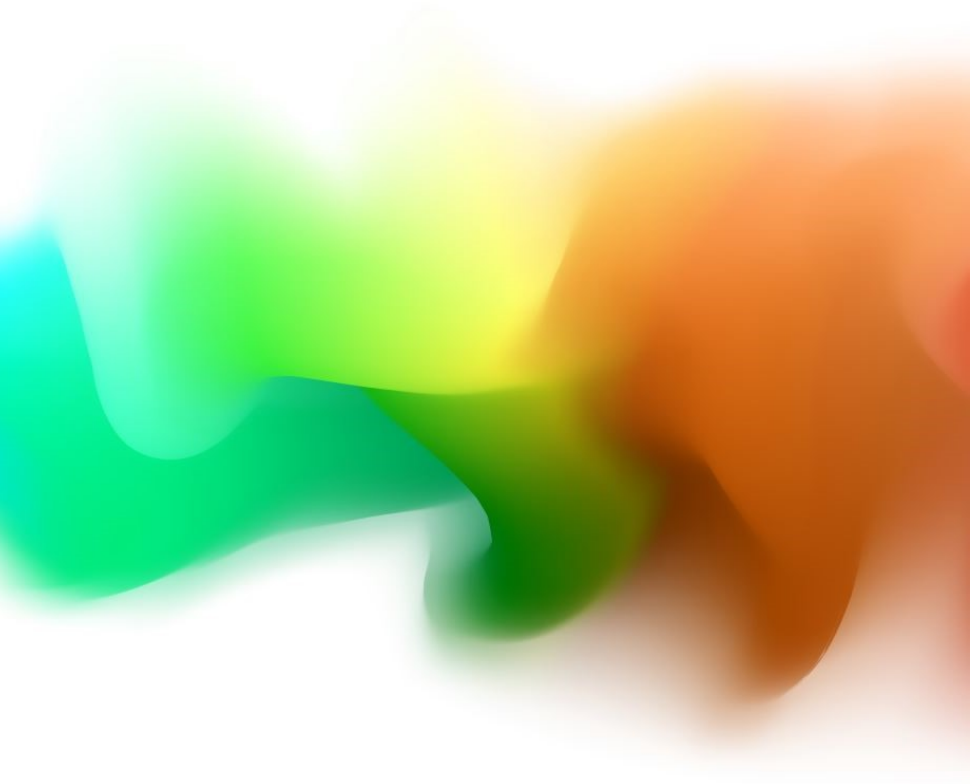


EU DATA PROTECTION LAW – FUNDAMENTALS OF THE LEGAL FRAMEWORK

ERA Young Lawyers Academy, 12-21 June 2023

Dr. Laura Drechsler, Research fellow, Centre for IT & IP Law at KU Leuven/Lecturer at Open Universiteit, Heerlen

Co-funded by the European Union

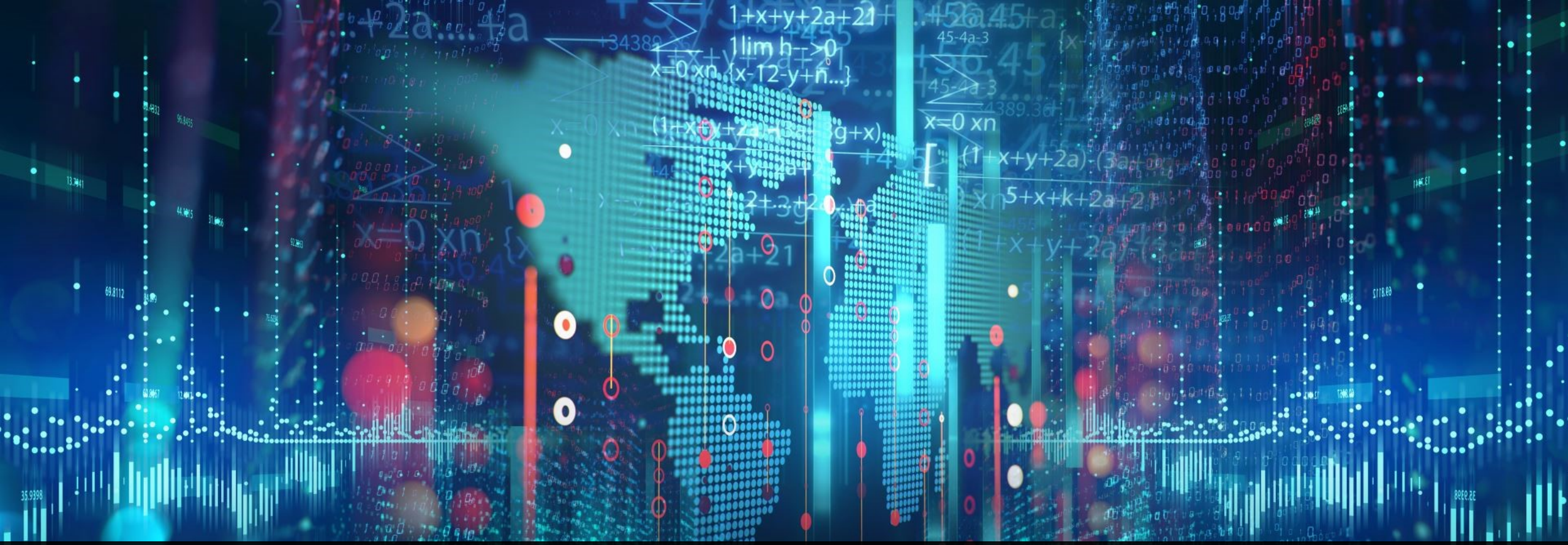
Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Academy of European Law. Neither the European Union nor the granting authority can be held responsible for them.

CLASS OVERVIEW

The development of EU data protection law

Key concepts

The 10 core data protection principles



1. THE DEVELOPMENT OF EU DATA PROTECTION LAW

In the 20th century ideas on regulating personal data first emerged in:

(A) Germany

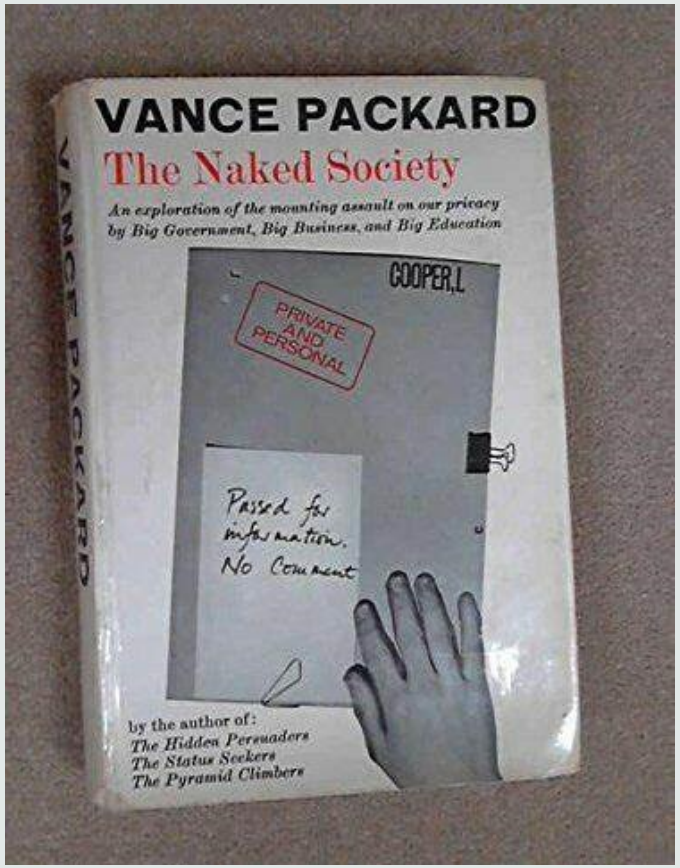
(B) United States

(C) Japan

(D) Sweden

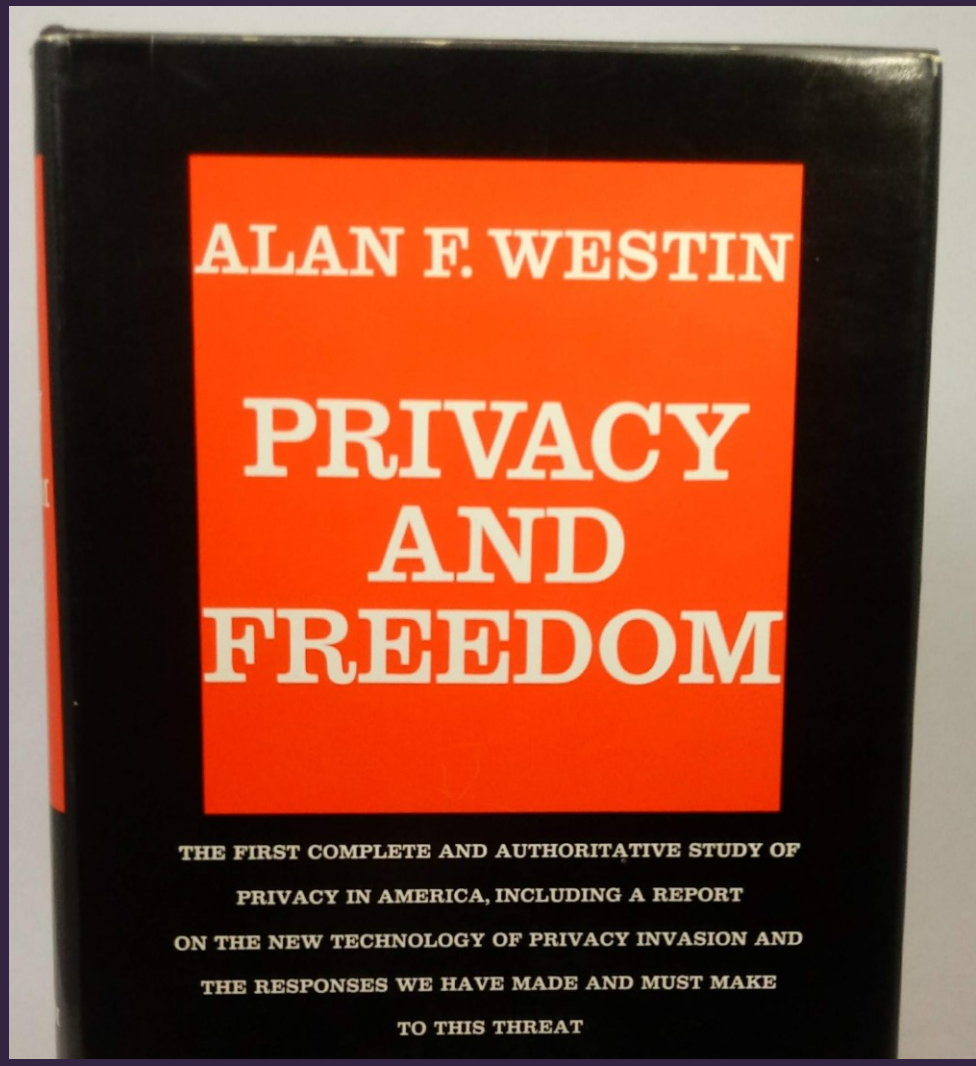
VANCE PACKARD, THE NAKED SOCIETY (PENGUIN BOOKS, 1964):

“Individually these *new social controls* we are seeing are cloaked in reasonableness. And some perhaps have comic overtones. But when we view them collectively, we must consider the possibility that they represent a massive, insidious impingement upon our traditional rights as free citizens to live our own lives.”



ALAN WESTIN, PRIVACY AND FREEDOM (IG PUBLISHING, 1967):

"The computer-born revolution in man's capacity to process data is obviously an enormous boon. In business, government, medicine, science, and a dozen other fields, men are now able to make more fact-based, more logical, and more predictable decisions than they could do before the age of electronic information storage and retrieval."(…) "The issue of privacy raised by computerisation is whether the increased collection and processing of information for diverse public and private purposes, if not carefully controlled, *could lead to a sweeping power of surveillance by government* over individual lives and organisational activity. As we are forced more and more each day to leave documentary fingerprints and footprints behind us, and as these are increasingly put into storage systems capable of computer retrieval, government may acquire a power-through-data position that armies of government investigators could not create in past eras."



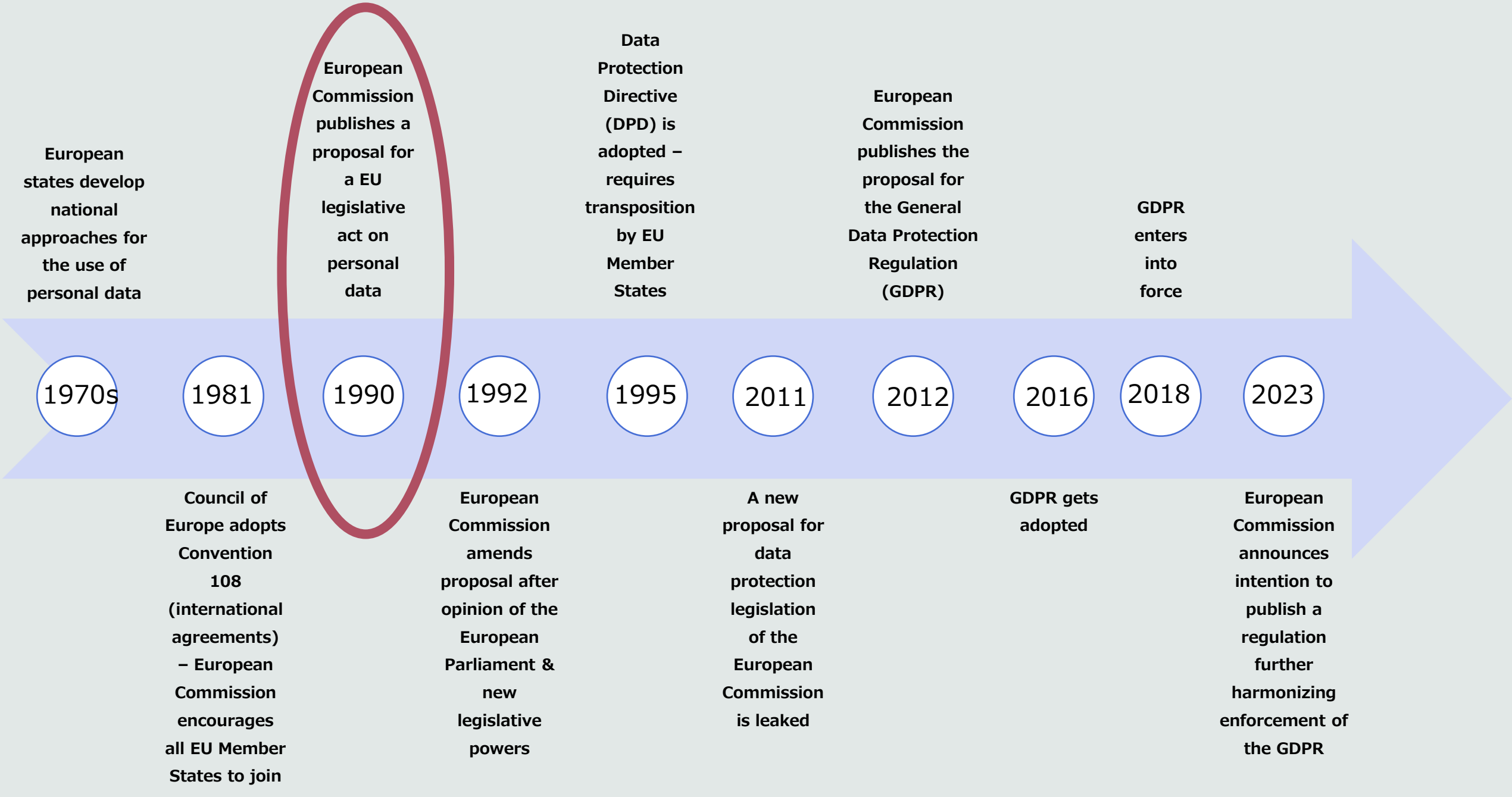
Comparison legislative steps:

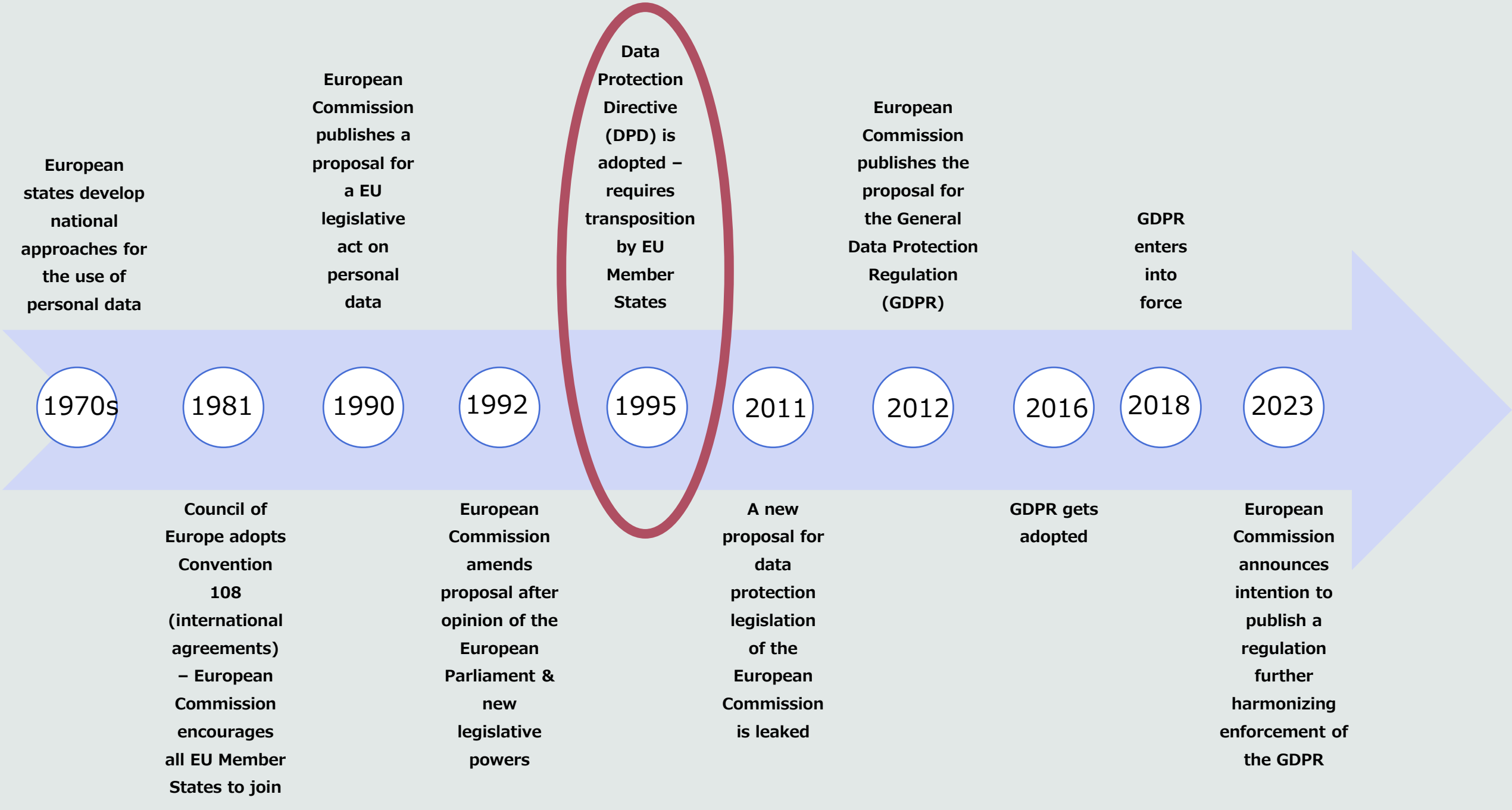
UNITED STATES

- → US Fair Credit Reporting Act of 1970
- → Federal Privacy Act of 1974 (federal agencies only)
- → Participation in OECD Privacy Guidelines of 1980 (non-binding)
- → Since 2018, increased activity on data protection at state level

EUROPE

- → Data protection legislation (e.g Hessen 1970, Sweden 1973, Austria 1979…
- → Binding ‘international agreement’: Convention 108 in 1981
- → EU Data Protection Directive in 1995
- → General Data Protection Regulation in 2016 applicable from 2018


1970s
European states develop national approaches for the use of personal data
1981
Council of Europe adopts Convention 108 (international agreements) – European Commission encourages all EU Member States to join
1990
European Commission publishes a proposal for a EU legislative act on personal data
1992
European Commission amends proposal after opinion of the European Parliament & new legislative powers
1995
Data Protection Directive (DPD) is adopted – requires transposition by EU Member States
2011
A new proposal for data protection legislation of the European Commission is leaked
2012
European Commission publishes the proposal for the General Data Protection Regulation (GDPR)
2016
GDPR gets adopted
2018
GDPR enters into force
2023
European Commission announces intention to publish a regulation further harmonizing enforcement of the GDPR


1970s
European states develop national approaches for the use of personal data
1981
Council of Europe adopts Convention 108 (international agreements) – European Commission encourages all EU Member States to join
1990
European Commission publishes a proposal for a EU legislative act on personal data
1992
European Commission amends proposal after opinion of the European Parliament & new legislative powers
1995
Data Protection Directive (DPD) is adopted – requires transposition by EU Member States
2011
A new proposal for data protection legislation of the European Commission is leaked
2012
European Commission publishes the proposal for the General Data Protection Regulation (GDPR)
2016
GDPR gets adopted
2018
GDPR enters into force
2023
European Commission announces intention to publish a regulation further harmonizing enforcement of the GDPR

The two rationales of the EU's approach to personal data legislation in the DPD

PROTECTION OF FUNDAMENTAL RIGHTS (PRIVACY AND PERSONAL DATA PROTECTION)

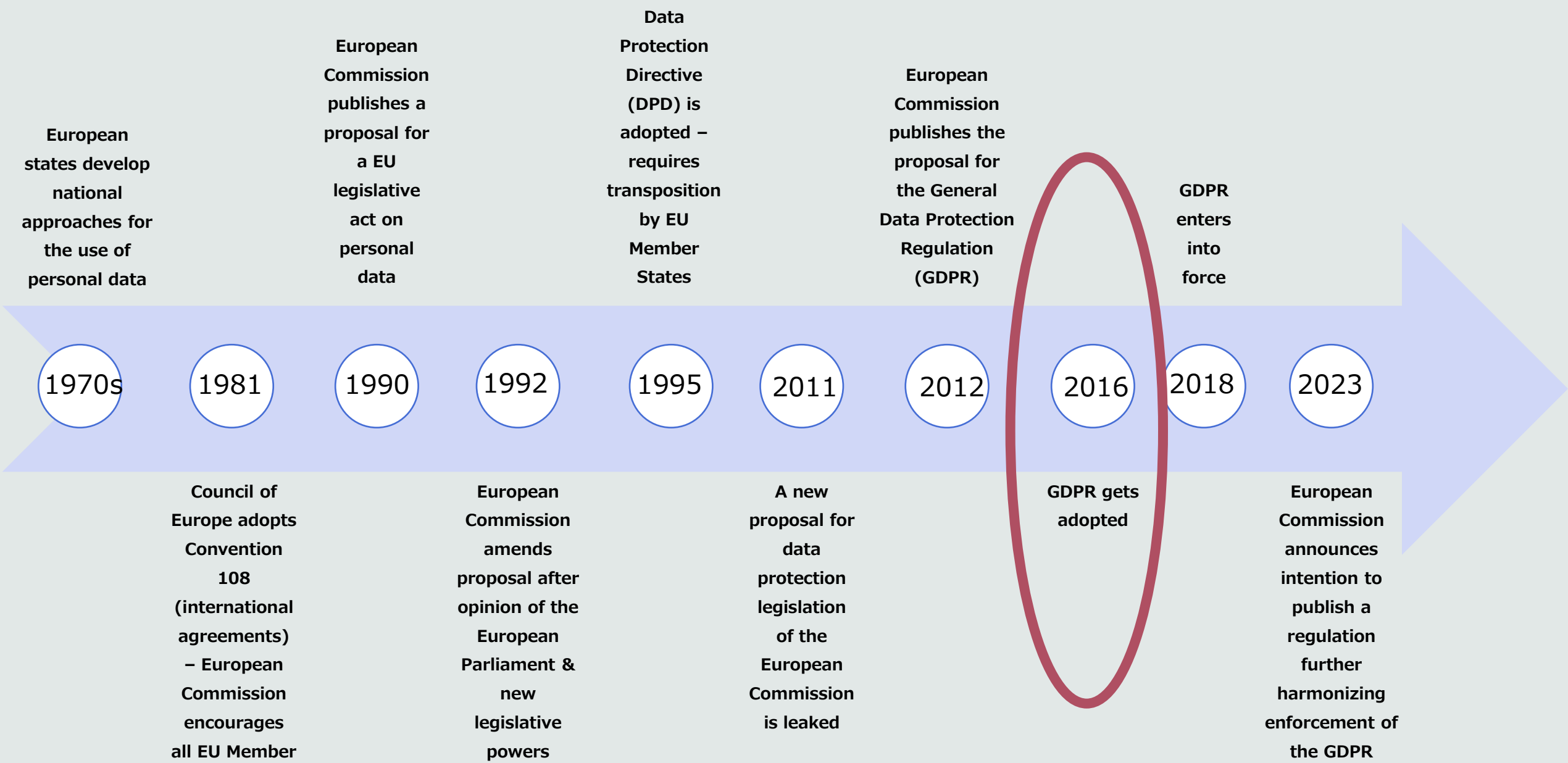
'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'.

(Article 1 paragraph 1 DPD)

FREE MOVEMENT OF PERSONAL DATA WITHIN THE EU

'Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1'.

(Article 1 paragraph 2 DPD)


1970s
European states develop national approaches for the use of personal data
1981
Council of Europe adopts Convention 108 (international agreements) – European Commission encourages all EU Member States to join
1990
European Commission publishes a proposal for a EU legislative act on personal data
1992
European Commission amends proposal after opinion of the European Parliament & new legislative powers
1995
Data Protection Directive (DPD) is adopted – requires transposition by EU Member States
2011
A new proposal for data protection legislation of the European Commission is leaked
2012
European Commission publishes the proposal for the General Data Protection Regulation (GDPR)
2016
GDPR gets adopted
2018
GDPR enters into force
2023
European Commission announces intention to publish a regulation further harmonizing enforcement of the GDPR

Article 16

(ex Article 286 TEC)

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

Art. 16 TFEU – EU competence to legislate on data protection

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.

Art. 8 Charter – data protection = fundamental right

The two rationales of the EU's approach to personal data legislation in the GDPR: no longer equal rationales?

PROTECTION OF FUNDAMENTAL RIGHTS (PRIVACY AND PERSONAL DATA PROTECTION)

'This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'.

(Article 1 paragraph 2 GDPR) = 1st RATIONALE

FREE MOVEMENT OF PERSONAL DATA WITHIN THE EU

'The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data'.

(Article 1 paragraph 3 GDPR) = ?

Case C-132/21, *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság,* 12 January 2023

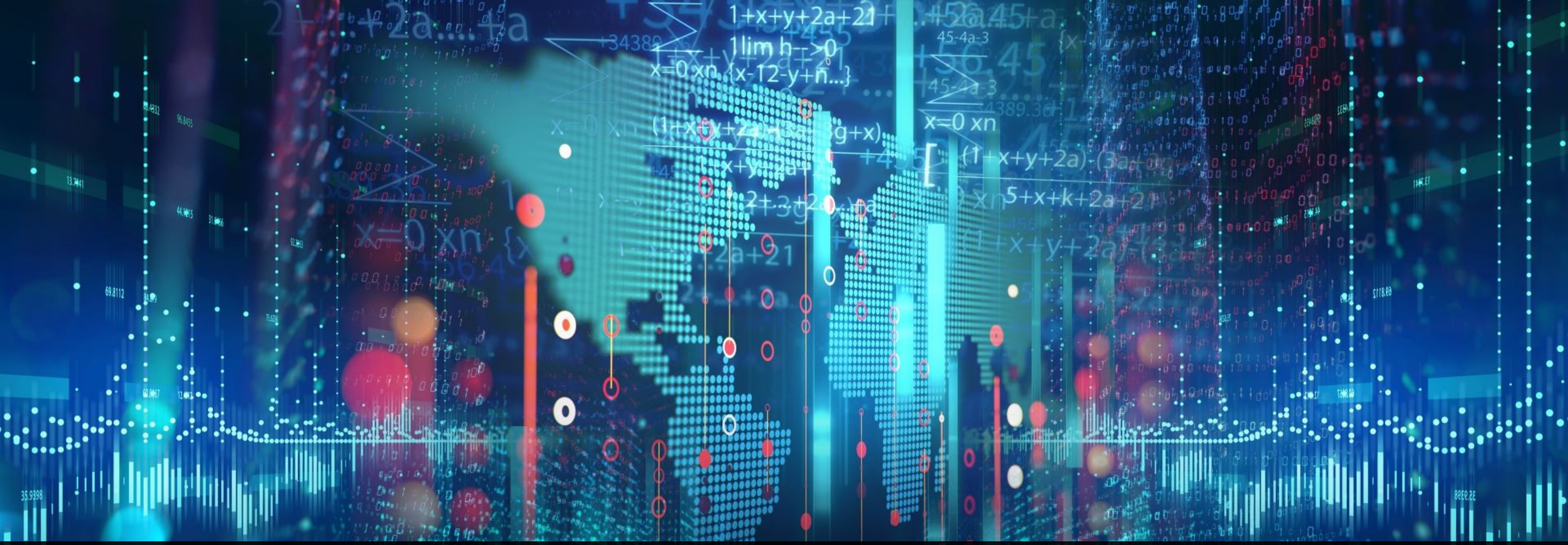
''Lastly, regarding the objectives pursued by that regulation [*the GDPR*] , it is apparent (…) that **the aim** of that regulation is to ensure a high level of protection of natural persons with regard to the processing of personal data within the European Union (…).''

(*CJEU, Case C-132/21, paragraph 42*)

Sources of the current EU data protection law

EU fundamental rights (Charter)/Article 16 TFEU

General Data Protection Regulation (GDPR)	EU Institution Data Protection Regulation (EUDPR)	Law Enforcement Directive (LED)	EU data law
National laws implementing opening clauses of the GDPR	EU bodies with own data protection rules (e.g. Europol)	National law transposing the LED	Digital Markets Act, Digital Services Act, Data Governance Act (to be adopted: Data Act, Health Data Space, AI Act)



2. KEY CONCEPTS

THE MATERIAL SCOPE OF THE GDPR:

The GDPR 'applies to the processing of personal data wholly or partly by automated means to the processing other than by automated means of personal data which form part of a filing system.'

(ARTICLE 2 PARAGRAPH 1 GDPR)

What are ‘personal data’?

ARTICLE 4 PARAGRAPH 1 GDPR

‘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;

Pseudonymized data = personal data

Anonymized data ≠ personal data

Images are covered by a video surveillance system in a public space. Can these images constitute personal data?

(A) Yes

(B) No

The service register of a car held by a mechanic or garage contains the information about the car, mileage, dates of service checks, technical problems, and material condition. Can this be considered as personal data if no further information is available?

(A) Yes

(B) No

What is ‘processing’?

ARTICLE 4 PARAGRAPH 2 GDPR

‘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, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction’.

Processing = organising personal data in paper files

Processing ≠ keeping personal data on random pieces of paper with no means to find anything easily

A search engine scraps the internet to provide answers to search queries typed into its search bar. When the name of X is typed in there, a number of results appear referring to old newspaper articles in which it is mentioned that X has unpaid debts towards the state. In relation to X, is the showing of results linked to X when his name is searched, a processing of personal data?

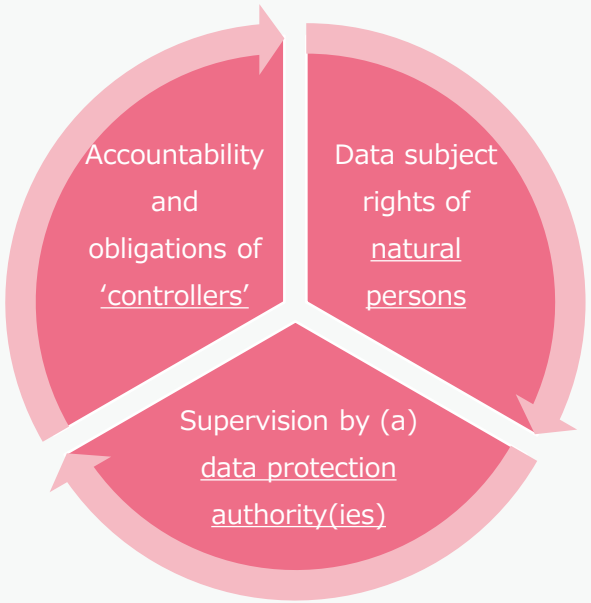
(A) Yes

(B) No

The “actors” of the GDPR

‘’Effective protection of personal data throughout the Union requires 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’’

Recital 11 GDPR



Article 3

Territorial scope

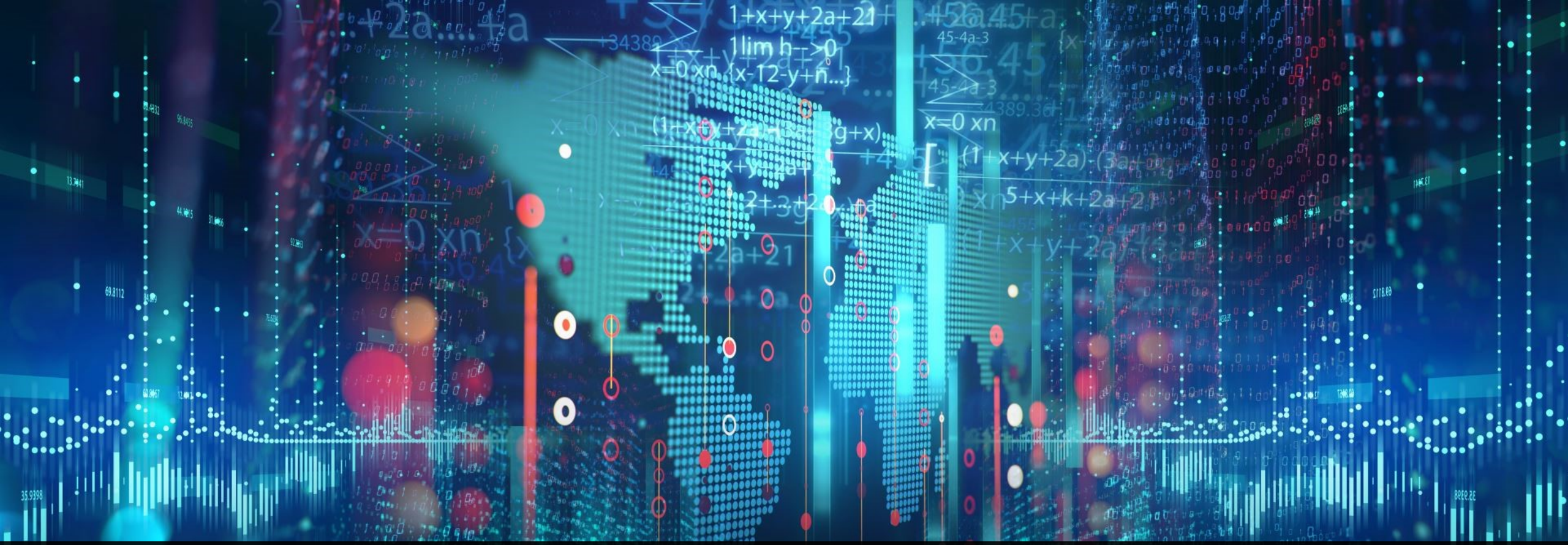
1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

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.

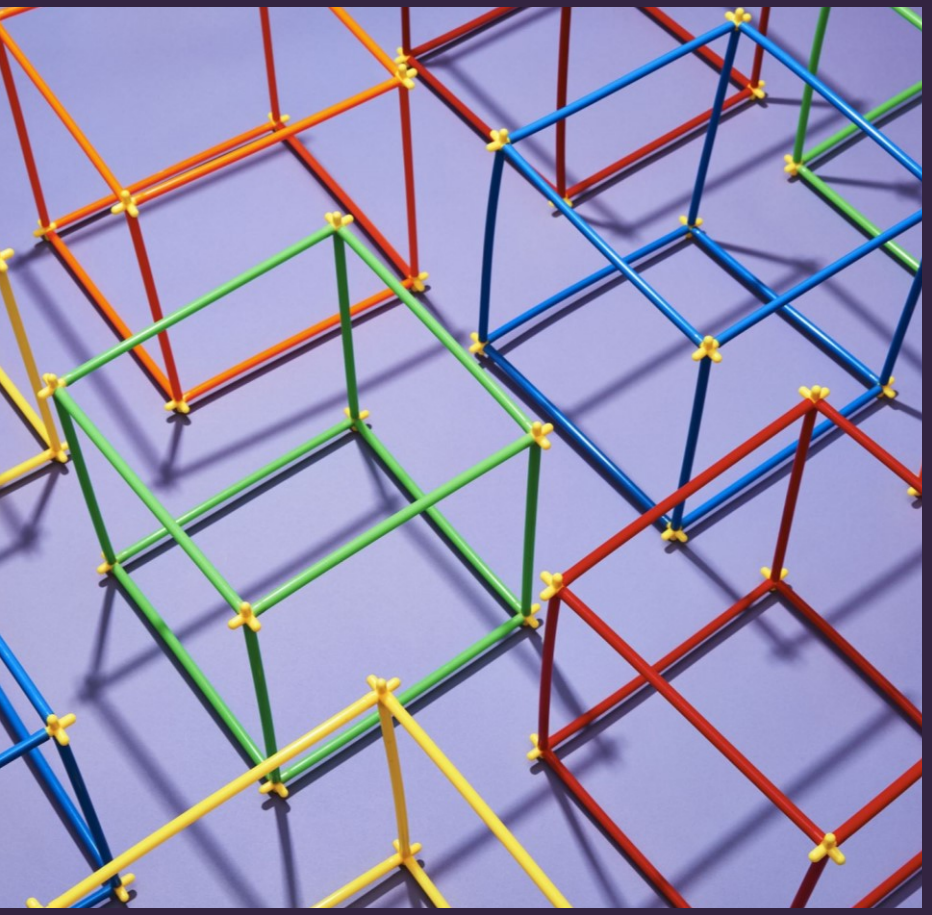
THE (EXTRA)TERRITORIAL SCOPE OF THE GDPR



3. THE 10 CORE DATA PROTECTION PRINCIPLES

ANY PROCESSING OF PERSONAL DATA MUST RESPECT THE DATA PROTECTION PRINCIPLES. THE CONTROLLER IS RESPONSIBLE FOR THIS.

(ARTICLE 5 PARAGRAPH 1 & 2 GDPR)



10 core data protection principles

1. Lawfulness (every processing needs a justification listed in the GDPR)
2. Transparency (inform data subjects about what happens to their data)
3. Fairness (no deception/discrimination of data subjects)
4. Purpose specification (inform in advance of the purpose of processing)
5. Purpose limitation (limit processing to specified purpose)
6. Data minimisation (use only the personal data necessary for purpose)
7. Accuracy (process accurate and up to date personal data)
8. Storage limitation (store personal data only as long as necessary)
9. Integrity and confidentiality (ensure data security)
10. Accountability (be prepared to justify any actions with personal data to authorities)

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;

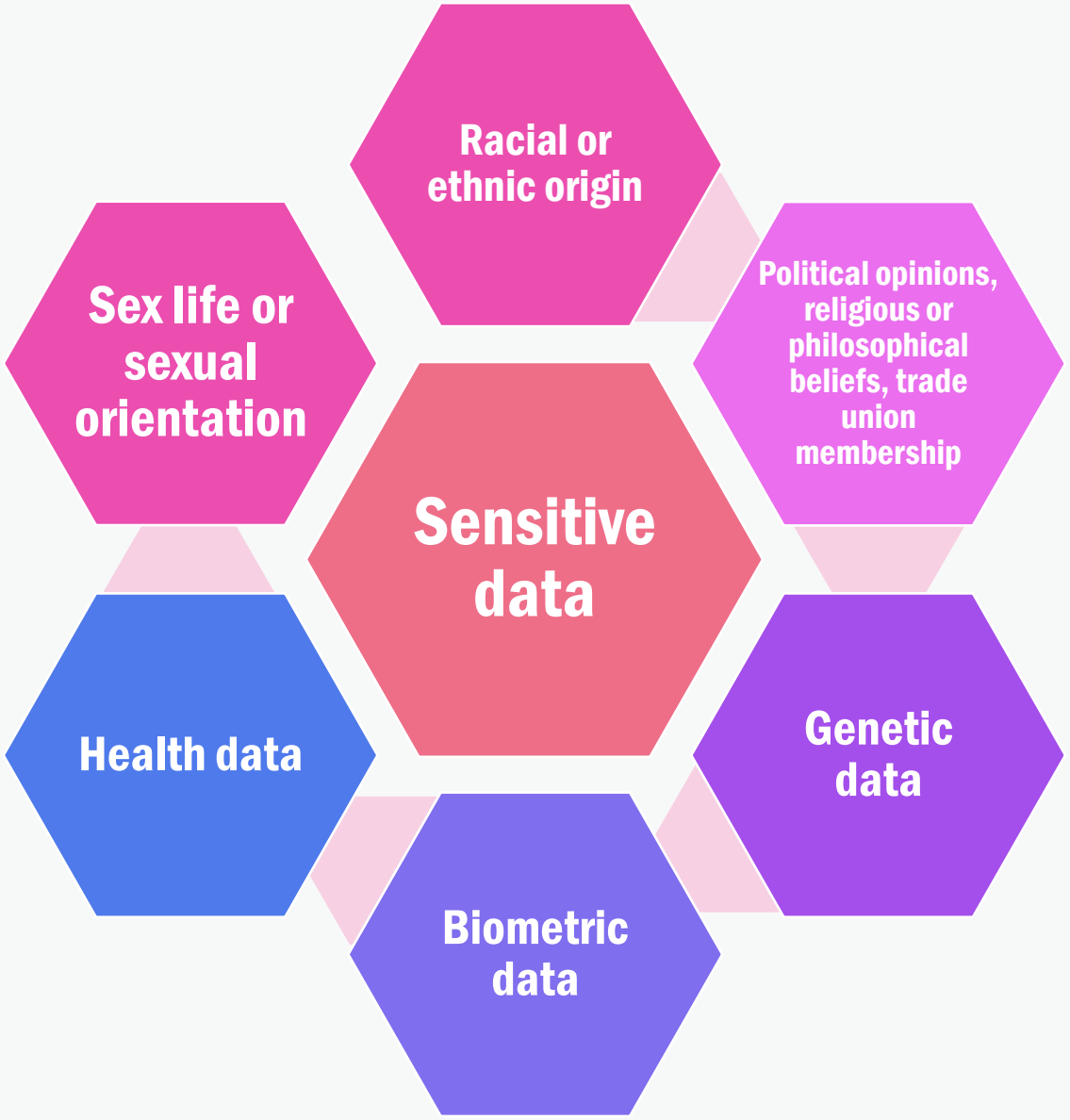
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(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.

1. LAWFULNESS

“Additional Lawfulness” for ‘special categories of personal data’ (Article 9 GDPR)



Special rules for ‘international personal data transfers’

International personal data transfer = personal data with a controller/processor in the scope of the GDPR becomes available to a controller outside the scope of the GDPR in a third country or international organization (Definition EDPB).

International transfers require an additional legal basis (adequacy/appropriate safeguards/derogations) under the GDPR (Chapter V GDPR).

For the US, the arrangement for data transfers (adequacy) has already been invalidated twice by the CJEU due to fundamental rights concerns (unrestricted access to the data by US authorities). The next agreement has been negotiated and is expected to enter into force by the end of the year.

2. FAIRNESS

Special rules to protect children

- For information society services (e.g. social media) children need to be at least 16 to consent. If younger, need for parental consent (Member States can put a lower age, but not lower than 13) (Article 8 paragraph 1 GDPR)
- Need for age verification measures (Article 8 paragraph 2 GDPR)
- Need for information understandable for a child (Article 12 paragraph 1 GDPR)

3. TRANSPARENCY

Protection of your personal data

This privacy statement provides information about the processing and the protection of your personal data.

Introduction

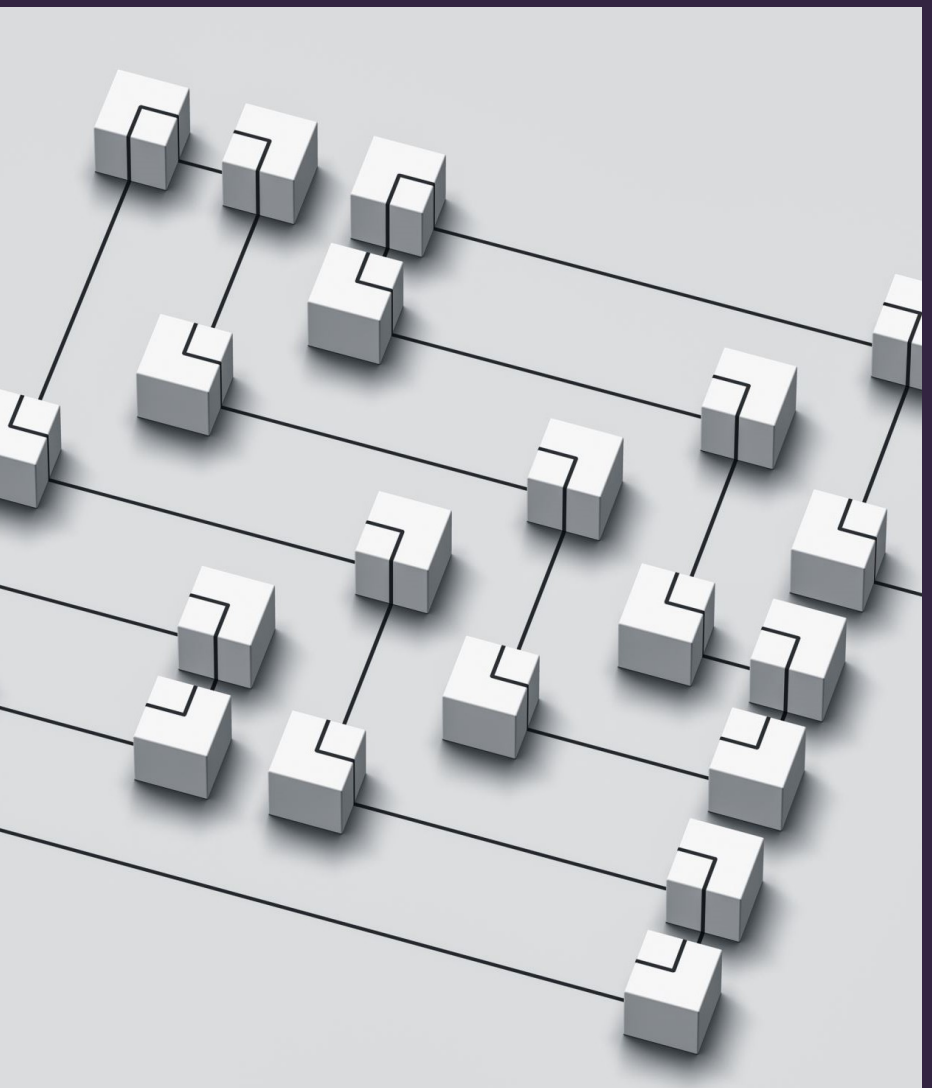
The European Commission (hereafter 'the Commission') is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

4. PURPOSE SPECIFICATION

Specify an explicit purpose for processing upon collection of personal data (& inform the data subject)

5. PURPOSE LIMITATION



Data protection-by-design & by-default (Article 25 GDPR)

- By-design: ensure data protection compliance for all processing operations
- By-default: Personal data should be default limited to its purpose.

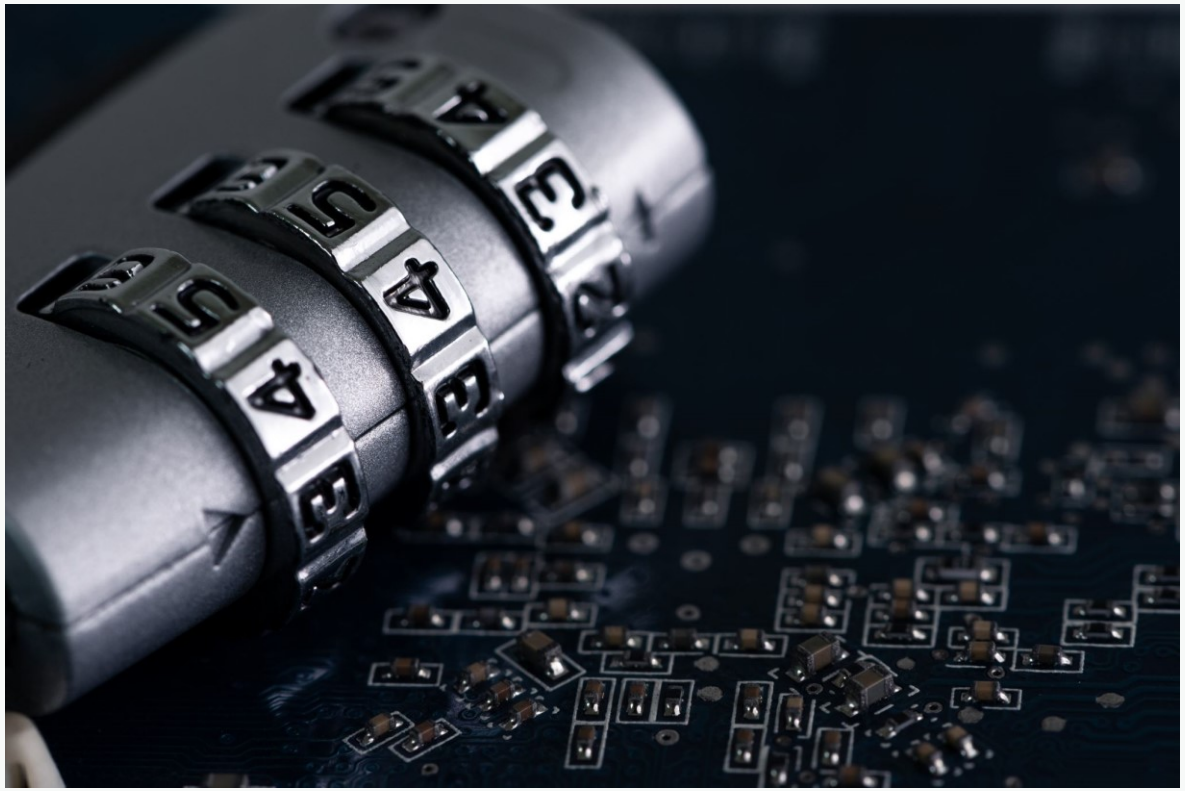
6. Data minimisation

Personal data shall be ‘adequate, relevant and limited to the purposes for which they are processed’ (Art. 5(1)(c) GDPR).

7. ACCURACY

8. Storage Limitation

Personal data shall 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” (Art. 5(1)(e) GDPR).



9. INTEGRITY AND CONFIDENTIALITY

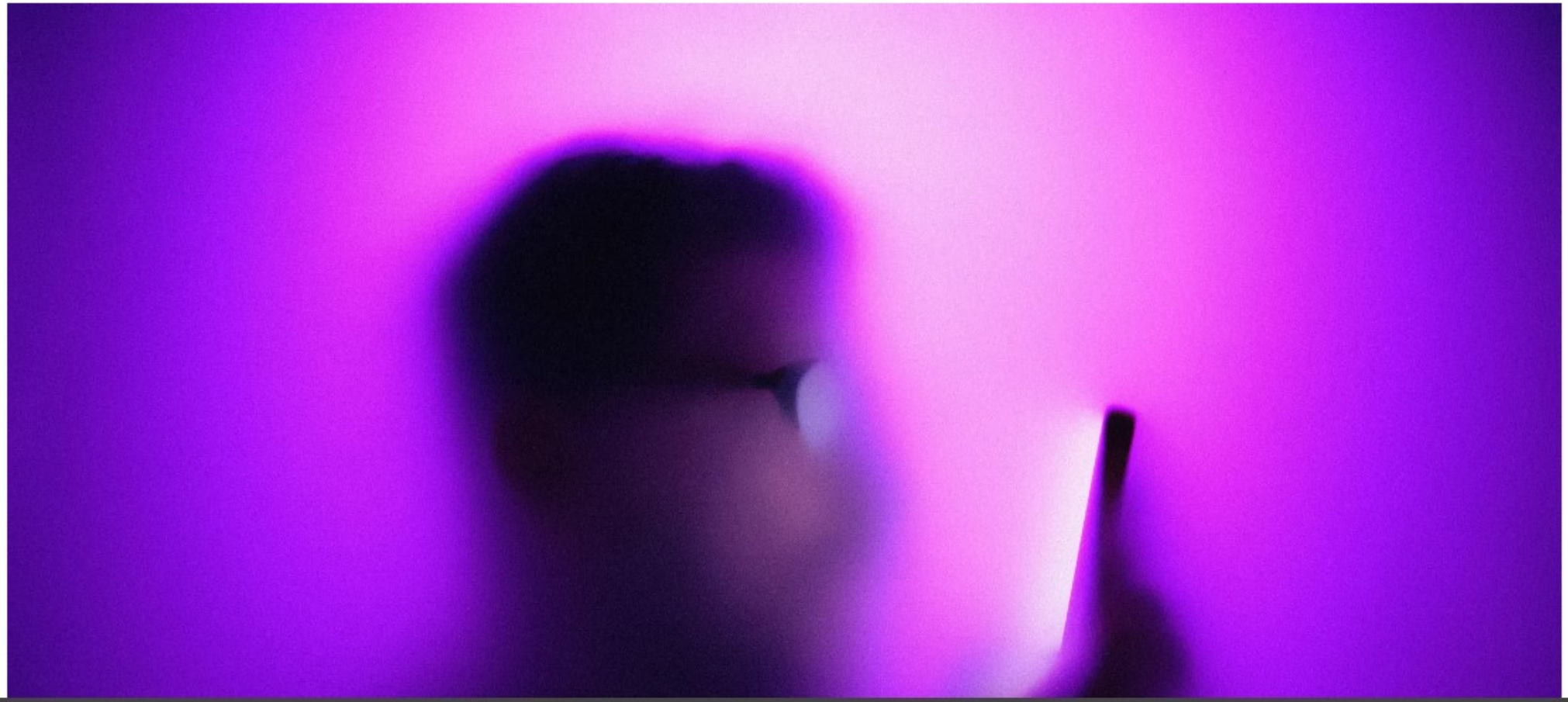
10. Accountability

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1” (Article 5(2) GDPR)

MATT BURGESS SECURITY APR 4, 2023 12:08 PM

ChatGPT Has a Big Privacy Problem

Italy's recent ban of Open AI's generative text tool may just be the beginning of ChatGPT's regulatory woes.



Artificial intelligence: stop to ChatGPT by the Italian SA

…

No way for ChatGPT to continue processing data in breach of privacy laws. The Italian SA imposed an immediate temporary limitation on the processing of Italian users' data by OpenAI, the US-based company developing and managing the platform. An inquiry into the facts of the case was initiated as well.

A data breach affecting ChatGPT users' conversations and information on payments by subscribers to the service had been reported on 20 March. ChatGPT is the best known among relational AI platforms that are capable to emulate and elaborate human conversations.

In its order, the Italian SA highlights that no information is provided to users and data subjects whose data are collected by Open AI; more importantly, there appears to be no legal basis underpinning the massive collection and processing of personal data in order to 'train' the algorithms on which the platform relies.

As confirmed by the tests carried out so far, the information made available by ChatGPT does not always match factual circumstances, so that inaccurate personal data are processed.

Finally, the Italian SA emphasizes in its order that the lack of whatever age verification mechanism exposes children to receiving responses that are absolutely inappropriate to their age and awareness, even though the service is allegedly addressed to users aged above 13 according to OpenAI's terms of service.

OpenAI is not established in the EU, however it has designated a representative in the European Economic Area. It will have to notify the Italian SA within 20 days of the measures implemented to comply with the order, otherwise a fine of up to EUR 20 million or 4% of the total worldwide annual turnover may be imposed.

Roma, 31 March 2023

Principle of integrity and confidentiality

Principle of transparency

Artificial intelligence: stop to ChatGPT by the Italian SA

...

No way for ChatGPT to continue processing data in breach of privacy laws. The Italian SA imposed an immediate temporary limitation on the processing of Italian users' data by OpenAI, the US-based company developing and managing the platform. An inquiry into the facts of the case was initiated as well.

A data breach affecting ChatGPT users' conversations and information on payments by subscribers to the service had been reported on 20 March. ChatGPT is the best known among relational AI platforms that are capable to emulate and elaborate human conversations.

In its order, the Italian SA highlights that no information is provided to users and data subjects whose data are collected by Open AI; more importantly, there appears to be no legal basis underpinning the massive collection and processing of personal data in order to 'train' the algorithms on which the platform relies.

As confirmed by the tests carried out so far, the information made available by ChatGPT does not always match factual circumstances, so that inaccurate personal data are processed.

Finally, the Italian SA emphasizes in its order that the lack of whatever age verification mechanism exposes children to receiving responses that are absolutely inappropriate to their age and awareness, even though the service is allegedly addressed to users aged above 13 according to OpenAI's terms of service.

OpenAI is not established in the EU, however it has designated a representative in the European Economic Area. It will have to notify the Italian SA within 20 days of the measures implemented to comply with the order, otherwise a fine of up to EUR 20 million or 4% of the total worldwide annual turnover may be imposed.

Roma, 31 March 2023

Principle of lawfulness

Principle of accuracy

Special protection for children

EU DATA PROTECTION LAW – FUNDAMENTALS OF THE LEGAL FRAMEWORK

ERA Young Lawyers Academy, 12-21 June 2023

Dr. Laura Drechsler, Research fellow, Centre for IT & IP Law at KU Leuven/Lecturer at Open Universiteit, Heerlen