CNPD Course:
Data Protection Basics

Basic elements

Esch-sur-Alzette

4 September 2018

Carmen Schanck

Legal Department

Outline

1. Introduction
2. **Basic elements**
3. The rights of data subjects
4. The obligations of controllers and processors
5. The role of the CNPD

Basic elements - Overview

1. Legal framework
2. What is "personal data"?
3. What is "processing"?
4. Key data protection actors
5. Main principles

1. Legal framework (1/3)

- Regulation (EU) 2016/679 of 27 April 2016 "**the GDPR**"
- Directive (EU) 2016/680 of 27 April 2016 ("Criminal Justice Directive")
- Act of 11 August 1982 on the protection of privacy
- Amended Act of 2 August 2002, implementing Directive 95/46/EC has been ***repealed***
- **Act of 1 August 2018** on the organisation of the National Data Protection Commission and the general data protection framework
- **Act of 1 August 2018** on the protection of individuals with regard to the processing of personal data in criminal and national security matters
- Amended Act of 30 May 2005, implementing Directive 2002/58/EC (electronic communications)

1. Legal framework (2/3)


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

"GDPR"

I

(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,

- *New legal framework*

✓ Strengthening of individuals' rights

✓ An increased responsibility for controllers

✓ A more important role for data protection authorities

- *Harmonisation:*

✓ The same rules in all 28 countries of the EU

✓ Directly applicable (since 25 May 2018)

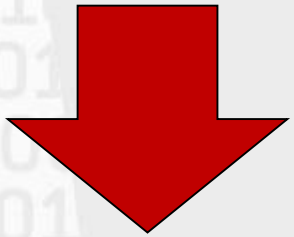
✓ To all organisations active on EU territory

1. Legal framework (3/3)

A paradigm shift

Prior formalities

Prior control



Principle of Accountability

Subsequent control

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

2. What is "personal data"? (1/3)

"Any information relating to an identified or identifiable natural person …"

Article 4(1) GDPR

2. What is "personal data"? (2/3)

- *"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

2. What is "personal data"? (3/3)

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

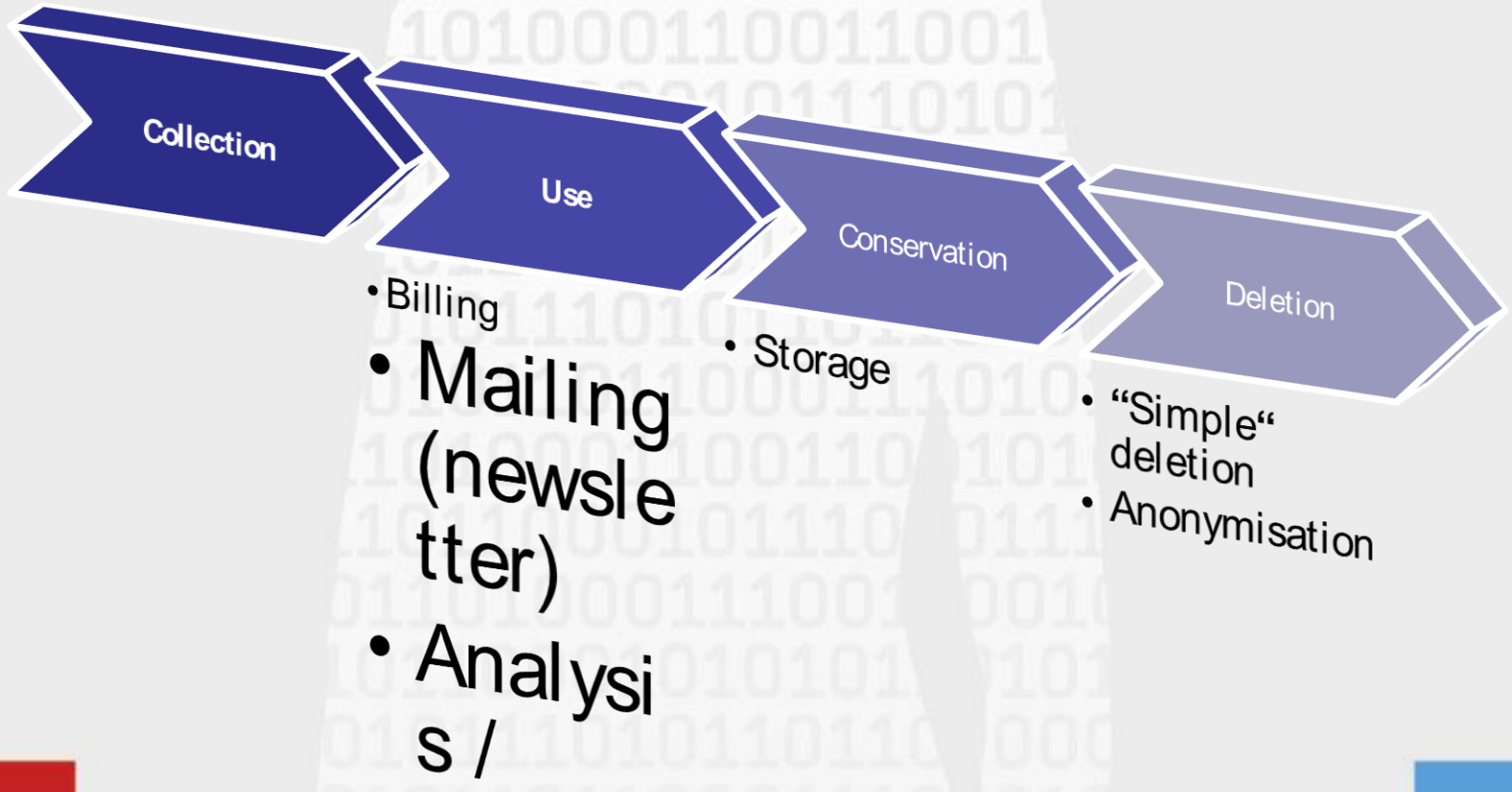
3. What is “processing”? (1/2)

“*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*”

Art.4 (2) GDPR

3. What is “processing”? (2/2)

The life-cycle of a processing activity:



4. Key data protection actors (1/3)

- Data subject
- Third parties
- Supervisory authorities
- Controller
- Processor
- Data protection officer

4. Key data protection actors (2/3)

- *Controller*
  - ✓ determines the purposes and means of the processing
- *Processor*
  - ✓ processes personal data on behalf and upon instruction of the controller

4. Key data protection actors (3/3)

- *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

5. Main principles (1/7)

Lawfulness, fairness and transparency

Purpose limitation

Data minimisation

Accuracy

Storage limitation

Integrity and confidentiality

Accountability

5. Main principles (2/7)

3.1 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

5. Main principles (3/7)

3.1 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.

5. Main principles (4/7)

3.2 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)

5. Main principles (5/7)

3.3 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

3.4 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

5. Main principles (6/7)

3.5 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* !

5. Main principles (7/7)

3.6 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

Thank you for your attention!

carmen.schanck@cnpd.lu

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

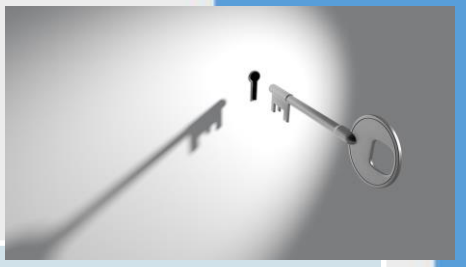
Exceptions (direct)

- 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 purposes 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 right 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

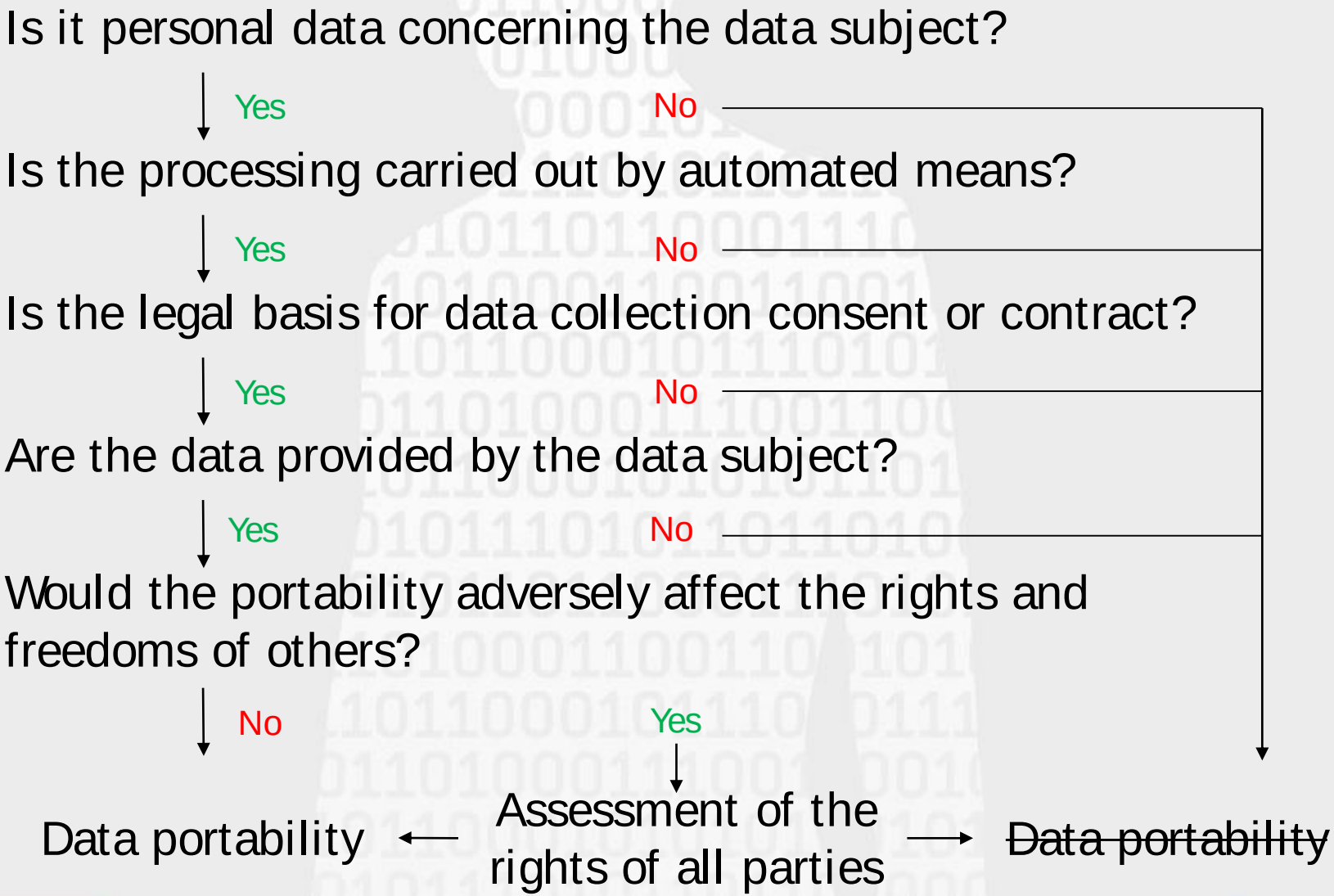
Consequences:

- 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

The right to object

The right to object to processing of his or her personal data at **any time of the processing**

Conditions for exercise

The particular situation of the data subject

+

Legitimate interests of the controller, **OR**

The performance of a task carried out in the public interest or in the exercise of official authority

Where the data are used for **marketing purposes,** *including profiling for direct marketing*

Exceptions

Compelling legitimate grounds of the controller, which override the rights of the DS

The establishment, exercise or defence of legal claims

Consequences and timeframe

Restriction pending the verification of the legitimate grounds and, if not valid, erasure, if requested by the data subject

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

The controller cannot use the data for marketing purposes

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 performance of a contract
  - authorised by Union or Luxemburgish law
  - based on the data subject's explicit consent

Transparency and modalities

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

*Uwe Kils,

Remedies

Right to lodge a complaint with the CNPD

- **WHERE?**
  - Authority of his **habitual residence**,
  - Authority of his **place of work**,
  - Authority of the **place of the alleged infringement**.
- The supervisory authority shall inform the data subject within three months on the progress or outcome of the complaint lodged.

Right to an effective judicial remedy against a supervisory authority

- Each natural or legal person has the right to an effective judicial remedy against a « **legally binding decision of a supervisory authority** concerning them » or a **failure to reply within three months**.
- The courts of the Member State where the supervisory authority is established are competent.

Right to an effective judicial remedy against a controller or processor

- **Each data subject has the right to an effective judicial remedy** in case of an infringement of his rights against the controller or the processor (before the courts of the Member State where the data subject has his habitual residence or the Member State where the controller has an establishment).

Remedies

Right to compensation

Principle: compensation for material or non-material damage suffered by any person resulting from an infringement of the Regulation can be received from the controller or processor.

Processor: Non-compliance with the obligations of the GDPR OR where it acted outside or contrary to lawful instructions of the controller.

In case of responsibility of the controller and the processor : responsibility for the entire damage

Thank you very much for your attention !

CNPD Training:
Data Protection Basics

The obligations of controllers and processors

Esch-sur-Alzette

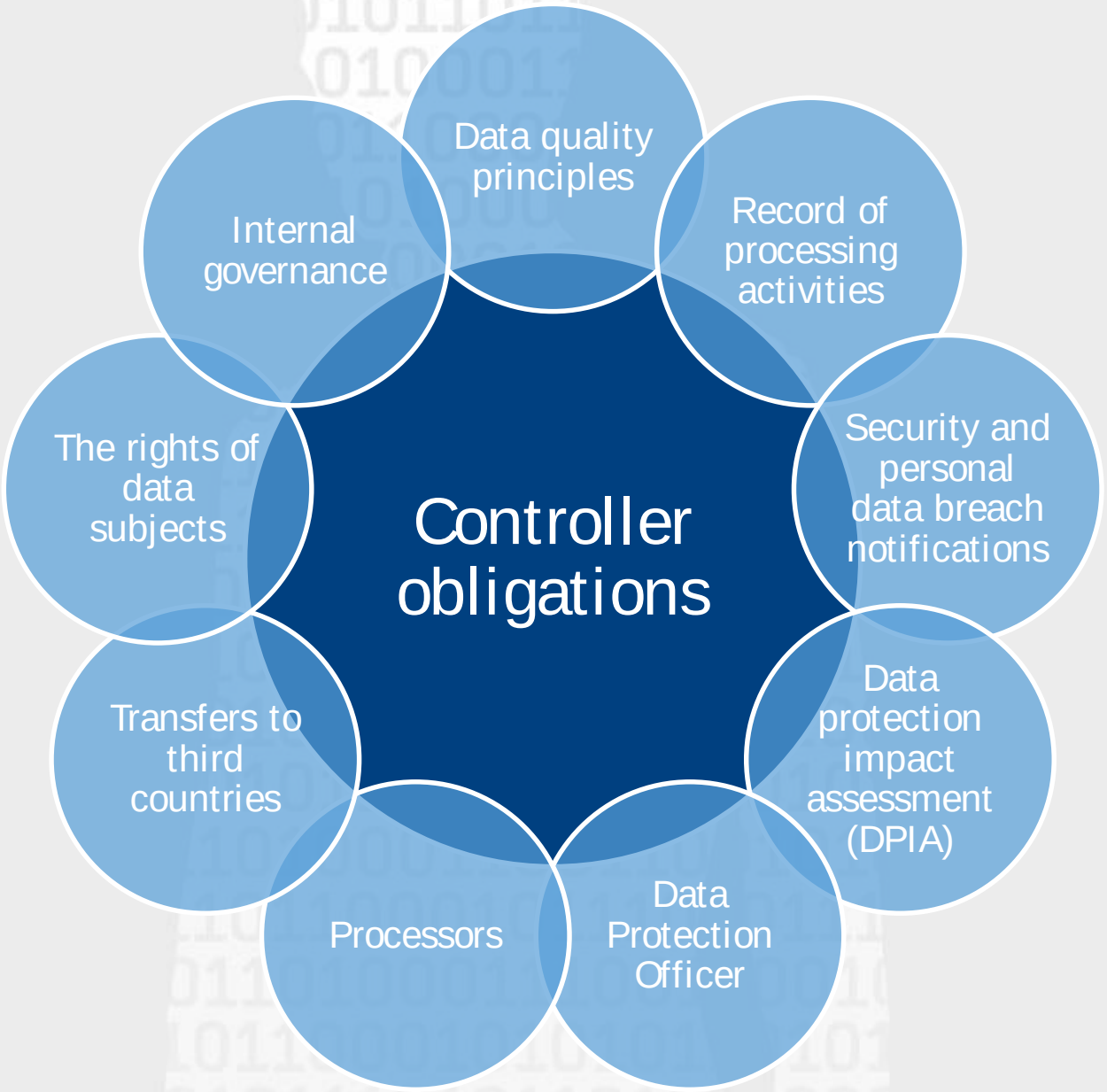
4 September 2018

Mathilde Stenersen

Legal service

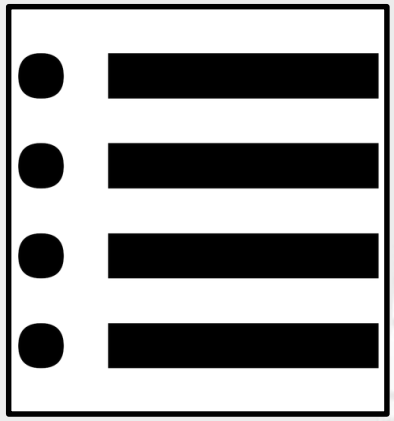
Outline

1. Introduction
2. Basic elements
3. The rights of the data subjects
4. **The obligations of controllers and processors**
5. The role of the CNPD


Controller obligations
Data quality principles
Record of processing activities
Security and personal data breach notifications
Data protection impact assessment (DPIA)
Data Protection Officer
Processors
Transfers to third countries
The rights of data subjects
Internal governance

1. Data quality principles

2. Record of processing activities



A document/file which describes all your processing activities

GDPR: Record indicating (at least) the following information for each processing activity:

a) the name and contact details of the controller (…)
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed (…)
e) where applicable, transfers of personal data to a third country or an international organisation (…)
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of the technical and organisational security measures(…)

Exemples:

- « Compliance Support Tool » of the CNPD which also contains a register
- Other tools: CPVP (Belgian authority), CNIL (French authority)

Format: The Regulation does not specify the format of the record. While the above example may aid in the set up of the record, we advise setting up a record, which suits the needs of your organisation, both in terms of format and vocabulary.

2. Record of processing activities
Basic Checklist

Objective: Provide a practical tool to carry out a basic assessment your level of readiness for a specific processing activity

The suggested checklist is based of the data quality principles set out in the GDPR (Article 5). While not exhaustive, it may be helpful to begin the assessment your processing activities. The in-depth analysis must be made on the basis of the GDPR.

2. Record of processing activities
Basic Checklist

Fact sheet

Roles and responsibilities
- Analyse whether you decide what is done with the data or if you execute orders

Purposes of the processing
- Describe the objective of the processing (e.g. payment of salary, invoicing, marketing,…)

Data processed
- List the types of data processed (e.g. names, addresses, illness notices, accountancy documents,…)

Data subjects
- List the categories of persons whose data are processed (e.g. clients, employees, sales leads,…)

Erasure
- Describe when the data will be deleted or the required processing duration

Data flows
- Analyse whether you receive or transfer data to other organisations, including those located outside the EU

This document is based on the information that must be contained in the register, as required by Article 30 GDPR.

Questionnaire

	Questions	Comment
1	Is my processing activity lawful?	**Principle:** Lawfulness
2	Have the data subject been informed about the processing activity?	**Principle:** Transparency
3	Do I use data for other purposes / do I use data that are collected for another purpose?	**Principle:** Purpose limitation
4	Are all the data necessary – and not only useful?	**Principle:** Data minimisation
5	Are the data accurate and up-to-date?	**Principle:** Accuracy
6	Must I delete the data at the end of the processing activity or are there other obligations to keep the data?	**Principle:** Storage limitation
7	Are the data sufficiently secure?	**Principle:** Integrity and confidentiality

The questionnaire is based on the data quality principles, as set out in Article 5 GDPR

2. Record – examples

Fiche de registre	ref-000
Description du traitement	
Nom / sigle	
N° / REF	ref-000
Date de création	
Mise à jour	

Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
Responsable du traitement						
Délégué à la protection des données						
Représentant						
Responsable(s) conjoint(s)						

Finalité(s) du traitement effectué
Finalité principale
Sous-finalité 1
Sous-finalité 2
Sous-finalité 3
Sous-finalité 4
Sous-finalité 5
Mesures de sécurité
Mesures de sécurité techniques
Mesures de sécurité organisationnelles
Catégories de données personnelles concernées
Etat civil, identité, données d'identification, images...
Vie personnelle (habitudes de vie, situation familiale, etc.)
Informations d'ordre économique et financier (revenus, situation financière,
Données de connexion (adress IP, logs, etc.)
Données de localisation (déplacements, données GPS, GSM, etc.)

Example

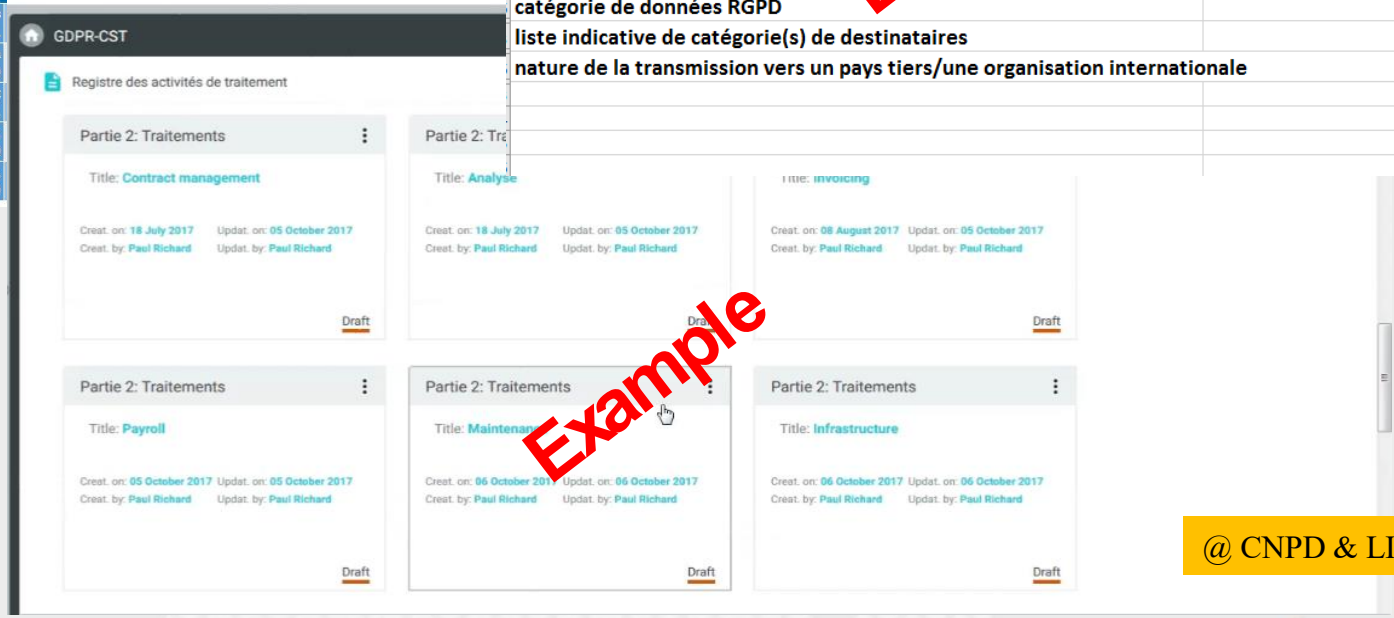
@ CNIL

Vous trouverez dans cet onglet quelques listes qui pourront vous aider à compléter le registre.

A
Vous trouverez dans cet onglet quelques listes qui pourront vous aider à compléter le registre.
Ces listes sont indicatives, tant en ce qui concerne le niveau de détail que l'exhaustivité. Il incombe au responsable du traitement d'indiquer au besoin des informations plus détaillées au sujet du traitement.
Cliquez sur le '+' à côté du nom d'une liste pour l'ouvrir.
Liste indicative de types de finalités
Fondement du traitement
Liste indicative des catégories de données fonctionnelles
type de traitement
catégorie de données RGPD
liste indicative de catégorie(s) de destinataires
nature de la transmission vers un pays tiers/une organisation internationale

Example

@ CPVP



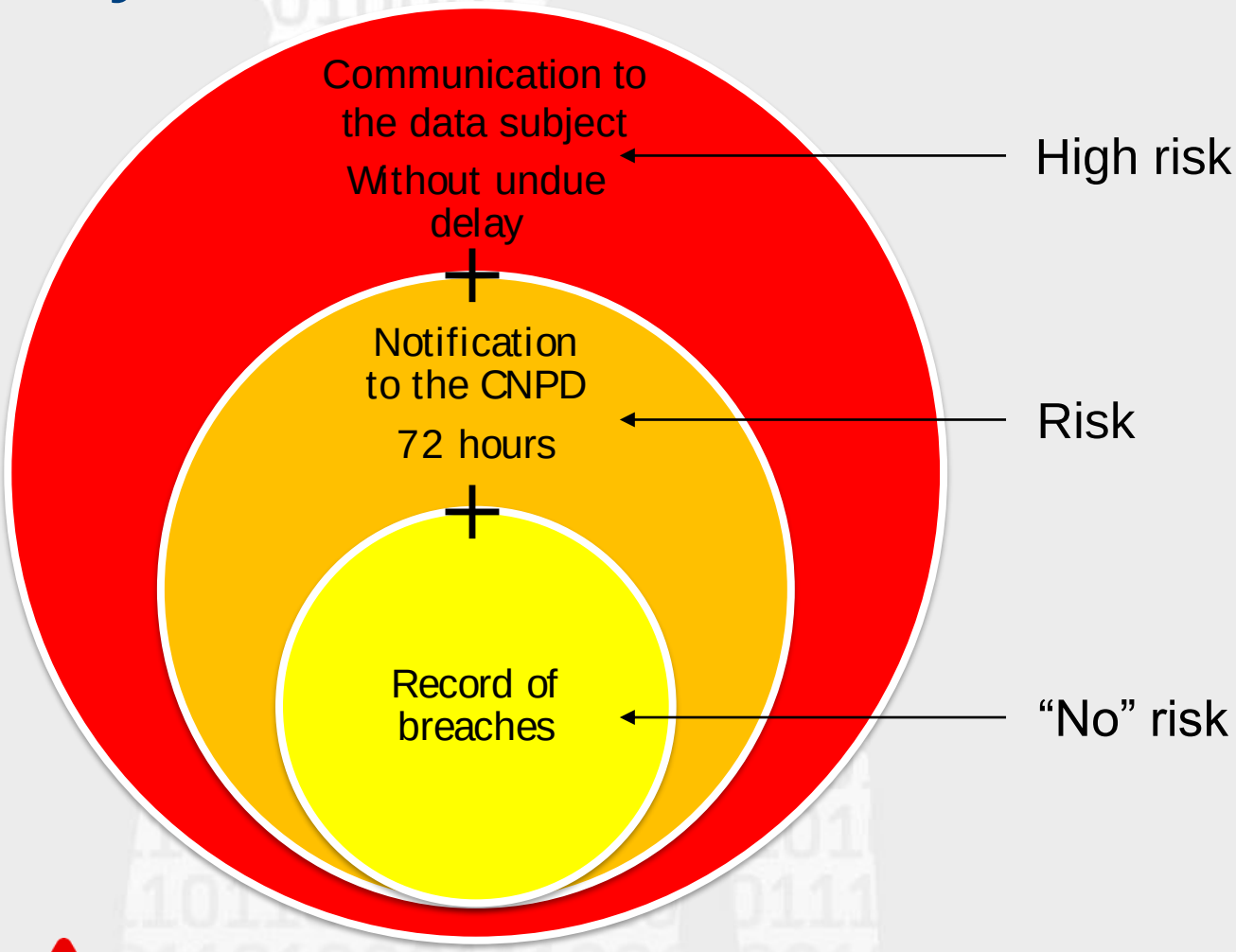
Example

@ CNPD & LIST

3. Security and data breach notifications

- Technical and organisational measures taking into account
  - the “ state of the art”
  - the risk for data subjects
- Measures to reduce risk must be adapted to the context and particularities of each sector
  - Analysis of risks : nature of data, legal prescriptions, complexity of the system, etc.
- The measures must be reviewed and updated on a continuous basis
  - New threats every day
  - New vulnerabilities
  - Changes in the organisation may occur → new risks

3. Security and data breach notifications



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

4. Data protection impact assessment

If data processing activities are likely to result in a high risk to the rights and freedoms of data subjects

The controller must carry out an

assessment of the impact

of the envisaged processing operations on the protection of personal data, to evaluate the risks

(**Data Protection Impact Assessment - DPIA**)

e.g. bike rental service with geolocation

4. Data protection impact assessment

The following criteria should be considered to decide if a DPIA is necessary:

- Evaluation or scoring, including profiling
- Automated decision-making with legal or similar significant effect
- Systematic monitoring of data subject
- Sensitive data
- Large scale processing
- Datasets that have been matched or combined
- Data concerning vulnerable data subjects
- Innovative use of personal data or application of technological or organisational solutions
- When the processing in itself "*prevents data subjects from exercising a right or using a service or a contract*"

5. Data Protection Officer

A data protection officer will be **mandatory after 25 May 2018 for a:**

- Public authority or body
- Undertaking fulfilling certain criteria (e.g. large scale processing of sensitive data)

Role: Information, advice, internal compliance function and contact point for the supervisory authority

5. Data Protection Officer

“Pilote à bord”

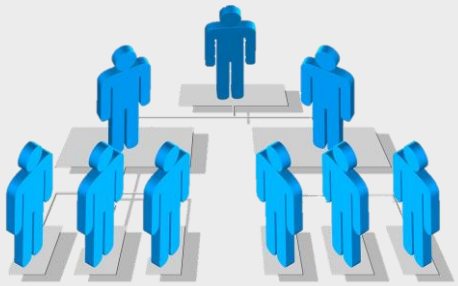
Major advantage for: compliance with the GDPR obligations, communication with supervisory authorities, managing litigation and liability risk

6. Processing

- The controller must :
  - Choose a sufficiently qualified processor and always keep control of the processing activities
  - Maintain oversight and control over sub-processing
  - Conclude a written contract with each processing, which sets out, amongst others, that:
    - The processors only processes the personal data on documented instructions of the controller
    - The obligations of the controller (e.g. security measures, confidentiality) also apply for the processor
    - The processor must assist the controller in being compliant with the requirements of the GDPR (e.g. rights of data subject, personal data breach notifications)

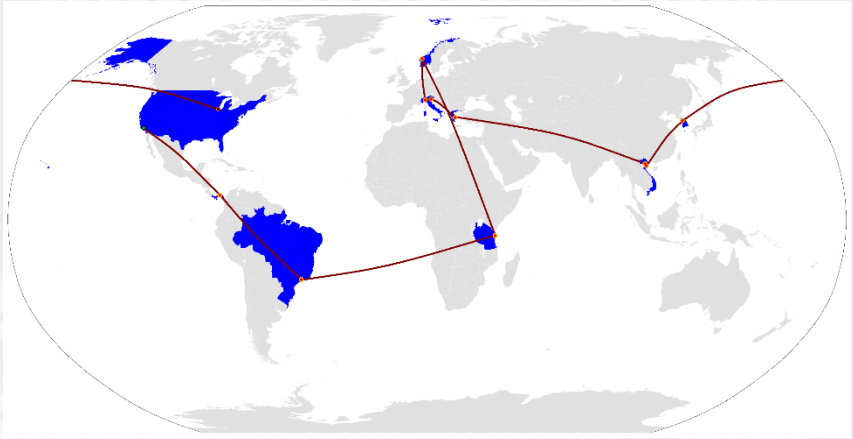
6. Processing

- Obligations of the processor
  - Only process the personal data on documented instructions of the controller
    - Observe the contract concluded with the controller
    - If a processor processes the data for other purposes, the processor becomes the controller for that processing activity
  - Sub-processing
  - Security measures
  - DPO
  - Record of processing activities
  - Transfers of personal data to third countries
  - Data breach notification
  - Cooperation with the CNPD



7. Transfers to third countries

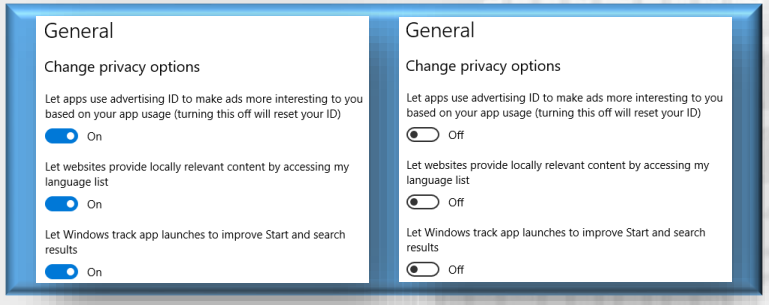
- Free flow of data within the EU/EEA
- Transfer of personal data to third countries (= outside the EU) only possible, if:
  - Adequacy decision
  - Adequate safeguards (e.g. BCRs or Standard Contractual Clauses, etc.)
  - Derogations for specific transfers (e.g. consent, contract, etc.)



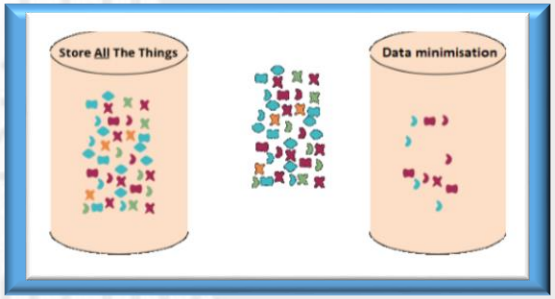
8. The rights of data subjects

9. Internal governance

- Develop a **data protection friendly culture**
- Taking into account the principle of **data protection by design and by default**



(*Privacy by design*)

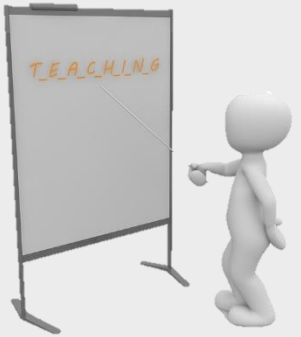


(*Privacy by default*)

- **Anticipate** the risks and possible issues
- Be able to react promptly in case of a data breach
- Develop **secure data management** throughout the **entire life cycle of the data processing**

9. Internal governance

- **Raise awareness** among employees
- Organise **internal reporting**



- Implement procedures to process **complaints and requests** from data subjects in relation to their rights
- **Be transparent and inform the public** about their rights

- Right to information
- Right of access
- Right to rectification
- Right to erasure
- Right to data portability…

9. Internal governance

- **Document** compliance
  - Record of processing activities,
  - DPIA,
  - Framework for the transfers of personal data outside the EU,
  - Record of data breaches,
  - Contracts with processors,
  - …
- **Obligation to cooperate with the CNPD**

Commission nationale pour la protection des données

1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette (Belval)
261060-1
www.cnpd.lu
info@cnpd.lu

CNPD Course:
Data Protection Basics

Presentation of Luxembourg's supervisory authority

Esch-sur-Alzette

4 September 2018

Dani Jeitz

Legal Department

Introduction

- Independent authority organised by the Act of 1 August 2018
- Public institution with financial and administrative autonomy having legal personality
- Monitors and verifies the compliance with the :
  - GDPR
  - Act of 1 August 2018 having specific provisions for:
    - Freedom of expression and information
    - Scientific or historical research and for statistical purposes
    - Processing of special categories of personal data
  - Act of 1 August 2018 in criminal / national security matters
  - Amended Act of 30 May 2005 (electronic communications)

New organisational setup (1/2)

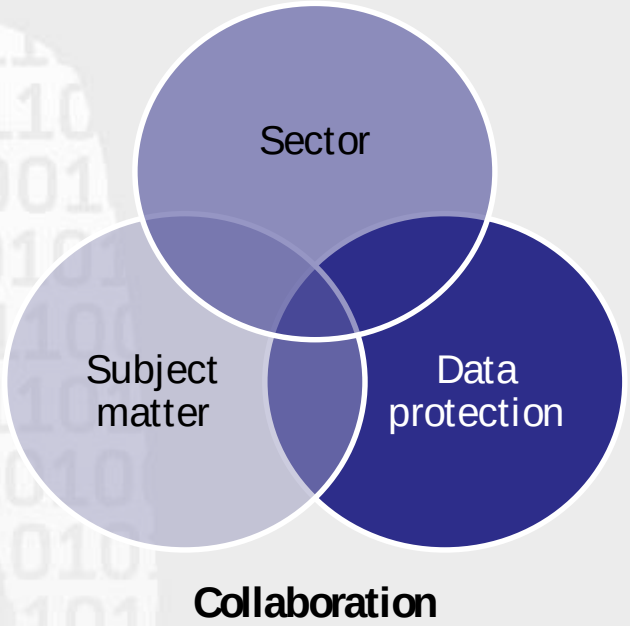
CNPD

Compliance

Guidance

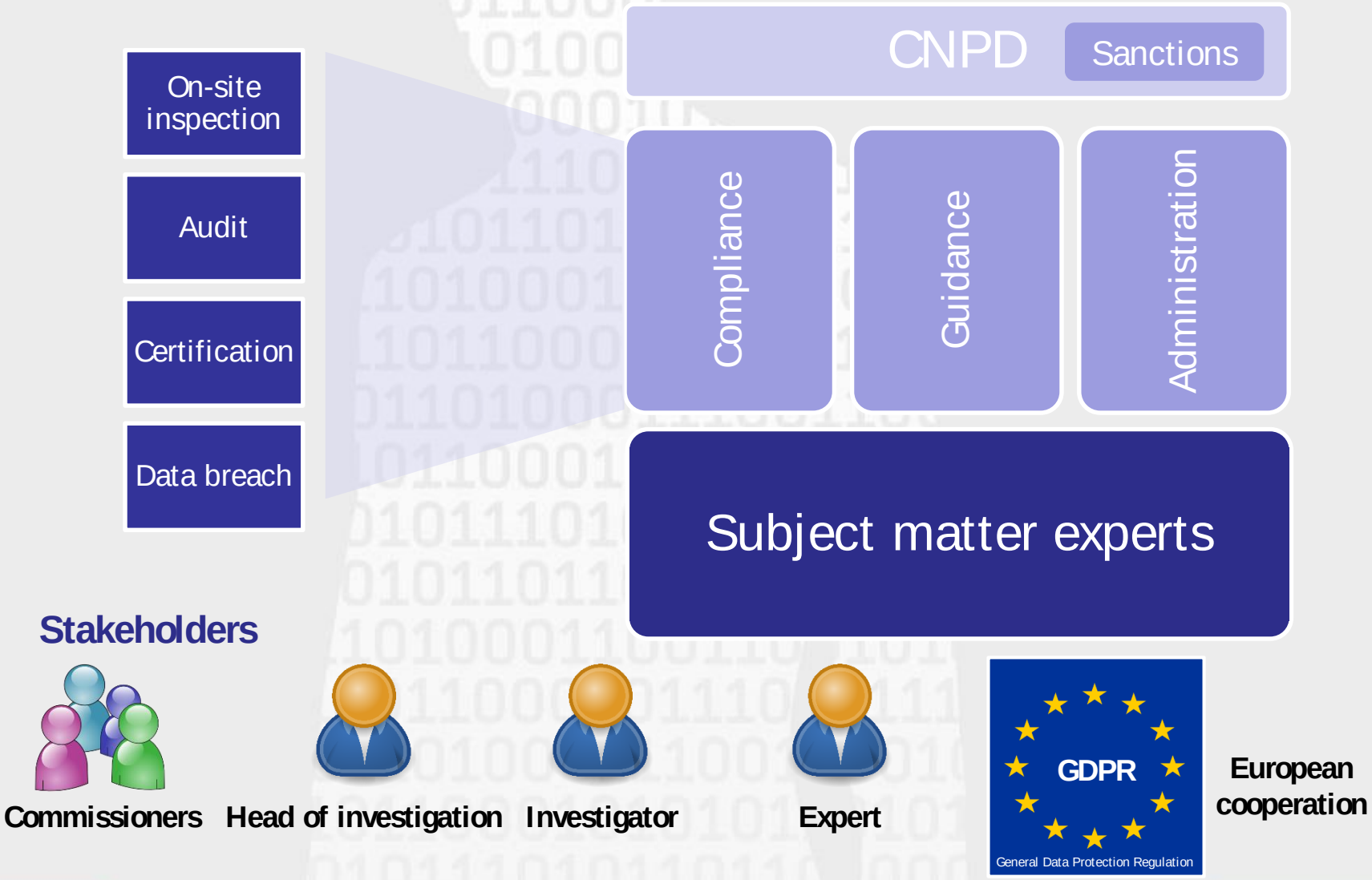
Administration

Subject matter experts

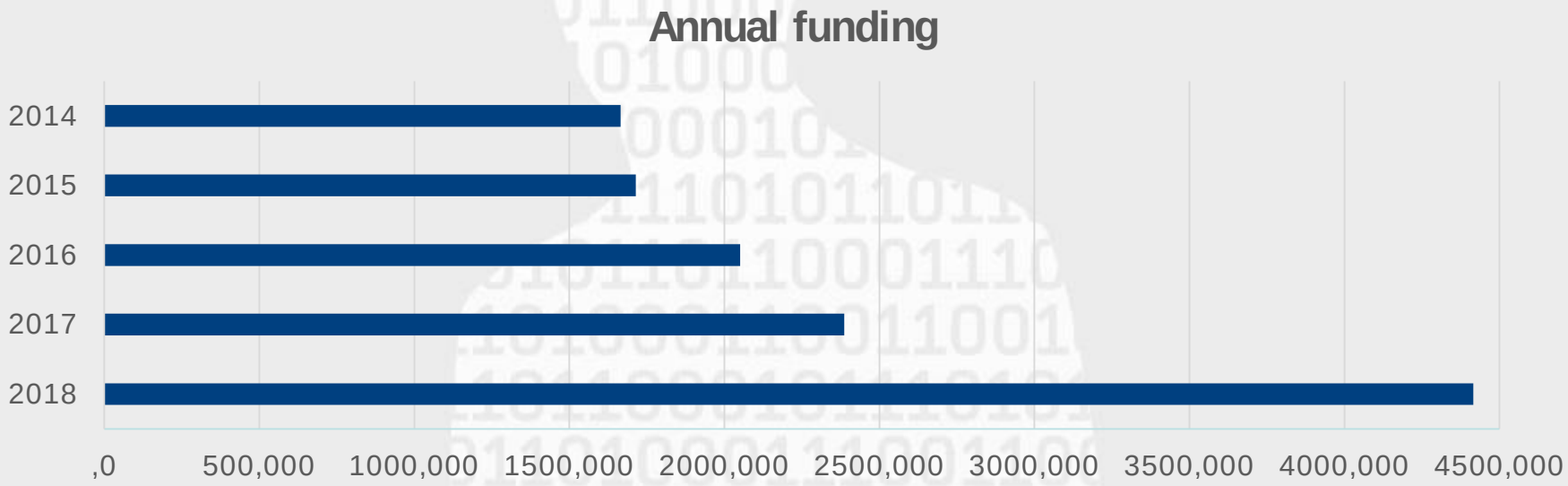


Collaboration

New organisational setup (2/2)



Evolution of the CNPD



Staff

2014	2017	2018
15	25	35

Territorial jurisdiction of the CNPD

- Jurisdiction on the territory of Luxembourg
- Introduction of the **"one stop shop"**
  - One single point of contact for companies established in several Member States
  - "**lead authority**" will be:
    - authority of the main establishment of the controller
    - place of the sole establishment of the controller
- Reinforced EU cooperation between the « lead authority » and « concerned » authorities
  - Aim is to adopt a single decision
  - In case of disagreement → binding decision by the "European Data Protection Board"

A paradigm shift

Removal of prior formalities (notifications / authorisations)

prior monitoring

Principle of Accountability

subsequent control

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

Tasks (1)

- 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

Tasks (2)

- Verify data breach notifications
- DPIA: prior consultation of the CNPD in case of remaining high residual risks
- Monitoring at the workplace (art. 261-1 CT):
  - Possible request of a prior opinion by the CNPD :
    - By the staff delegation or the concerned employees
    - Deadline: within 15 days of the prior information
  - CNPD has 1 month to answer
  - Request has a suspensive effect

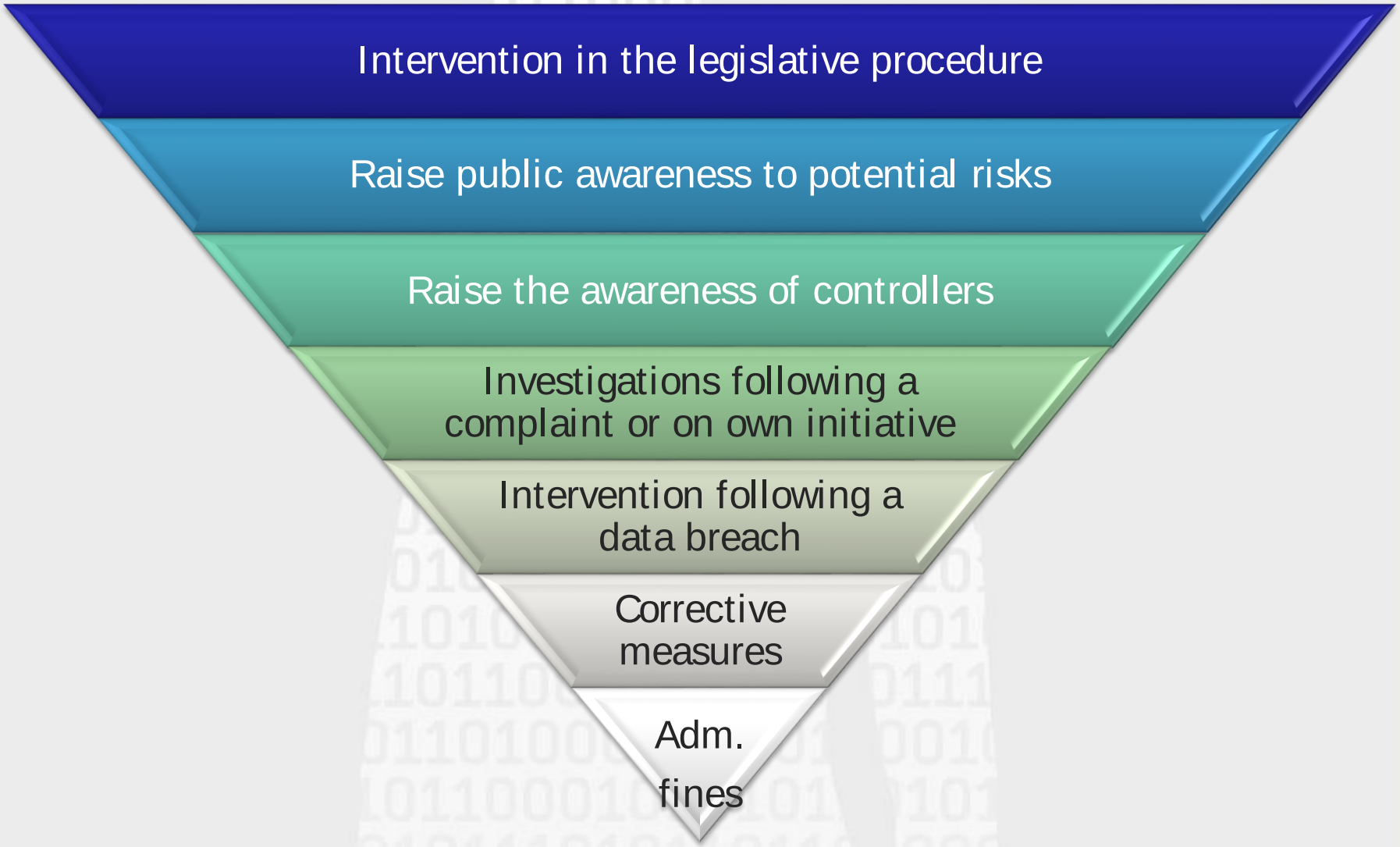
Tasks (3)

- Widening of competence to include processing activities in criminal / national security matters:
  - Old system: « Article 17 » Supervisory Authority (State Public Prosecutor + 2 members of the CNPD)
  - Law of 1 August 2018 implementing Directive 2016/680:
    - Processing operations by competent authorities for criminal purposes : competence of the CNPD
    - Exception for processing operations by courts + public prosecutor when acting in their judicial capacity : competence of a judicial control authority (≠ CNPD)

Investigative powers

- 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 […];

The right balance



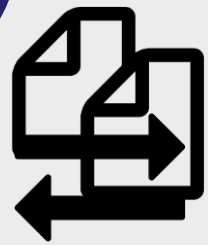
Different types of investigations

On-site inspection

- Inspection at the premises of the controller / processor
- Specific/limited scope
- One-off visit – where applicable triggers a file inspection

File inspection

- Questionnaire including a document request
- Review of answers and other relevant documents
- Switch to on-site inspection or data protection audit according to preliminary results



Data protection audit

- In depth review – broader in scope
- Multiple exchanges in form of meetings
- communication to exchange information and documents
- Risk based approach – refinement of scope during audit execution

Corrective powers

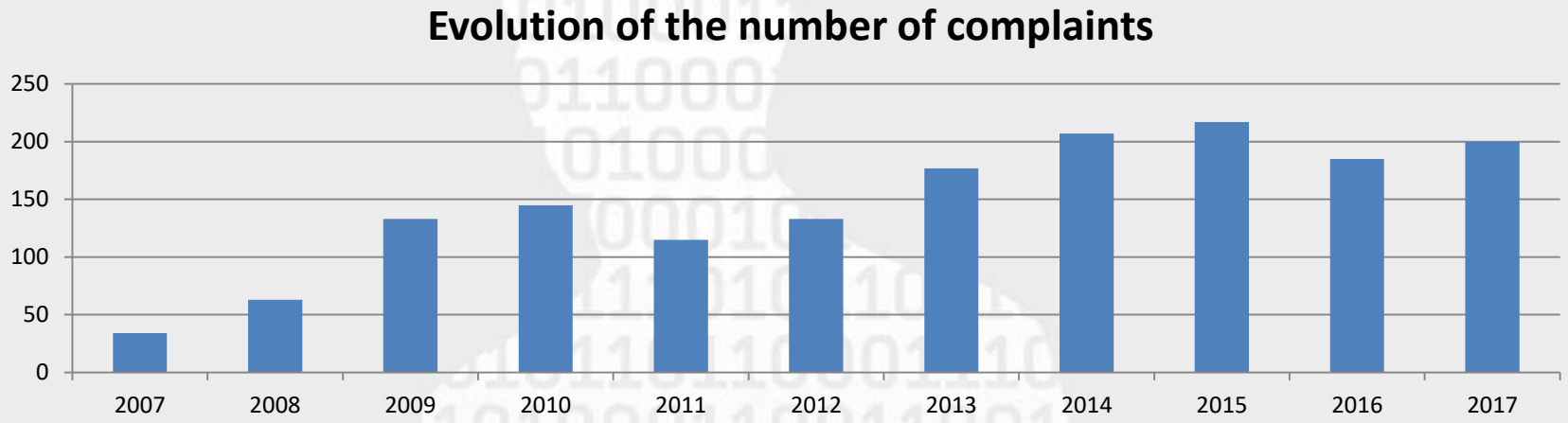
- Issue warnings and reprimands
- Order the controller/processor to bring processing operations into compliance with the GDPR
- Impose a temporary or definitive limitation, including a ban on processing
- Power to impose administrative fines:
  - Major innovation for the Grand Duchy
  - Imposed in addition, or instead of, other corrective measures

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.

Legal remedies

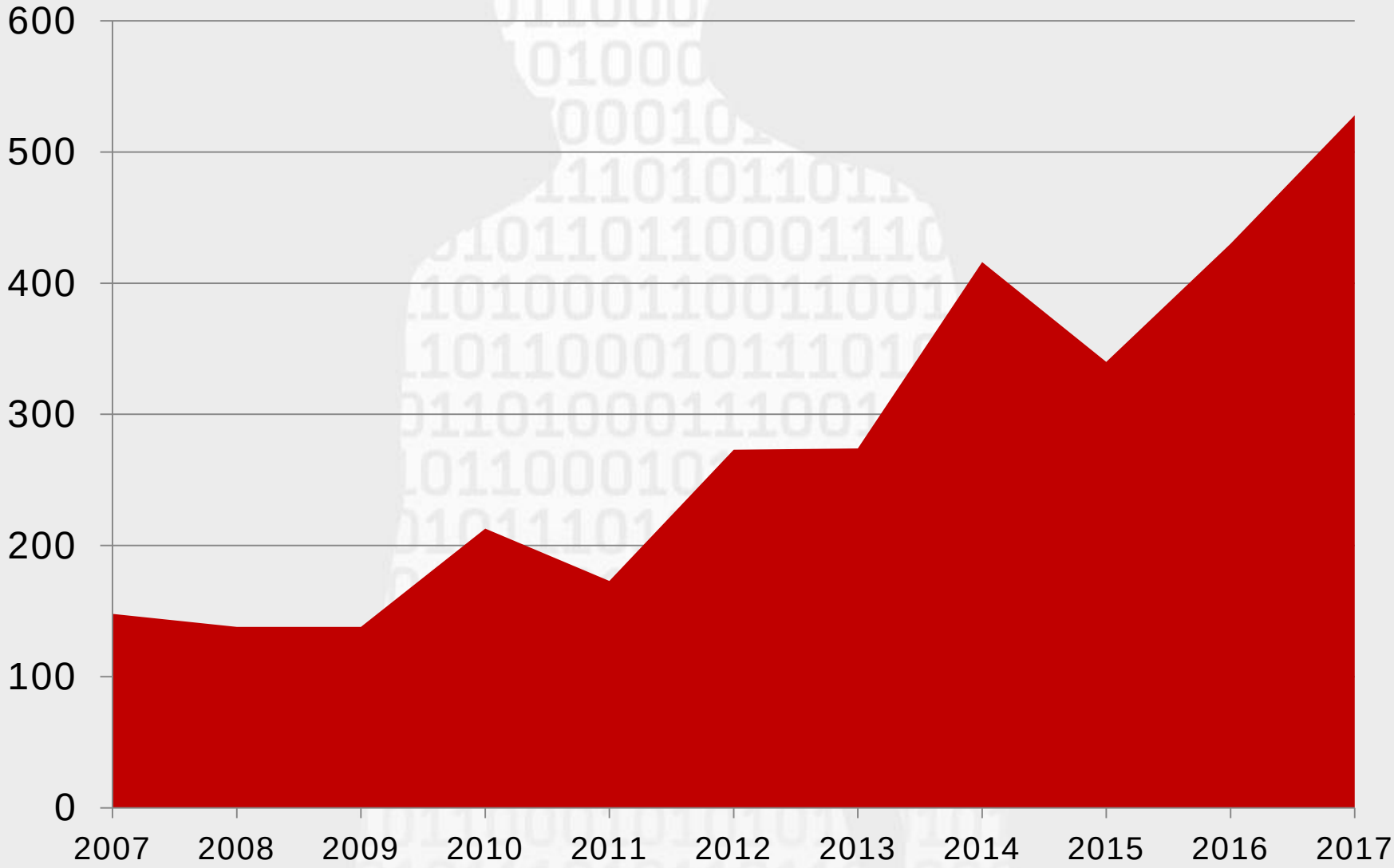
- Right for every data subject to lodge a complaint
  - with a supervisory authority of the MS of the data subject's habitual residence, place of work or place of the alleged infringement
- Right to an effective judicial remedy against a supervisory authority
  - against a legally binding decision concerning a data subject
  - against a failure to reply within 3 months
  - competence of the courts of the MS where the supervisory authority is established:
    - Competence of the Luxembourgish Administrative Tribunal "*Tribunal administratif*" deciding on the merits of the case

Increase of complaints (2017)

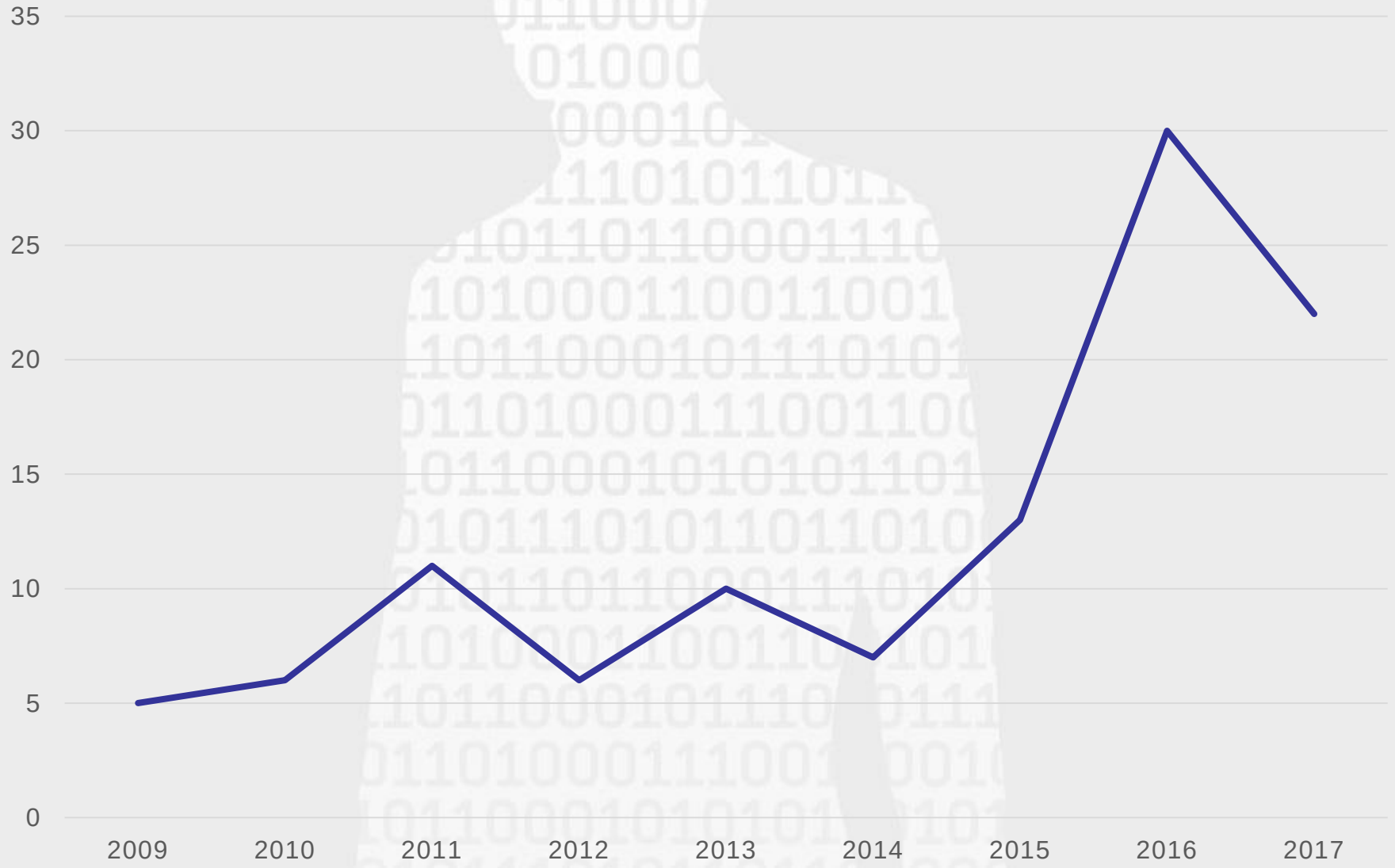


- Lawfulness of certain administrative/commercial practices (30%)
- Refusal of the data subject's right of access (13,5%)
- Illicit communication to third parties (18.5%)
- Supervision at the workplace / video-surveillance (12%)
- Requests of erasure or rectification of data (12%)
- Objection for marketing purposes (5%)
- Right to be forgotten (5%)
- Other (4%)

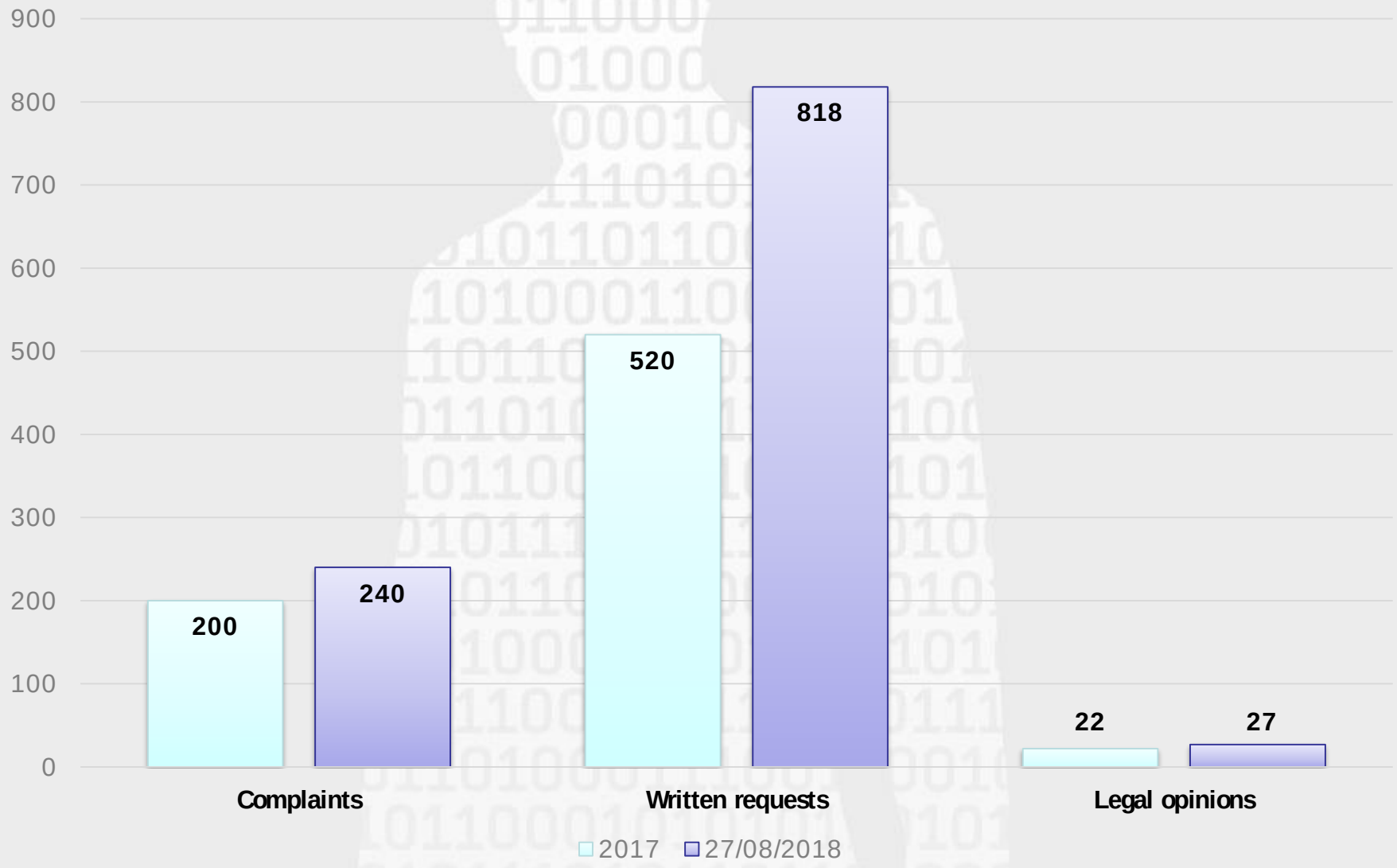
Increase of written information requests (2017)



Legal opinions (2017)



Statistics for 2018



Commission nationale pour la protection des données

Thank you for your attention!