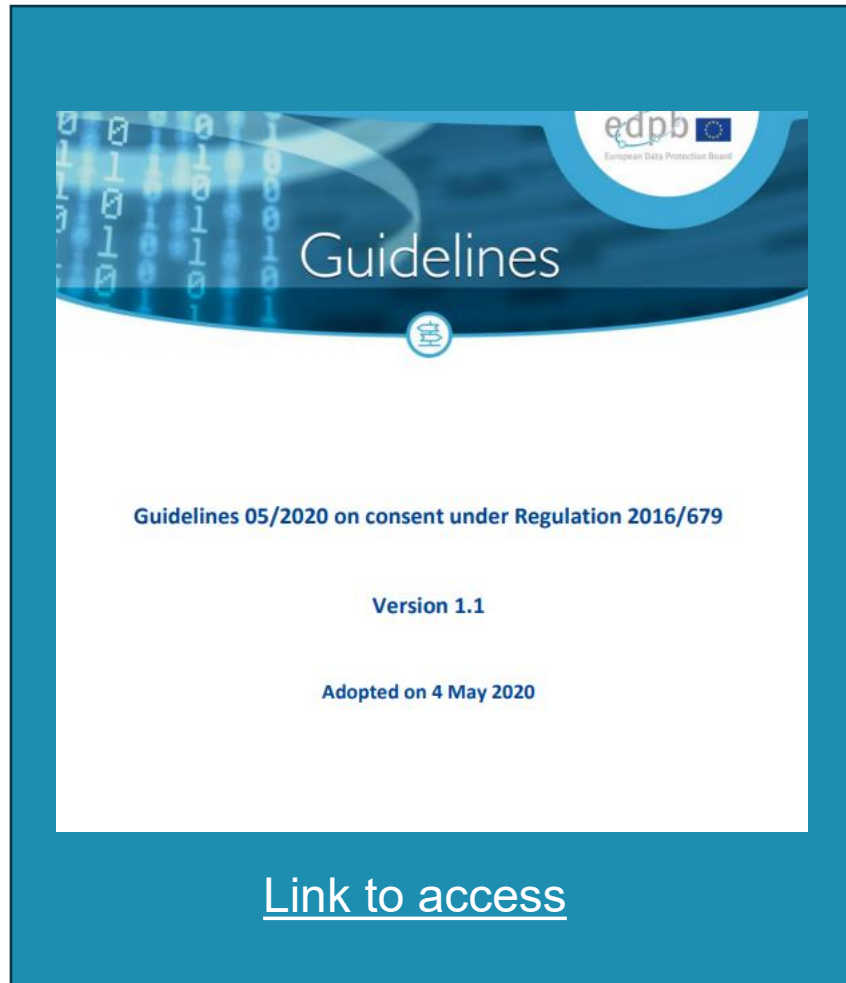
Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
 - (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
 - (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
 - (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
 - (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
 - (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

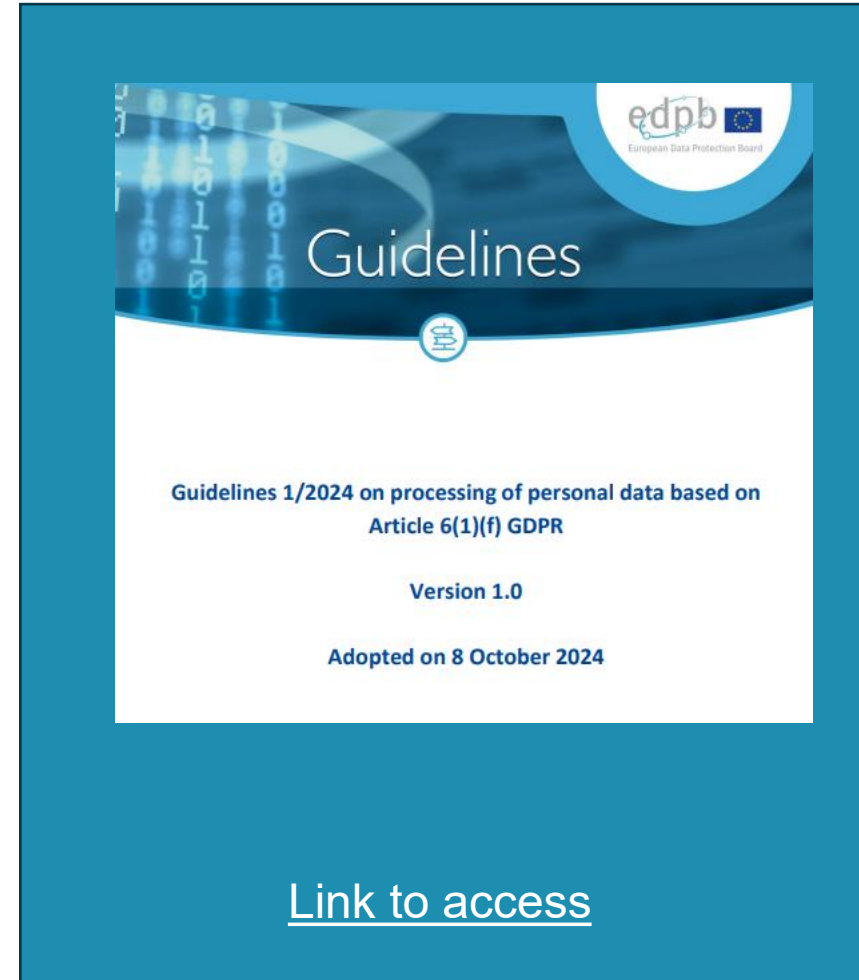
Lawfulness: consent



- **Freely given**
 - Power dynamics
 - Contract = utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract (Art. 7(4))
- **Specific**
 - Written = distinguishable from the other matters
- **Informed**
 - Intelligible, clear and plain language
- **Unambiguous**
 - Written, including electronic, or an oral statement
 - Ticking a box – as long as it is an action
 - Controller must be able to demonstrate
- Right to **withdraw** the consent at any minute

Lawfulness: consent

- Legitimate interest test:
 1. Defining the legitimate interest
 2. Necessity test
 3. Balancing with the fundamental rights and freedoms



Lawfulness and special categories of data

Article 9 = additional requirements for special categories of data

- Racial or ethnic origin
- Political opinions, religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (uniquely identifying a natural person)
- Health data
- Sex life or sexual orientation

Other points of attention

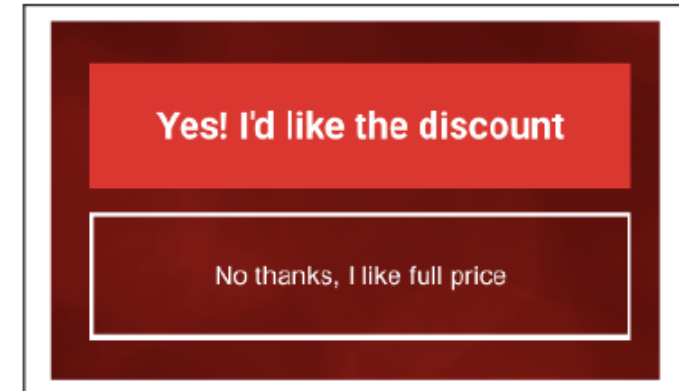
- Children's data (Article 8)
- Data relating to criminal convictions and offences (Article 10)

Fairness

- Objective, good faith ☐ must consider the reasonable expectations of data subjects
 - Dark patterns and manipulative practices
- Avoid disproportionate effects, including discriminatory

Figure A.2. Example of a confirmshaming dark pattern

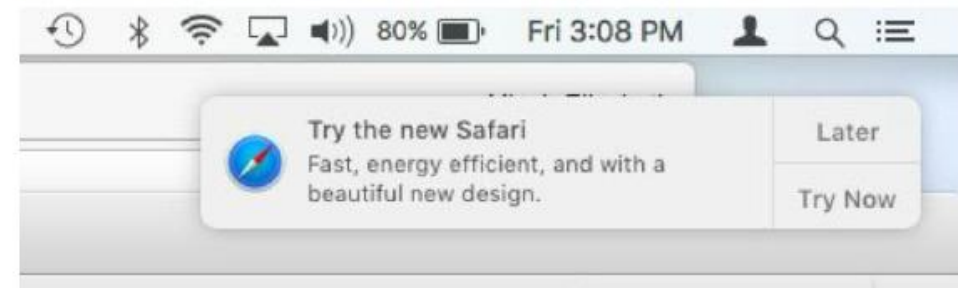
The consumer is shamed into opting for a discount.



Source: Mathur et al (2019^[24]).

Figure A.3. Example of nagging dark pattern

A dialogue box that does not provide the option to permanently dismiss the message.



Source: <https://darkpatterns.uxp2.com/pattern/apple-no-no-option/>

Transparency

- Control depends on having information about the data processing
 - Who, what, why, how and rights
- Translates into both an **obligation** and a **right**
 - *Ex-ante* and *ex-post*

Purpose limitation

- **Specific**
- **Explicit**
- **Legitimate**

When? The latest by the moment of collection

Compatibility test

- Data cannot be processed in an incompatible manner with the initial purposes
 - Archiving, scientific or historical research, statistical purposes = presumed compatibility (+ Art. 89)

Data minimisation

- Data must be **adequate, relevant, and necessary** to the specific purpose of the processing
- Predictions, AI training and unforeseen exploitation? ... in the next session

Accuracy

- Data shall be accurate and, where necessary, kept up to date;
 - Evaluation = context based
- Inaccurate data = erased or rectified without delay
 - Direct connection to right to rectification
 - Controller must notify recipients of the data erased or rectified (Article 19)

'My life was ruined by a typo'

21 March 2017



Nigel says he feared his children might be attacked after he was wrongly arrested

By Adam Eley and Jo Adnitt

BBC Victoria Derbyshire programme

When Nigel Lang was wrongly arrested on suspicion of sharing indecent images of children, he says his life fell apart. It all stemmed from nothing more than a typing error by police.

Source: [BBC UK](#)

Storage limitation

- Data must be 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;
- Secondary processing and purpose limitation and data minimization;
- Erasure, destruction of data

Integrity and confidentiality

- Guarantee the security of the data against data breaches
 - Personal data breach = breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
- Preventive measures
 - Inspiration in environmental law

Thank you!

LinkedIn: Isabela Maria Rosal
Email: isa.rosalsantos@kuleuven.be

<http://www.law.kuleuven.be/citip>



Challenges at the intersection of new technologies and privacy

17.06.2026



Isabela Maria Rosal



isa.rosalsantos@kuleuven.be



Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Academy of European Law. Neither the European Union nor the granting authority can be held responsible for them.

Agenda



Personal data and new technologies



Data subjects' rights and remedies



Other limits and solutions in the intersection between GDPR and new technologies

Importance of personal data for new technologies



Still on principles... Accountability

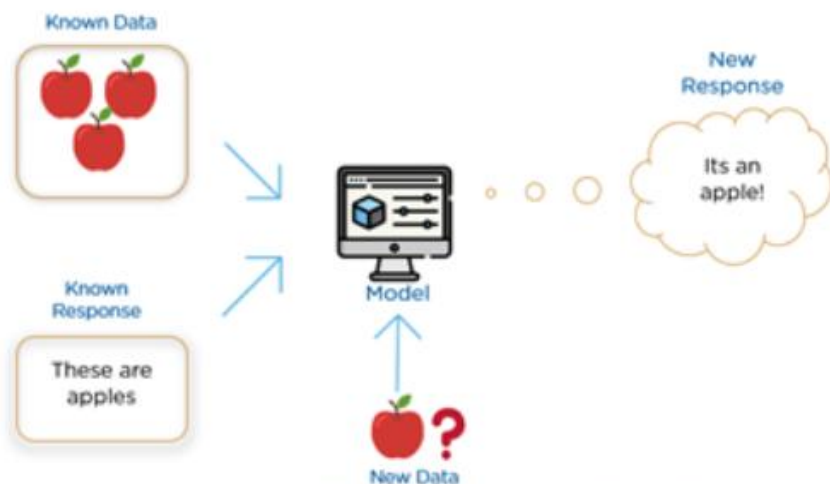
- Controller is responsible for and must be able to demonstrate compliance with the principles;
 - Via = data records of processing activities.
 - Cooperate with supervisory authorities, including by making these records available.
 - Data Protection Officer (DPO) → bridge, not responsible

Data protection-by-design and by-default (Article 25)

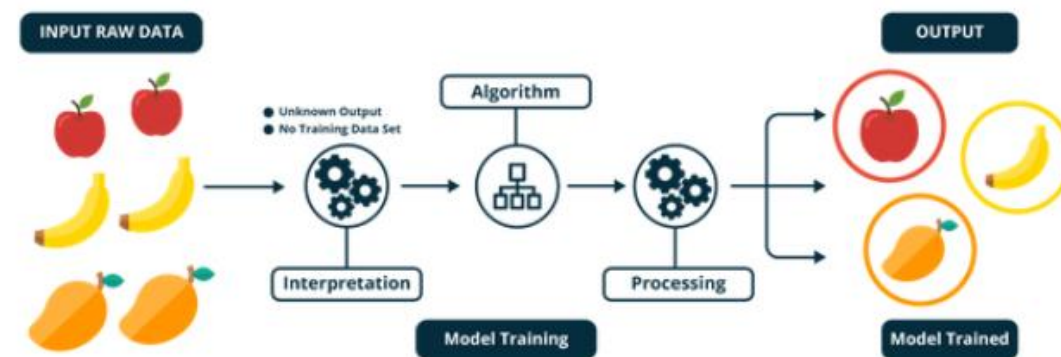
- By-design: since the beginning of development of products and services;
- By-default: no additional actions to guarantee the data minimisation.
 - Obligation to the controller, **not** the subject

Growing importance of data protection

- Data (personal and non-personal) is the input for new business models and technological development



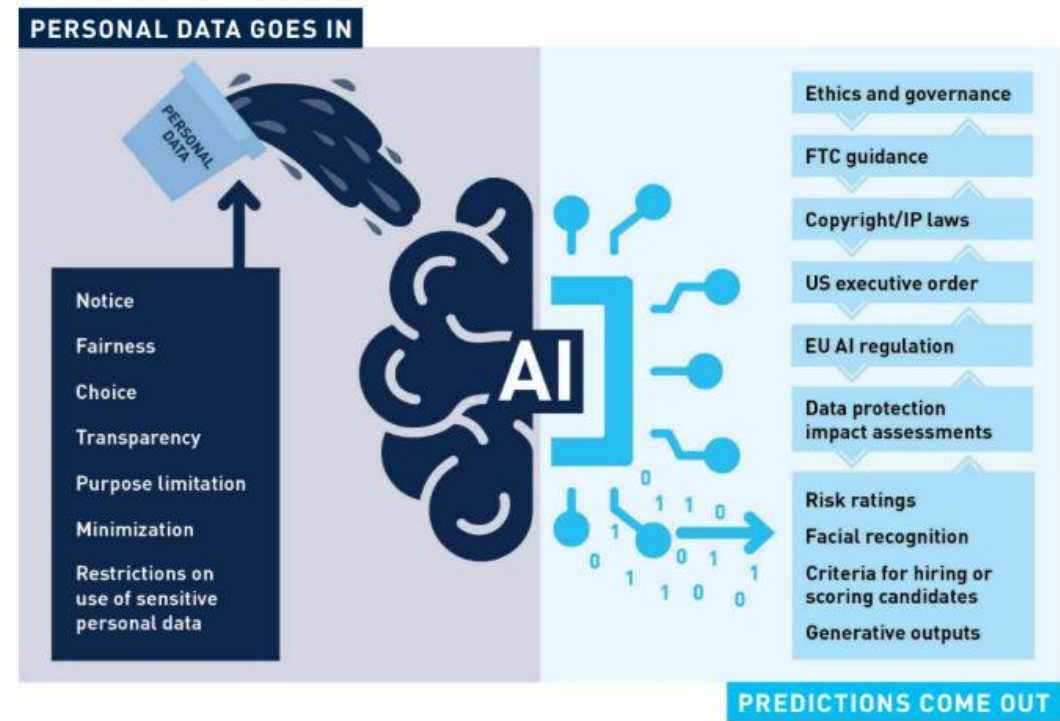
Above, supervised learning is explained with apples.



Unsupervised training

Growing importance of data protection

- Data (personal and non-personal) is the input for new business models and technological development



Growing importance of data protection

- EU understood the importance of data
 - Data Governance Act
 - Data Act
 - Open Data Directive
 - AI Act...
- Making more data more available
- Simplifying GDPR
 - SMEs and documentation

Publicly available data
≠ freely usable data

Publicly available data

Publicly accessible  Freely reusable

Social media and data scrapping: what do you think?

Growing importance of data protection

- EU understood the importance of data = Data Strategy + Digital Omnibus
- Making more data more available
- BUT
- Personal data protection still applies



Growing importance of data protection

- EU understood the importance of data = Data Strategy + Digital Omnibus
- Making more data more available
- BUT
- Personal data protection still applies

- GDPR is an established framework
- Data protection = strategic investment
- Data subjects' rights = useful remedies
- Co-existence of legal instruments

Data subjects' rights and remedies



General rules

- Depend on a request by the data subject
 - Importance of knowing who the controller is
- Time for response: **1 month** + 2months (Art. 12(3) GDPR)
- Free of charge (Art. 12(5) GDPR)
- No need to justify the request
- Controller must notify recipients
- Form: writing or standardised icons (Art. 12 (1) and (7) GDPR)
 - Special attention to children

Right of access

- *Ex-post* $\leftrightarrow$ Right to information (art. 13 and 14 GDPR)
- Initial step for exercising other rights
 - Completeness of the information
- 3 components:
 - Confirmation about their data being processed or not;
 - Access to their personal data;
 - Access to information about the processing.
- Cannot have adverse effects on the rights and freedoms of others
- Identification of the data subject

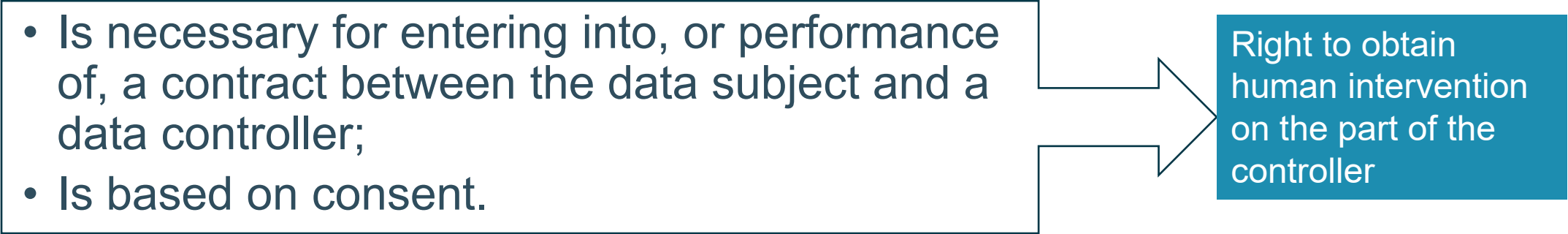
Right of access

Example 17: An individual fraudulently uses the identity of someone else in order to play poker online. The perpetrator pays the online casino using the credit card they stole from the victim. When the victim finds out about the identity theft, the victim asks the provider of the online casino to provide him or her with access to his or her personal data and more specifically, to the online games played and information about the credit card used by the perpetrator.

There is a link between the collected data and the victim as the latter's identity has been used. After the detection of the fraud, the personal data mentioned above still has a link by reason of their content (the victim's credit card is clearly about the victim), purpose and effect (the information about the online games played by the perpetrator may for instance be used to issue invoices to the victim). Therefore, the online casino shall grant the victim access to the aforementioned personal data.

Right against automated individual decision-making

- Right to not be subject to a decision based solely on automated processing that produces **legal effects** or **similarly significantly affects** the data subject
 - No human involvement in the decision process
- A person can be subject to a completely automated processing if:
 - Is authorized by law;
 - Is necessary for entering into, or performance of, a contract between the data subject and a data controller;
 - Is based on consent.



```
graph LR; A["• Is necessary for entering into, or performance of, a contract between the data subject and a data controller;"] --> B["Right to obtain human intervention on the part of the controller"]; C["• Is based on consent."] --> B;
```

Right to obtain human intervention on the part of the controller

Right of access and understanding automated decisions = right to explanation

JUDGMENT OF THE COURT (First Chamber)

27 February 2025 (*)

(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Article 15(1)(h) – Automated decision-making, including profiling – Scoring – Assessment of the creditworthiness of a natural person – Access to meaningful information about the logic involved in profiling – Verification of the accuracy of the information provided – Directive (EU) 2016/943 – Point 1 of Article 2 – Trade secret – Personal data of third parties)

In Case C-203/22,

REQUEST for a preliminary ruling under Article 267 TFEU from the Verwaltungsgericht Wien (Administrative Court, Vienna, Austria), made by decision of 11 February 2022, received at the Court on 16 March 2022, in the proceedings

CK

v

Magistrat der Stadt Wien

other party:

Dun & Bradstreet Austria GmbH,

Right to explanation

- **Existence and logic involved** in an automated processing
 - Clear information considering the targeted public

Example

A controller uses credit scoring to assess and reject an individual's loan application. The score may have been provided by a credit reference agency, or calculated directly based on information held by the controller.

Regardless of the source (and information on the source must be provided to the data subject under Article 14 (2) (f) where the personal data have not been obtained from the data subject), if the controller is reliant upon this score it must be able to explain it and the rationale, to the data subject.

The controller explains that this process helps them make fair and responsible lending decisions. It

provides details of the main characteristics considered in reaching the decision, the source of this information and the relevance. This may include, for example:

- the information provided by the data subject on the application form;
- information about previous account conduct, including any payment arrears; and
- official public records information such as fraud record information and insolvency records.

The controller also includes information to advise the data subject that the credit scoring methods used are regularly tested to ensure they remain fair, effective and unbiased.

The controller provides contact details for the data subject to request that any declined decision is reconsidered, in line with the provisions of Article 22(3).

Right to object

- **At any time**, object to processing based on **public interest** or legitimate interest.
 - *Including profiling*
- Controller must stop the processing activity, unless they can demonstrate compelling reasons that override the interests, rights and freedoms of the data subject **or** for the establishment, exercise or defence of legal claims.
 - Or scientific or historical research or statistical purposes for reasons of public interest
- Very important for direct marketing purposes = opt-out
- Can be exercised by automated means = technical specifications

Right to rectification

- Rectification of inaccurate personal data
- Complete incomplete personal data
- Directly connected to data **accuracy**
 - ... **and self-determination**

PRESS RELEASE No 34/25

Luxembourg, 13 March 2025

Judgment of the Court in Case C-247/23 | [Deldits] ¹

GDPR and transgender identity: the rectification of data relating to gender identity cannot be made conditional upon proof of surgery

[Link to access](#)

GenAI, accuracy and hallucinations

Man files complaint after ChatGPT said he killed his children

21 March 2025

Imran Rahman-Jones
Technology reporter

Share  Save 

[Rahman-Jones, 'Man files complaint after ChatGPT said he killed his children'. *BBC*](#)

[Sankaran V, 'ChatGPT cooks up fake sexual harassment scandal and names real law professor as accused', *The Independent UK*](#)

Tech

ChatGPT cooks up fake sexual harassment scandal and names real law professor as accused

'When first contacted, I found the accusation comical. After some reflection, it took on a more menacing meaning'

Vishwam Sankaran • Thursday 06 April 2023 07:15 BST •  3 Comments



Right to erasure ('right to be forgotten')

Situation 1: You put your name in a search engine platform, where you find news articles with inaccurate information about you. What can you do?



Right to erasure ('right to be forgotten') → a discussion prior to GDPR

JUDGMENT OF THE COURT (Grand Chamber)

13 May 2014 (*1)

'Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator's obligations and of the data subject's rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8'

In Case C-131/12,

REQUEST for a preliminary ruling under Article 267 TFEU from the Audiencia Nacional (Spain), made by decision of 27 February 2012, received at the Court on 9 March 2012, in the proceedings

Google Spain SL,

Google Inc.

v

Agencia Española de Protección de Datos (AEPD),

Mario Costeja González,

THE COURT (Grand Chamber),

CJEU, Case C-131/12, Google Spain v. Mario C. González, 13/05/2014

Right to erasure ('right to be forgotten') in the GDPR

- When?
 - Data no longer necessary
 - Consent withdraw with no other legal ground;
 - After an objection request, without overridden interests;
 - Data was unlawfully processed;
 - Erasure is needed for compliance;
 - Data collected to offer information society services to children
- If the data is **made public** = controller must take **reasonable steps**, considering the technology available and costs, to inform other controllers that are using the data

Right to erasure ('right to be forgotten') and inaccuracy

Judgment of the Court in Case C-460/20 | Google (Dereferencing of allegedly inaccurate content)

Right to erasure ('right to be forgotten'): the operator of a search engine must dereference information found in the referenced content where the person requesting dereferencing proves that such information is manifestly inaccurate

Such proof need not however result from a judicial decision made against the publisher of the website

Right to erasure: limits

- Right to erasure does not apply when the processing is **necessary**:
 1. For exercising the right of freedom of expression and information;
 2. For compliance with a legal obligation;
 3. For the performance of a task carried out in the public interest;
 - Area of public health, archiving in the public interest, scientific or historical research or statistical purposes are highlighted
 4. For the establishment, exercise or defense of legal claims.

Right to be forgotten in new technologies? Machine unlearning

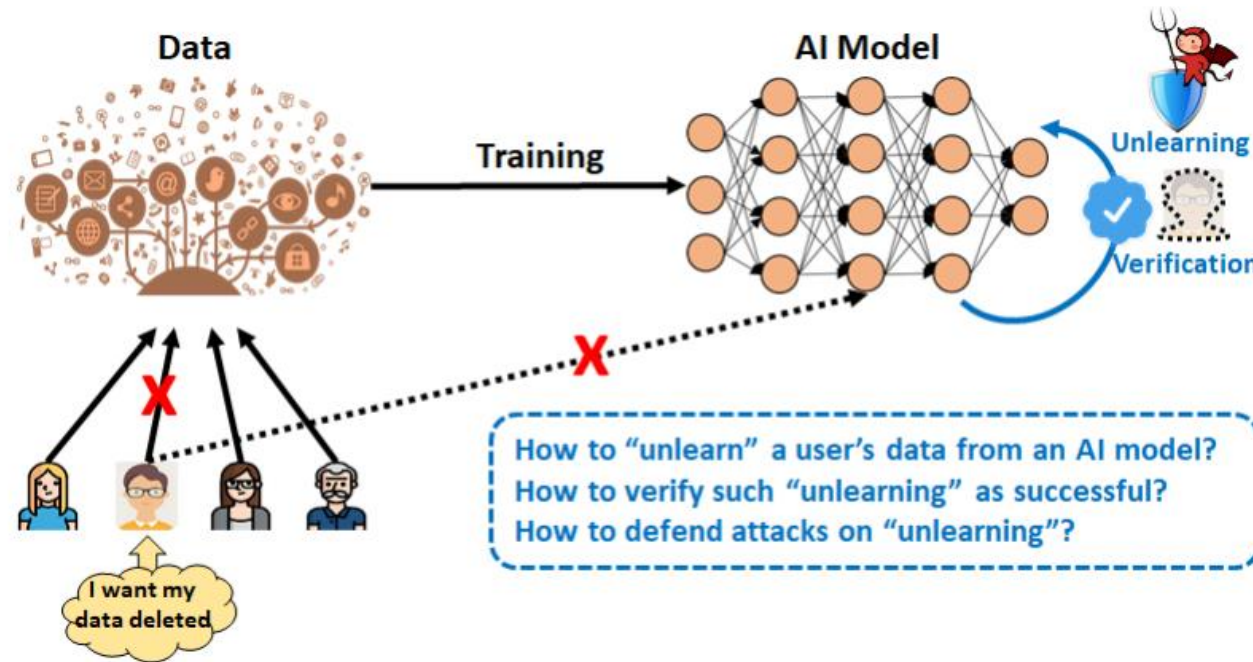


Fig. 1. Diagram of a **general scenario** for machine unlearning

Right to data portability

- Receive their personal data in a **structured, commonly used and machine-readable format** to another controller
- When?
 - Processing based on consent
 - Processing based on a contract
 - Processing is carried out by automated means
- Real goal = increase competition
 - Reality?

Other limits and solutions in the intersection between GDPR and new technologies



Identifiability and anonymisation

- As in previous class → Recital 26 GDPR and Identifiability test
- Synthetic data = a solution for AI training?
- Discrimination and training biases

Unique people's face photos, that do not exist, but they look like 100% real

Generate

Download

Generate Unreal: **Cat**
Horse
Art
Beach



Source: unrealperson.com

Lawfulness and purpose limitation

- Compatibility assessment
 - AI training
 - GenAI
 - General Purpose AI (GPAI)
 - Scientific purposes x real-life training
- More flexibility? Is this still a possible solution?

Recital 50 GDPR: The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required ... Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations.

Other (fundamental) rights



Encryption, freedom of expression and protection of children online



Anonymity and access to information and internet



Social media and democracy



Post-mortal rights?

when you thought everything would be
easy peasy lemon squeezy but it's
actually difficult difficult lemon difficult

And what is next?

Digital Omnibus: de-regulation or
simplification?



Thank you!

KU Leuven Centre for IT & IP Law (CiTiP) - imec
Sint-Michielsstraat 6, box 3443
BE-3000 Leuven, Belgium

<http://www.law.kuleuven.be/citip>