EU data protection law – fundamentals of the legal framework

11 June 2024 Christophe Buschmann

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

01 Legal framework

02 Defining “personal data”

03 Defining “processing activity”

04 Key data protection stakeholders

05 Data protection principles

Legal framework

Legal framework

4.5.2016 EN Official Journal of the European Union L 119/1

I

"GDPR"

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Harmonisation

- The same rules in all 28 countries of the EU
- Directly applicable (since 25 May 2018)
- To all organisations active on EU territory

New legal framework

- Strengthening of individuals' rights
- An increased responsibility for controllers
- A more important role for data protection authorities

Legal framework

A paradigm shift

Less bureaucracy, yet **more demanding** for controllers and processors

Prior formalities

Prior control

Principle of Accountability

Subsequent control

Defining “personal data”

Defining “personal data”

Article 4 (1) GDPR

“***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*

Defining “personal data”

“Clear text data”

- *Data that allow the immediate identification of a person*

Pseudonymised data

- *Possibility to identify a person after a more or less significant research effort*

Anonymised data

- *Absolute impossibility to link the data to a specific person*

Defining “personal data”

- **Special categories of data => “sensitive data”**

Racial or ethnic origin

Trade union membership

Religious or philosophical beliefs

Political opinions

Health data

Data on sex life

Genetic data

Biometric data

Judicial data

Defining “processing activity”

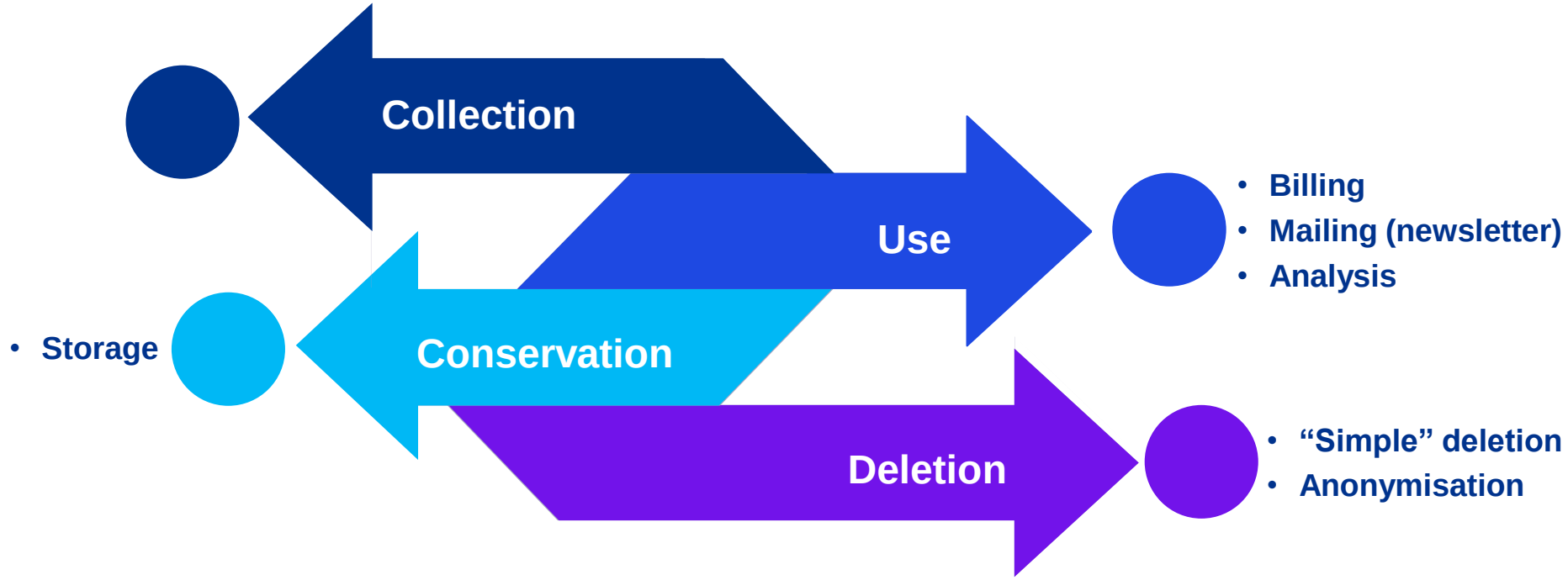
Defining “processing activity”

Article 4 (2) GDPR

*“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”*

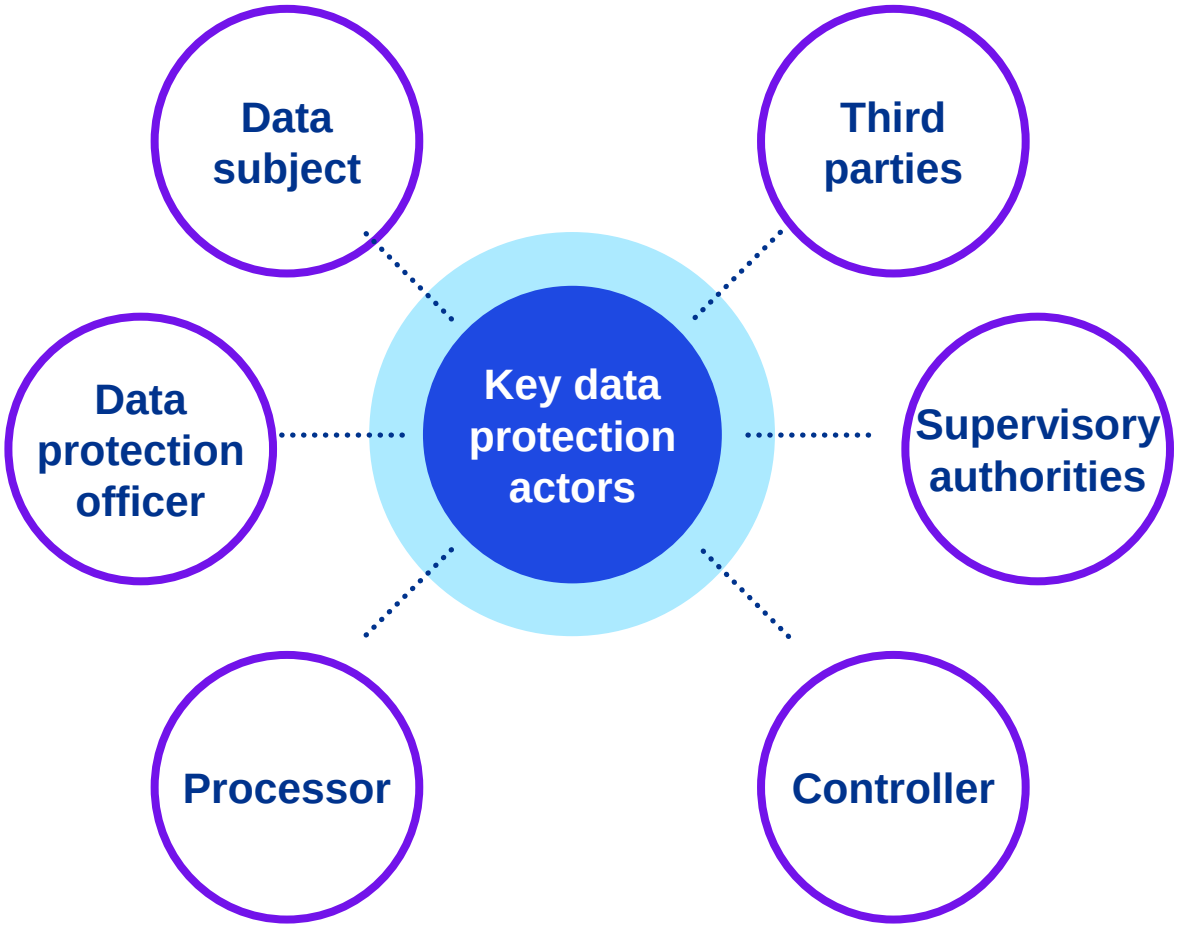
Defining “processing activity”

The life-cycle of a processing activity

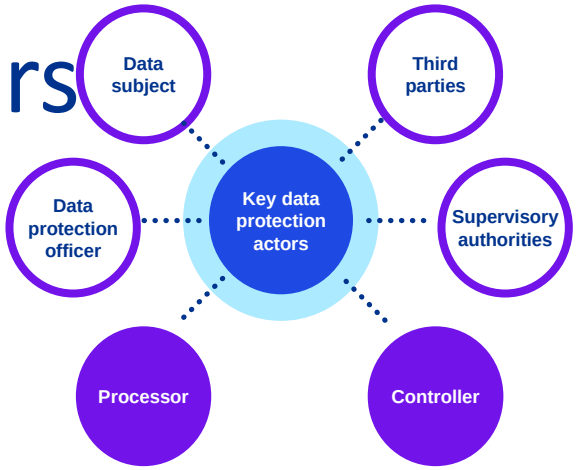


Key data protection stakeholders

Key data protection stakeholders



Key data protection stakeholders



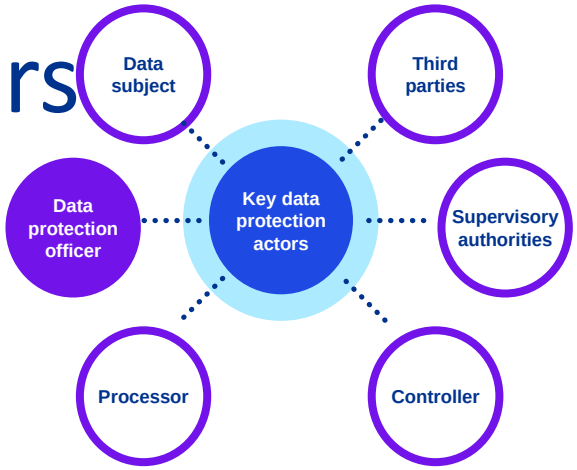
Controller

- *Determines the purposes and means of the processing*

Processor

- *Processes personal data on behalf and upon instruction of the controller*

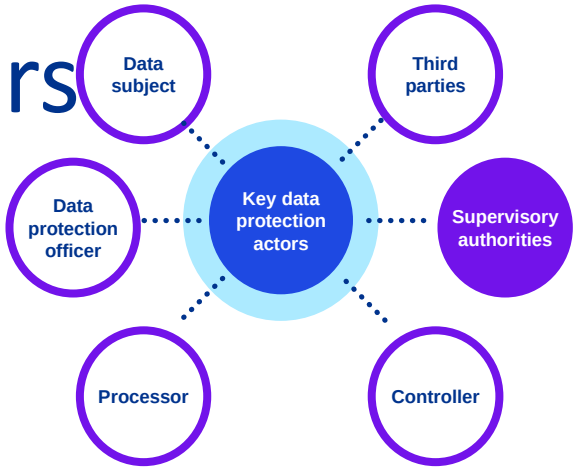
Key data protection stakeholders



Data Protection Officer (DPO)

- *Designation is mandatory in certain cases*
- *Professional qualities and expert knowledge*
- *Independent*
- *Must be given adequate resources & time to fulfil duties*

Key data protection stakeholders



On-site inspection

Audit

Certification

Data breach

SA

Sanctions

Compliance

Guidance

Administration

Subject matter experts

Stakeholders

Commissioners

Head of investigation

Investigator

Expert

European cooperation

Key data protection stakeholders

- Monitor and enforce the application of the data protection framework
- Advise the national parliament and government
- Provide guidance and inform the general public
- Handle complaints and conduct investigations
- Accredit the certification bodies
- Cooperate with other supervisory authorities
- Publish an annual activity report including:
  - A list of types of infringement notified
  - A list of types of imposed sanctions
- Verify data breach notifications
- DPIA: prior consultation of the SA in case of remaining high resiual risks

Key data protection stakeholders

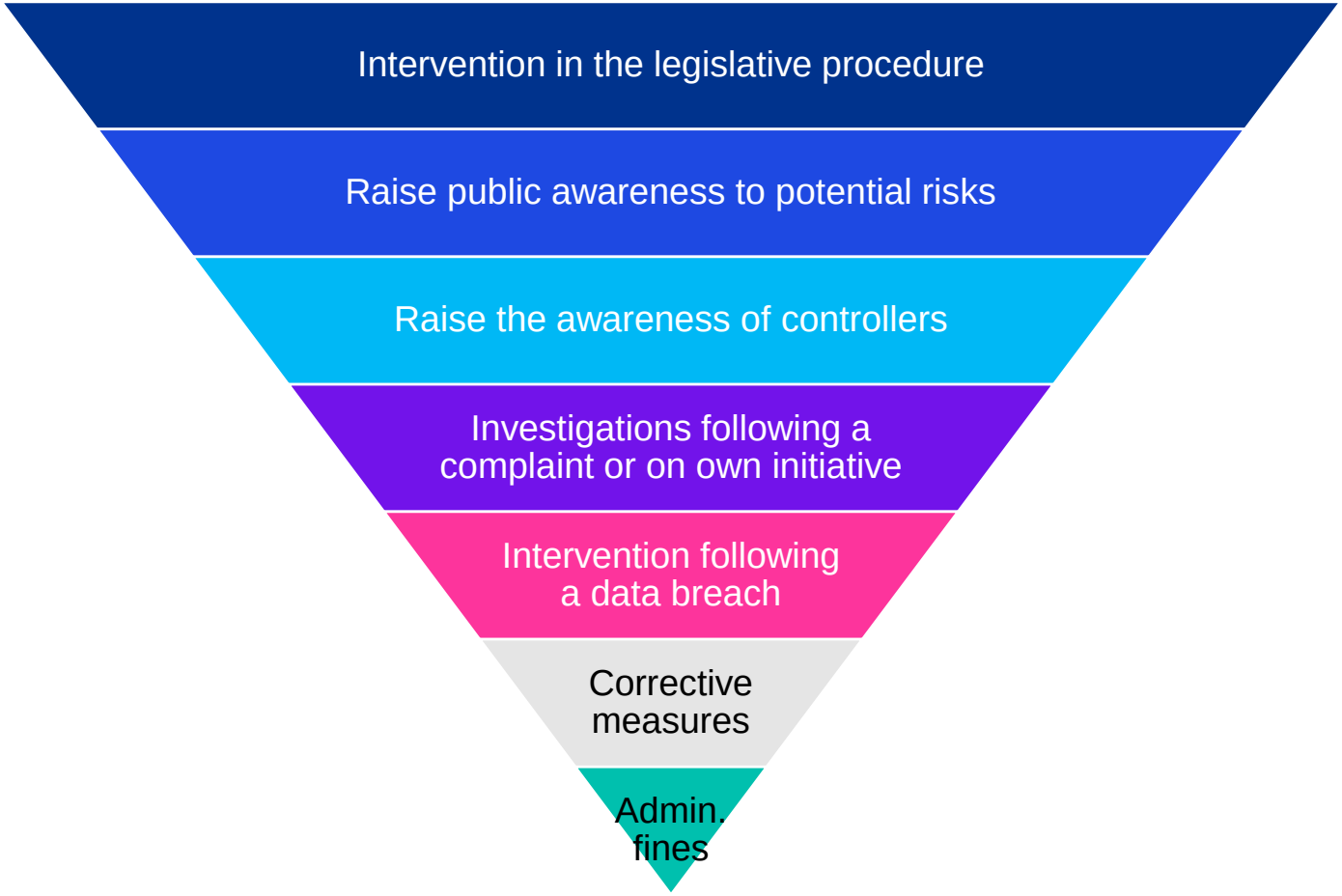
- Art. 58 of the GDPR: “Each supervisory authority shall have all of the following investigative powers:”
  - To carry out investigations in the form of data protection audits;
  - To obtain, from the controller and the processor, access to all personal data […];
  - To obtain access to any premises of the controller and the processor […]

Key data protection stakeholders

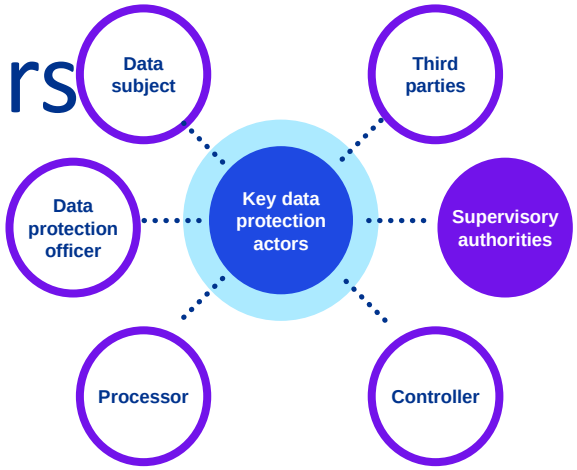
- Issue warnings and reprimands
- Order the controller / processor to bring processing operations into complianc with the GDPR
- Impose a temporary or definitive limitation, including a ban on processing

Infringements can be subject to a max. administrative fine of up to 20 million EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year

Key data protection stakeholders



Key data protection stakeholders



European Data Protection Board

The European Data Protection Board (EDPB) is an independent European body with legal personality. It ensures that the General Data Protection Regulation and the Law Enforcement Directive are applied consistently and ensures cooperation, including on enforcement.

The EDPB is composed of the heads of the national data protection authorities (Supervisory Authorities) of the countries in the European Economic Area, as well as the European Data Protection Supervisor (EDPS).

The data protection authorities are responsible for enforcing data protection law at a national level and at a cross-border level by cooperating through the one-stop-shop mechanism.

The EDPB takes binding decisions on cross-border cases on which no consensus is reached.

The EDPB has a Secretariat, based in Brussels and provided by the EDPS. A Memorandum of Understanding determines the terms of cooperation between the EDPB and the EDPS.

Data protection principles

Data protection principles

01
Lawfulness, fairness and transparency

02
Purpose limitation

03
Data minimisation

04
Accuracy

05
Storage limitation

06
Integrity and confidentiality

07
Accountability

Data protection prin

1. Lawfulness = legal basis for processing (1/2)

"General regime" = processing activity permitted, if:

- ✓ *Consent*
- ✓ *Necessary for compliance with a legal obligation*
- ✓ *Necessary for a contract or pre-contractual measures*
- ✓ *Necessary for a mission in the public interest*
- ✓ *Necessary to protect the vital interest of the data subject*
- ✓ *Necessary for the legitimate interest of the controller*

Data protection prin

1. Lawfulness = legal basis for processing (2/2)

Sensitive data = processing activity prohibited except when allowed by the GDPR:

- ✓ ***Explicit consent,*** *unless where law states that prohibition may not be lifted*
- ✓ *Processing is necessary for the purposes of carrying out the obligations and exercising specific* ***rights of the controller or of the data subject in the field of employment and social security and social protection law*** *on the basis of a legal obligation or collective agreement…*
- ✓ *Etc.*

Data protection prin

2. Purpose limitation

Purpose *= objective pursued by the controller for the processing of personal data*

- ✓ *Purpose(s) must be defined in advance*
- ✓ *Data must only be collected for specified, explicit and legitimate purpose(s)*
- ✓ *Data cannot be further processed in a way incompatible with the initial purposes (criterion = reasonable expectation of the data subject)*

Data protection prin

3. Data minimisation

Only process the data necessary to achieve the purpose

- ✓ *Data must be adequate, relevant and not excessive in relation to the purposes for which they are collected*

Need to have, not nice to have

4. Accuracy

The data must be accurate and, if necessary, kept up to date

- ✓ *Every effort must be made to delete or rectify inaccurate or incomplete data*

Data protection prin

5. Storage limitation

Do not store data for longer than is necessary for the purposes for which the data are processed

- ✓ *If the purpose is fully achieved, the data must either be (definitively) erased or (fully) anonymised*
- ✓ *The adequate retention period depends on the purpose*
- → *case-by-case analysis*

!**Data cannot be retained forever only because it **might perhaps** be useful **one day!

Data protection prin

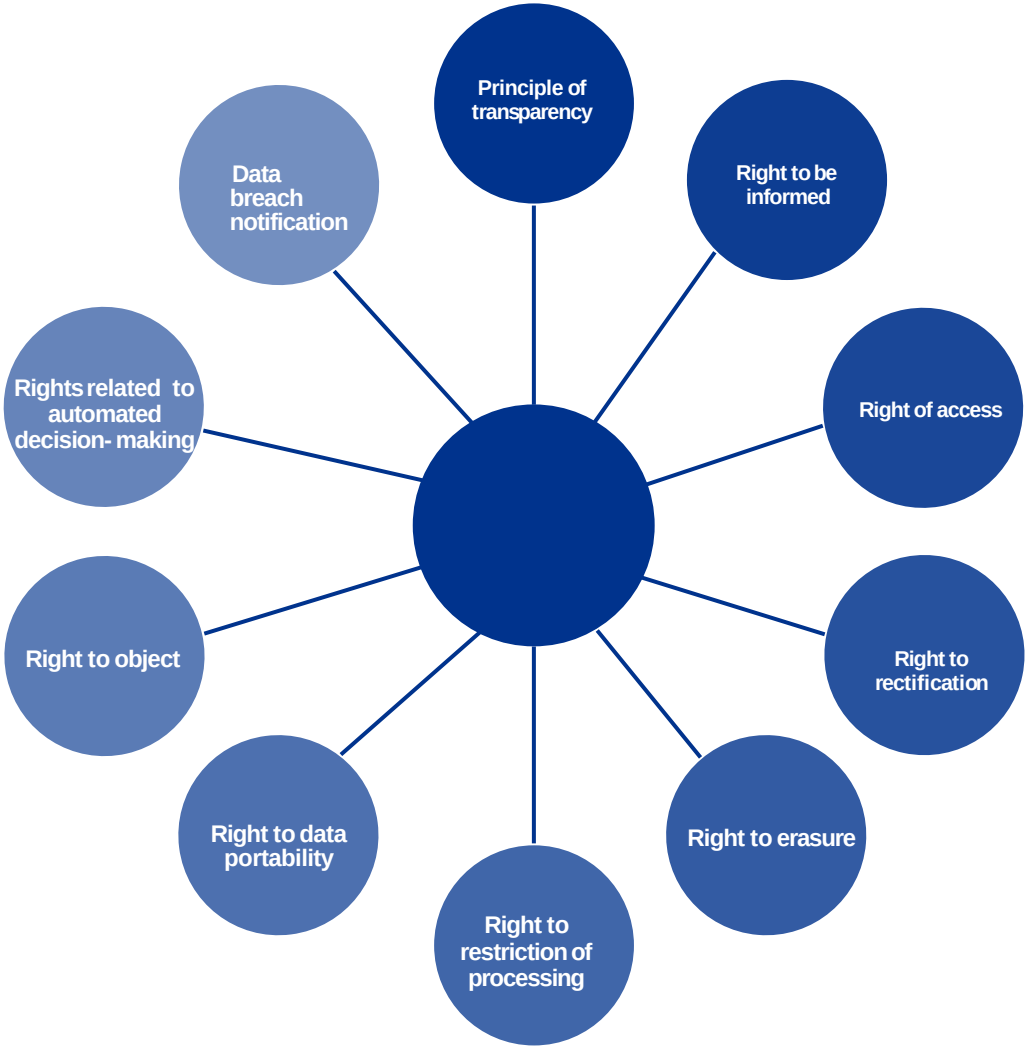
7. Accountability

Implement appropriate measures & be able to demonstrate compliance

- *How?*
  - ✓ *Organisational and technical measures*
  - ✓ *Maintaining documentation demonstrating compliance with the GDPR requirements*
  - ✓ *Transparency towards the data subject and the CNPD*

Individual rights and remedies according to the GDPR

Rights of the data subject



Right to be informed

The data are collected	Directly	Indirectly
The identity and contact details of the controller (& representative, if applicable)	☑	☑
The contact details of the DPO (if applicable)	☑	☑
The purposes of the processing, the legal basis for the processing and the legitimate interests (if processing is founded on legitimate interest)	☑	☑
The categories of personal data concerned		☑
The recipients or categories of recipients of the personal data	☑	☑
The transfers of personal data to third countries (including safeguards)	☑	☑
The storage duration (or, if impossible, the criteria used to determine that period)	☑	☑
The rights of the DS	☑	☑
The rights to withdraw consent (if applicable)	☑	☑
The right to lodge a complaint with a supervisory authority	☑	☑
The source of the personal data (incl. if from publicly accessible sources)		☑
If there is a statutory or contractual requirement to provide the data, if the provision of the personal data is obligatory & possible consequences of a refusal	☑	
If automated decision-making, incl. profiling, is used (if so, meaningful information about the logic, significance & envisaged consequences for the DS)	☑	☑
Further processing of the personal data	☑	☑

Right to be informed

Timeframe

- If the data are **collected directly** from the DS:
  - When the data are collected from the data subject
- If the data are **not collected directly** from the DS:
  - Within a reasonable time (max. 1 month) of the collection
- If the data are collected to communicate with a DS or to transmit the data to another controller
  → during the first communication with the data subject / to the new controller

Exceptions (direct)

- The DS already has the information

Exceptions (indirect)

- The DS already has the information
- Impossible or disproportionate effort
- Collection or disclosure foreseen by law
- Professional secrecy

Right of access

Elements

The right to be informed whether or not their data are being processed and, if so, the right to access the data and to be informed about

- The purpose and the categories of personal data concerned
- The recipients (in particular in third countries)
- The storage duration (or the criteria used to determine that period)
- The DS rights, incl. the right to lodge a complaint with a DPA
- The source of the personal data (if collected indirectly)
- If automated decision-making, incl. profiling, is used (if so, meaningful information about the logic, the significance & consequences)

The right to receive a (free) copy of the personal data

Timeframe

- Without undue delay and in any event within 1 month of the request (possible extension of 2 months)

Exceptions

- The rights shall not adversely affect the rights and freedoms of others

Right to rectification

Elements

The right to obtain the correction or completion of incomplete or incorrect data

- Inaccurate data → rectification
- Incomplete data → completion

Timeframe

- Without undue delay and in any event within 1 month of the request (possible extension of 2 months)

Notification

- Obligation to notify the rectification to each recipient to whom the data have been disclosed (unless impossible or disproportionate effort)
- Obligation to inform the DS of these recipients, at the request of the latter

Right to erasure

Elements

The right to have personal data deleted without undue delay, if:

- The data are no longer necessary
- Withdrawal of consent
- The DS exercises right to object
- Unlawful processing
- Legal obligation requiring deletion

Timeframe

- Without undue delay and in any event within 1 month of the request (possible extension of 2 months)

Exceptions

- The right of freedom of expression and information
- Compliance with a legal obligation
- Reasons of public interest in the area of public health
- Archiving purposes (*in limited cases)*
- The establishment, exercise or defence of legal claims

Notification

- If the personal data have been made public, inform controllers that an erasure request has been made
- Obligation to notify the erasure to each recipient to whom the data have been disclosed (unless impossible or disproportionate effort)
- Obligation to inform the DS of these recipients, at the DS' request

Right to restriction of processing

Content

- The right to obtain restriction of processing

When?

- Rectification request
- Objection request – unlawful processing
- Objection request – illegitimate interests
- Data is no longer necessary

Consequences

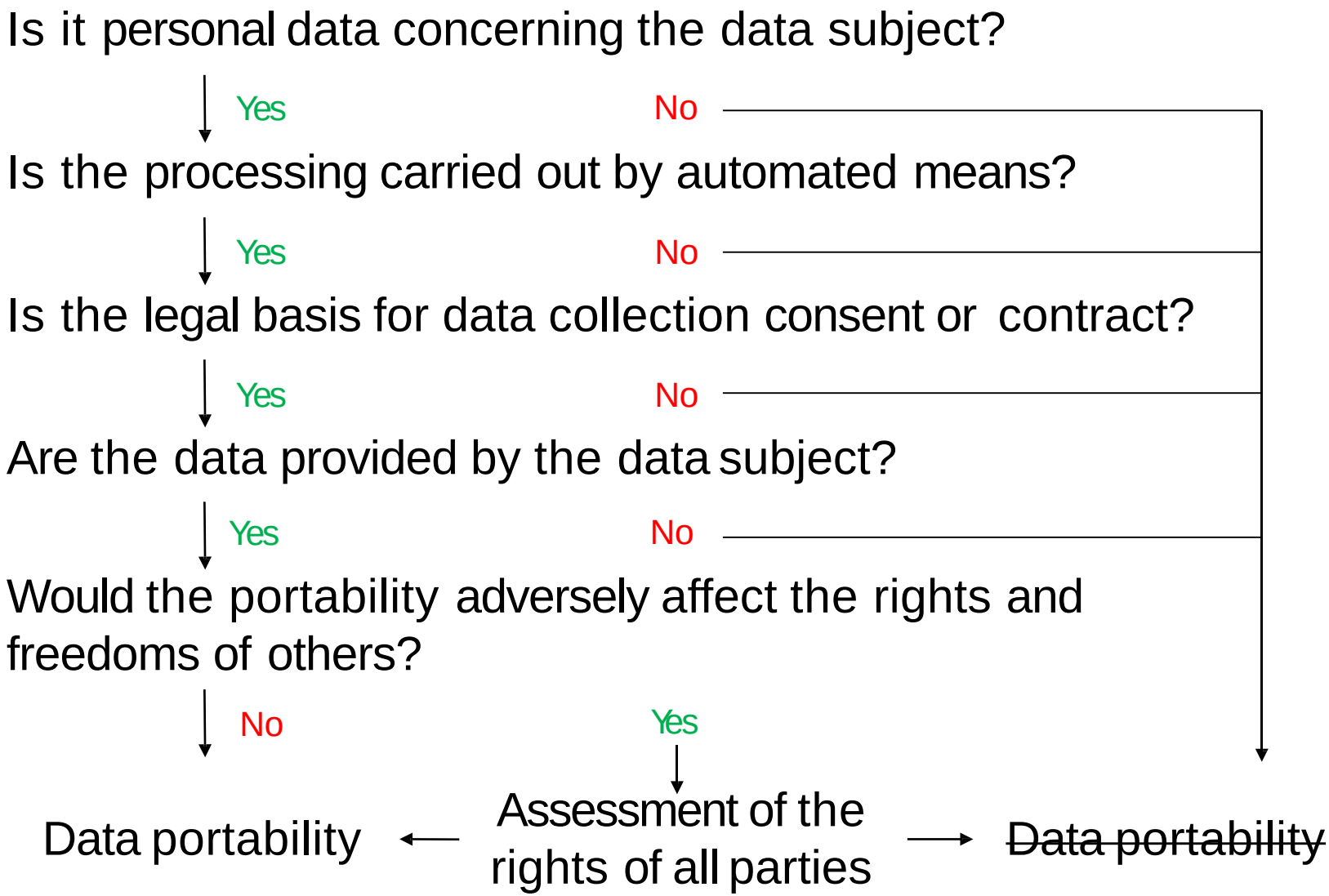
- Storage period of data
- “Prohibited processing”

Right to data portability

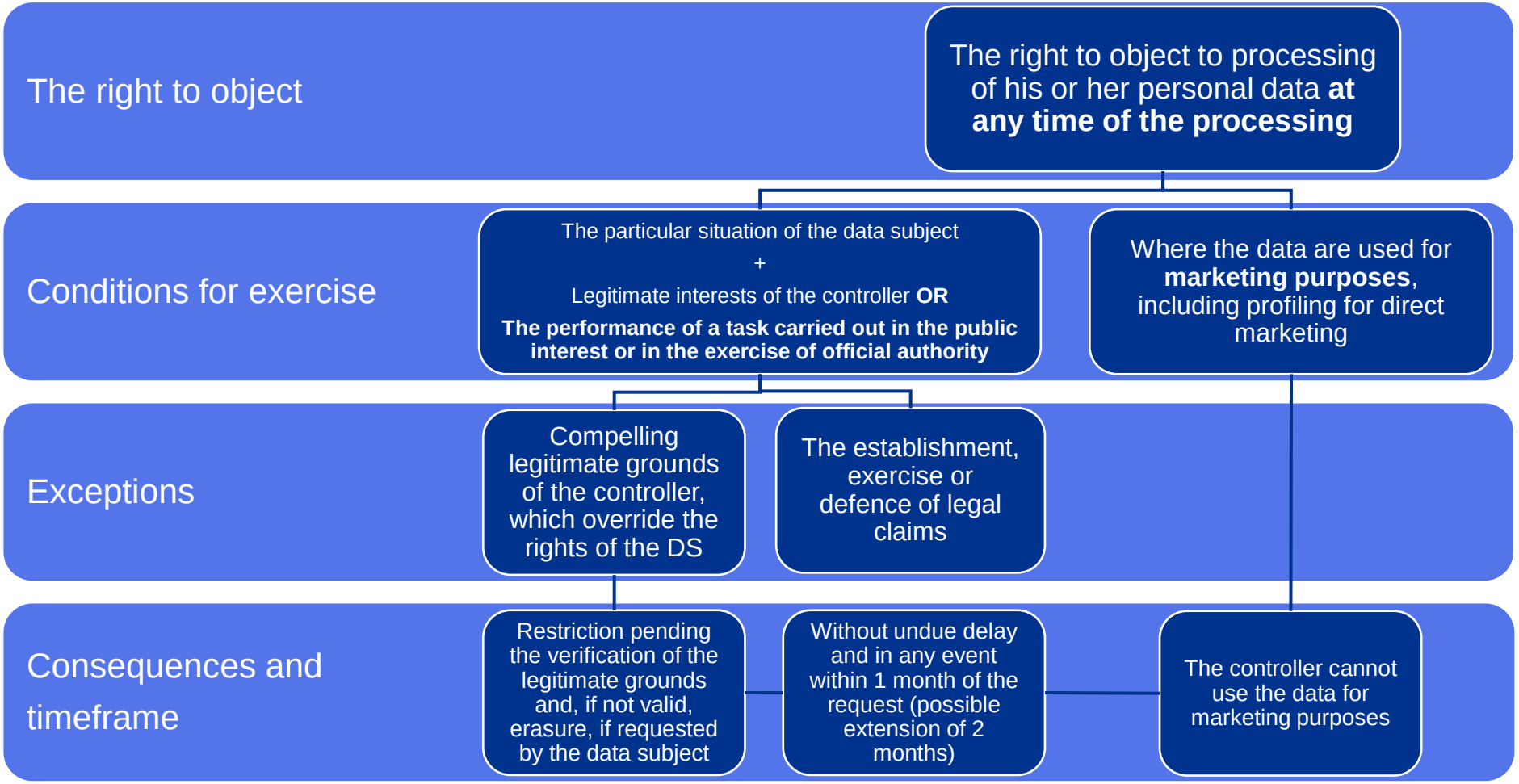
The right to **receive** the personal data concerning him or her from the controller

The right to **transmit** those data to another controller where technically feasible

Right to data portability



Right to object



Principle – Automated individual decision-making

The right **not to be subject to a decision**…

…**based solely on automated processing**, including profiling…

… which produces **legal effects**…

… or **similarly significantly affects the data subject.**

Legal bases – Automated individual decision-making

The processing can be carried out if it is:

- ✓ **Necessary** for entering into or perfomance of a **contract**
- ✓ Authorised by **Union or Luxembourgish law**
- ✓ Based on the data subject's **explicit consent**

Transparency and modalities

Put in place **procedures and measures** to facilitate the exercise of data subjects' rights

- Review information notices
  - ✓ Concise, transparent, easily understandable and accessible
  - ✓ Use clear and plain language
- Review current procedures provided to data subjects to exercise right
  - ✓ Respect the strict deadlines
  - ✓ Provide easy access to information about processing and facilitate the exercise of rights
    - E.g. designate contact person / department incl. contact details
  - ✓ Technical and organisational measures
    - E.g. internal organisation, employee training, contracts with processing, IT systems, up-to-date list of recipients

Transparency and modalities

The exercise of the rights is free, unless the requests are manifestly unfounded or excessive (esp. due to their repetitive nature)

- The request can be rejected or a fee can be charged
  - Burden of proof on the controller
  - Manifestly unfounded or excessive
    - Does not cover the overall cost of the controllers' processes
    - Concerns the requests made by one data subject

"Customer-focused" approach

- Prompt,
- Transparent and
- Easily understandable communication

Transparency and modalities

Designate the competent department(s) and / or contact person(s)

Confirm the identity of DS

Analyse the nature of the right(s) exercised

Acknowledge receipt of the request

Provide information on actions taken **without undue delay**

Information provided within max. 1 month

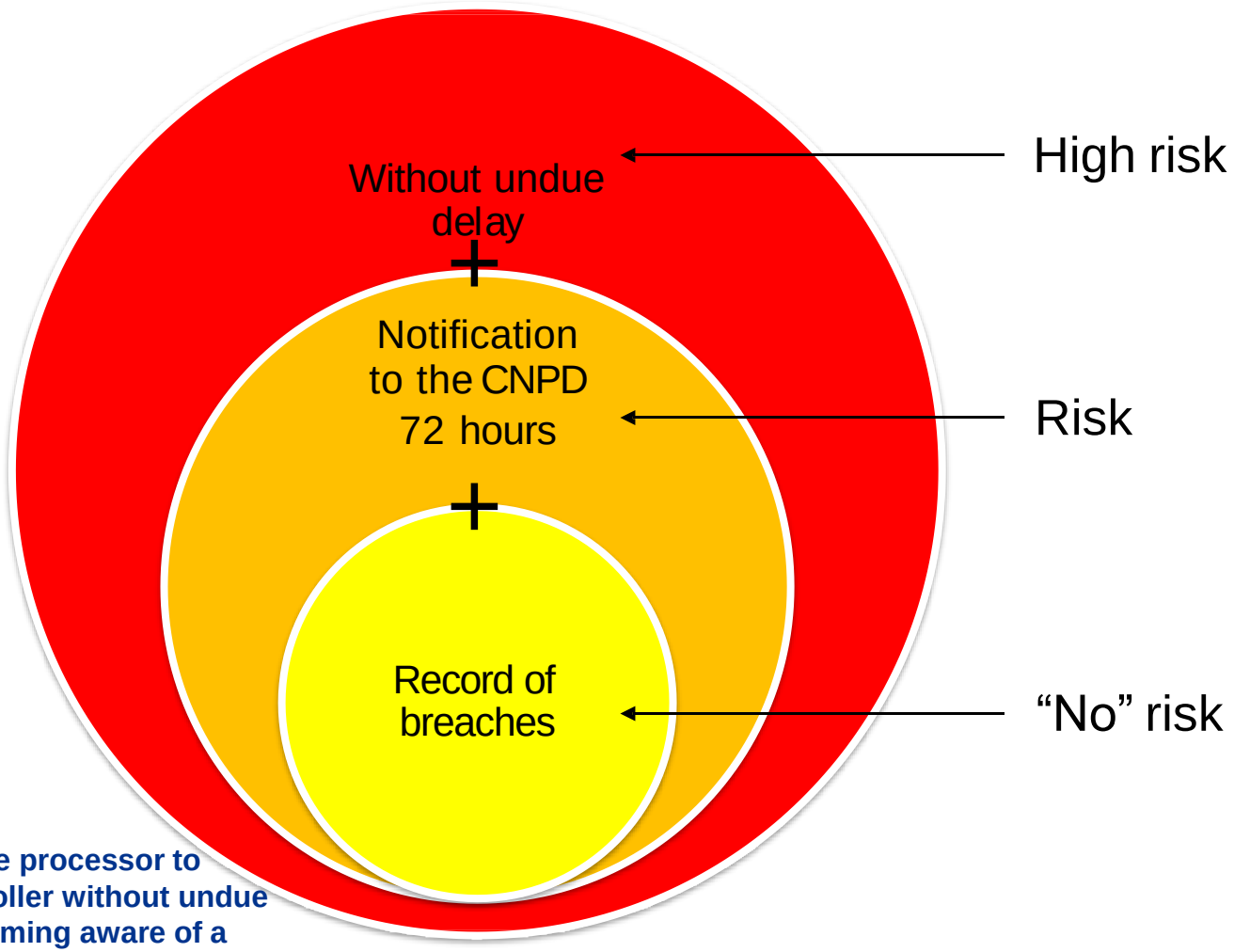
Information <u>cannot be provided</u> within 1 month:

Inform DS of the extension **within 1 month of receipt of request** (with reasons for the delay) possible extension by 2 months

If no action is taken, inform DS **without undue delay** (max. within 1 month of receipt)

Inform DS about right to lodge a complaint with the CNPD

Data Breach notification



Obligation of the processor to notify the controller without undue delay after becoming aware of a personal data breach

WORKSHOP: Exercising selected data subjects' rights

WORKSHOP: Exercising selected data subjects' rights

Thank you!