CNPD Training: Data Protection Basics

The obligations of controllers and processors

Esch-sur-Alzette

7-8 February 2018

Mathilde Stenersen

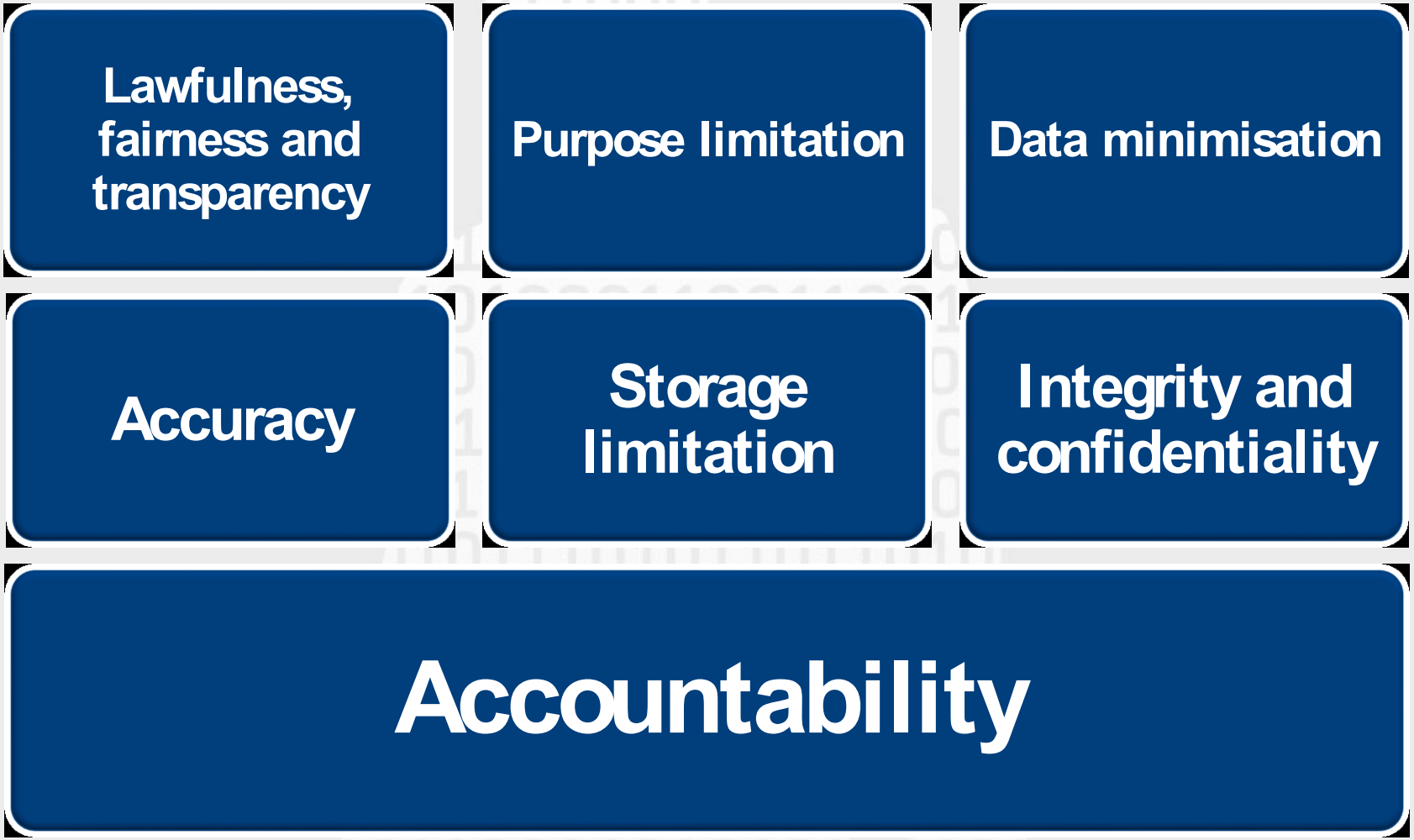
Legal service

Outline

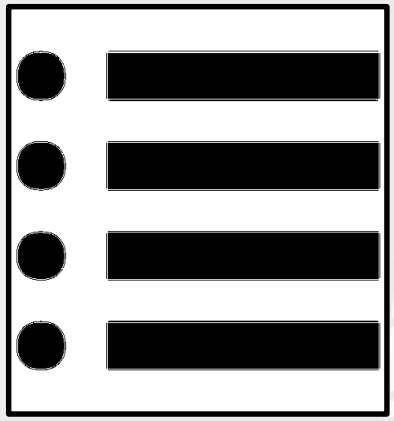
1. Introduction
2. Basic elements
3. The rights of the data subjects
4. **The obligations of controllers and processors**
5. The role of the CNPD


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(…)

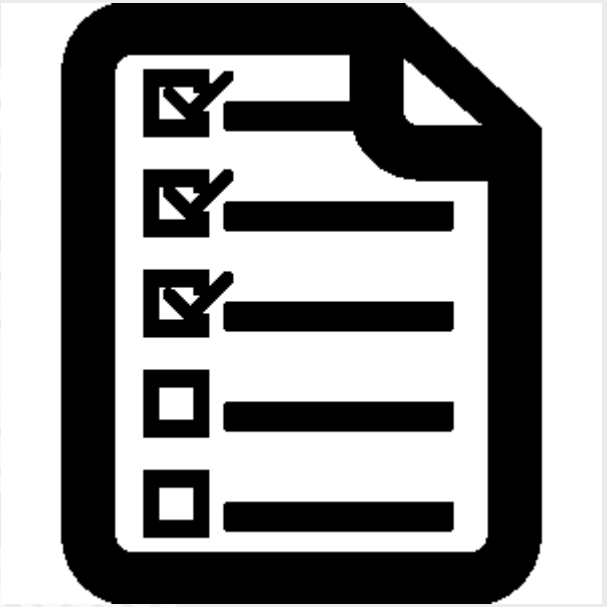
Exemples:

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

Re-use: 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 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

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

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

GDPR-CST

Registre des activités de traitement

Partie 2: Traitements — Title: Contract management — Creat. on: 18 July 2017 — Updat. on: 05 October 2017 — Creat. by: Paul Richard — Updat. by: Paul Richard — Draft

Partie 2: Traitements — Title: Analyse — Creat. on: 18 July 2017 — Updat. on: 05 October 2017 — Creat. by: Paul Richard — Updat. by: Paul Richard

Partie 2: Traitements — Title: Invoicing — Creat. on: 08 August 2017 — Updat. on: 05 October 2017 — Creat. by: Paul Richard — Updat. by: Paul Richard — Draft

Partie 2: Traitements — Title: Payroll — Creat. on: 05 October 2017 — Updat. on: 05 October 2017 — Creat. by: Paul Richard — Updat. by: Paul Richard — Draft

Partie 2: Traitements — Title: Maintenance — Creat. on: 06 October 2017 — Updat. on: 06 October 2017 — Creat. by: Paul Richard — Updat. by: Paul Richard — Draft

Partie 2: Traitements — Title: Infrastructure — Creat. on: 06 October 2017 — Updat. on: 06 October 2017 — Creat. by: Paul Richard — Updat. by: Paul Richard — Draft

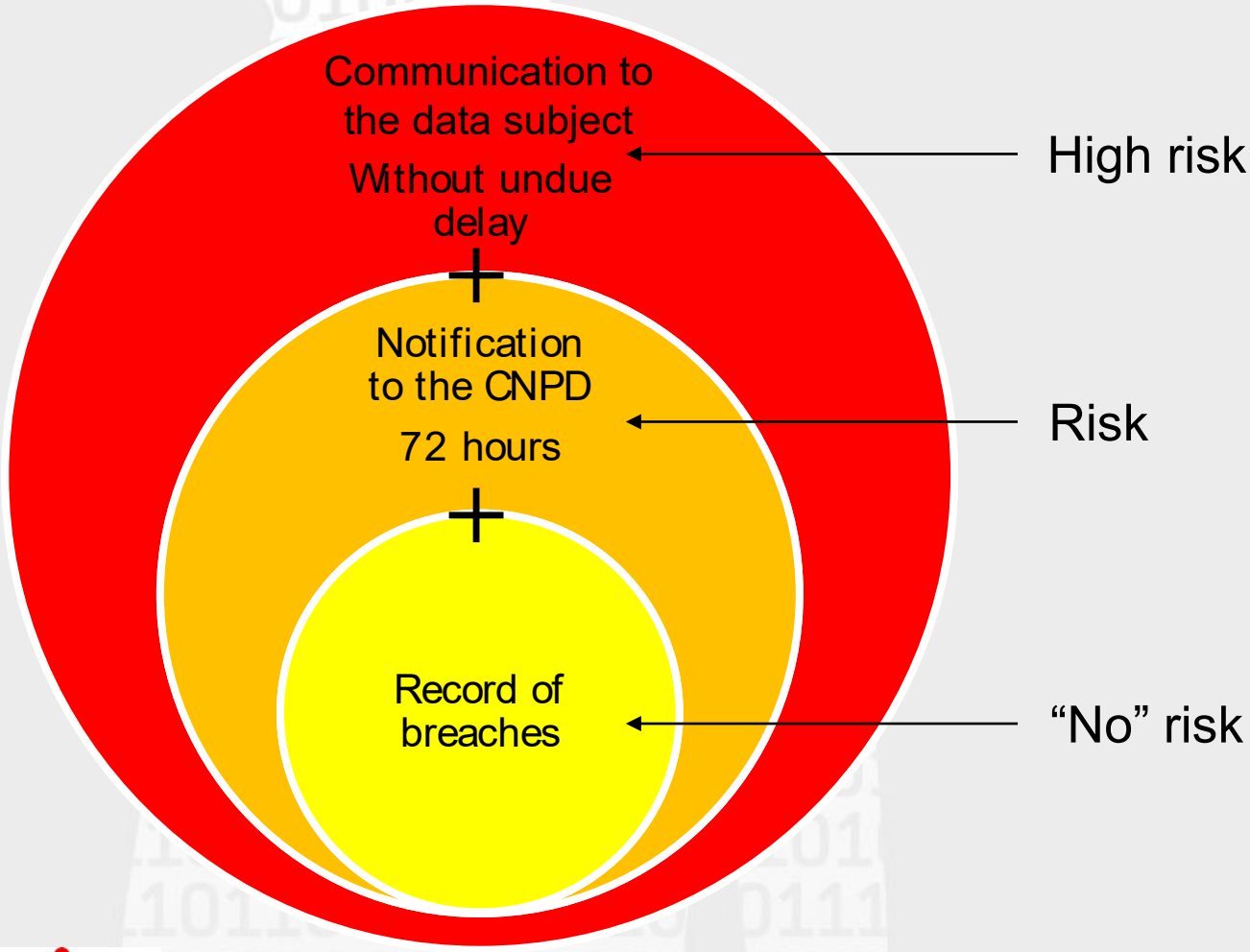
Example

@ 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)

Rôle: 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:

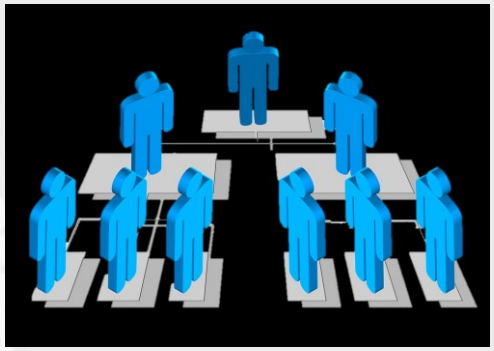
The processors only processes the personal data on documented instructions of the controller

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)

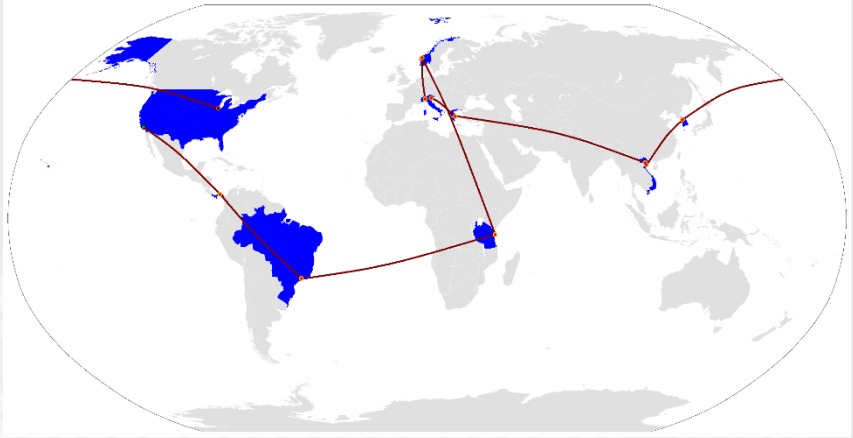
6. Processing

- 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

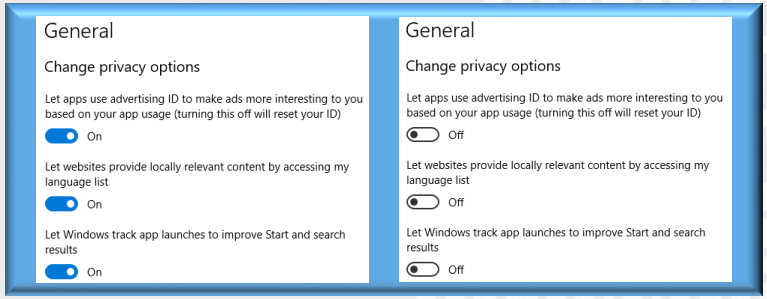
- Free flow of data within the EU/EEA
- Transfer of personal data to third countries (= outside the EU) only possible, if:
  - Adequacy decision
  - Adequate safeguards (e.g. BCRs or Standard Contractual Clauses, etc.)
  - Derogations for specific transfers (e.g. consent, contract, etc.)



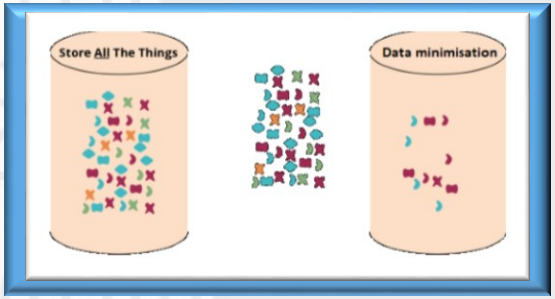
8. The rights of data subjects

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*)

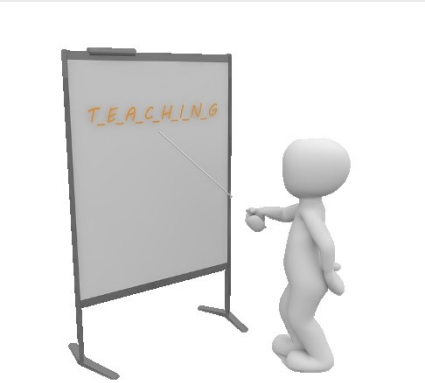


(*Privacy by default*)

- **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

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 data protection authority

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Esch-sur-Alzette

7-8 February 2018

Dani Jeitz

Legal service

Programme

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

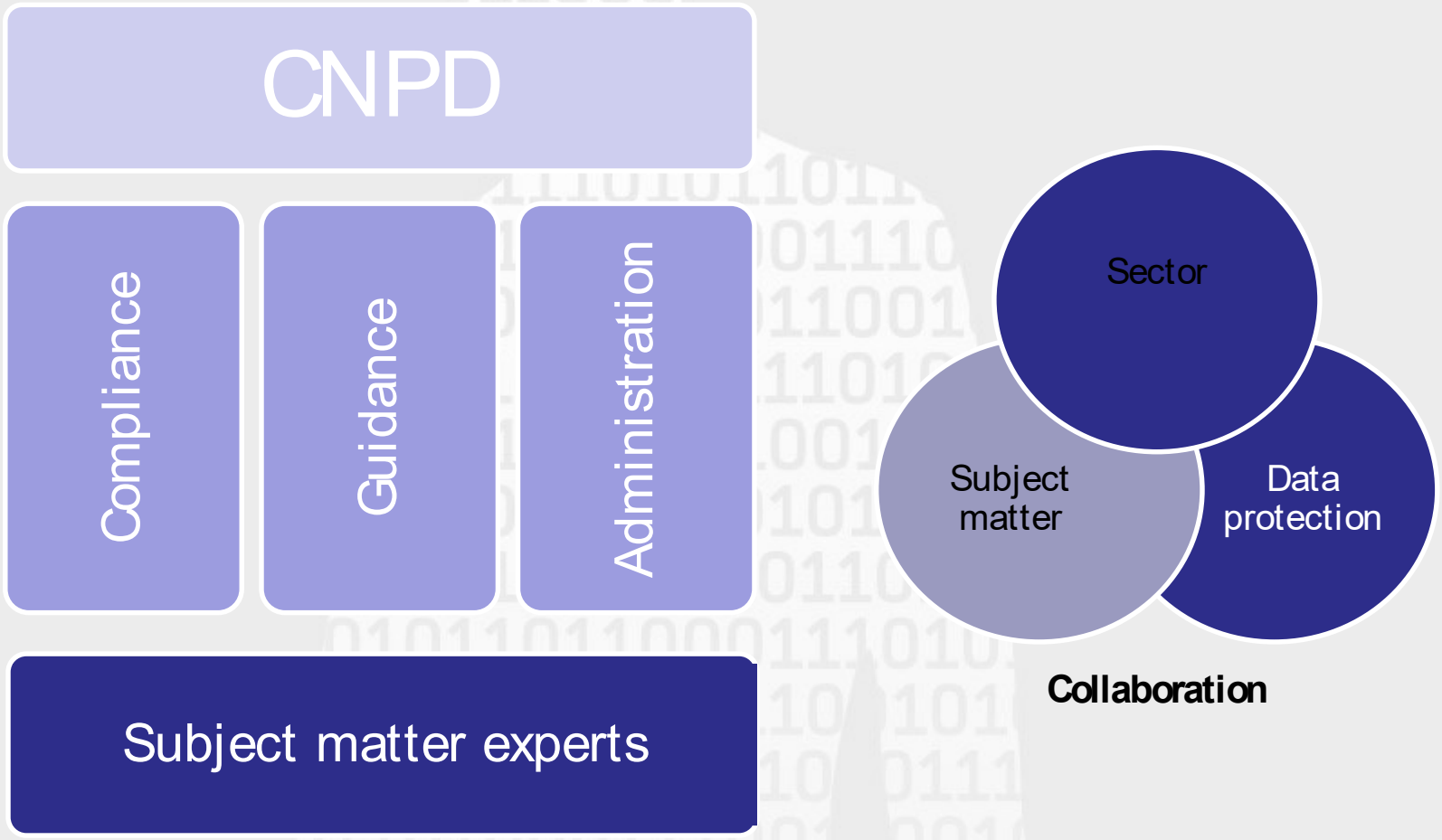
Outline

- Introduction
- Organisation and evolution of the CNPD
- Territorial jurisdiction
- Tasks
- Investigative and corrective powers
- Statistics

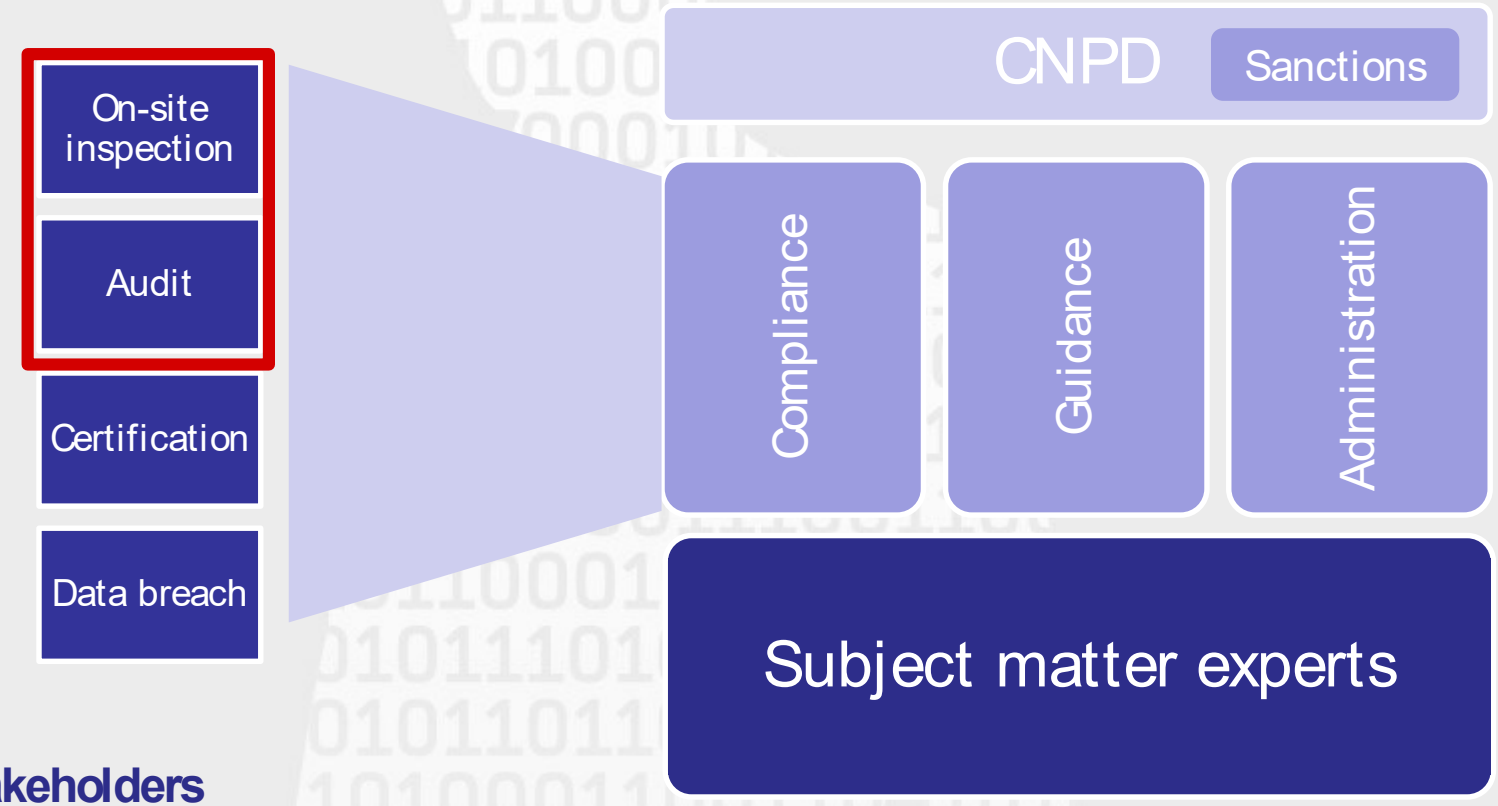
Introduction

- Independent authority created by law
  - Amended Act of 2 August 2002
  - Draft bill n°7184
- Public institution with financial and administrative autonomy
- Recent trends:
  - Sophisticated technologies: connected games, Smarthome, social media, smartphones, cloud, etc.
  - Personal data breaches (Uber, Ashley Madison, etc.)
  - Significant increase of complaints, requests for information and legislative opinions

New organizational setup (1/2)



New organizational setup (2/2)



Stakeholders

Commissioners

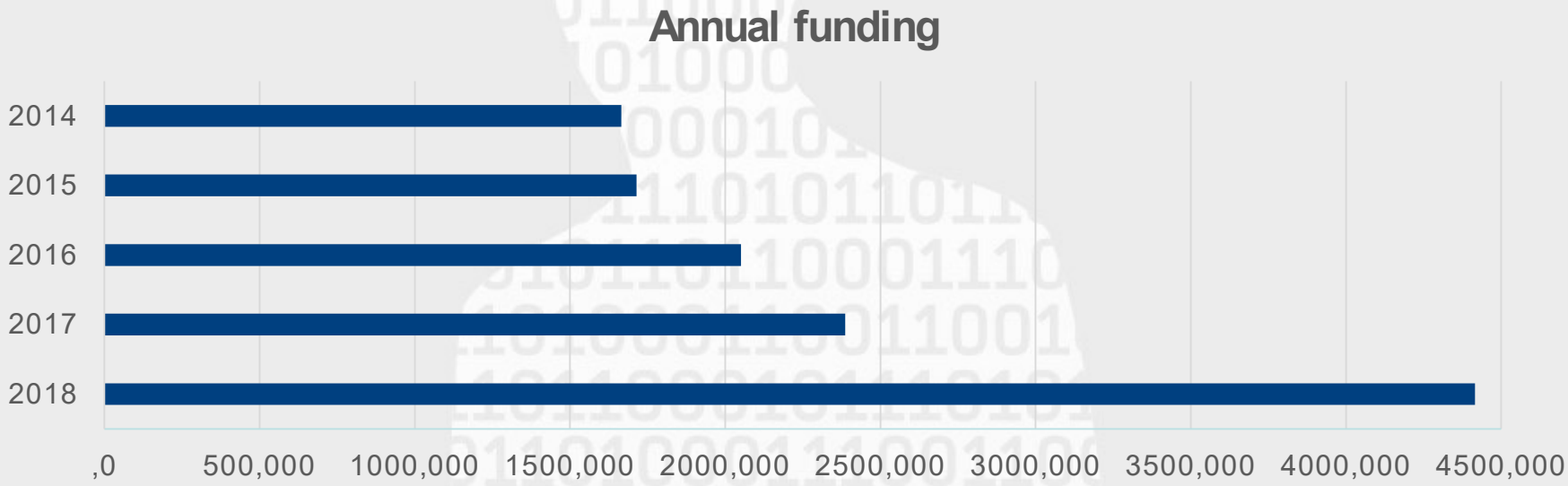
Head of investigation

Investigator

Expert

European cooperation

Evolution of the CNPD



Staff

2014	2017	2018
15	25	35

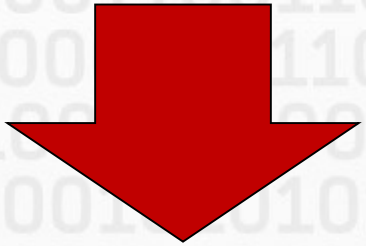
Territorial jurisdiction of the CNPD

- 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

- Monitor and enforce the application of the GDPR
- Advise the national parliament and government
- Raise public awareness and inform the general public
- Provide guidance to controllers / processors
- Handle complaints and conduct investigations
- Accredit the certification bodies
- Cooperate with other supervisory authorities
- Write and publish an annual activity report

Tasks

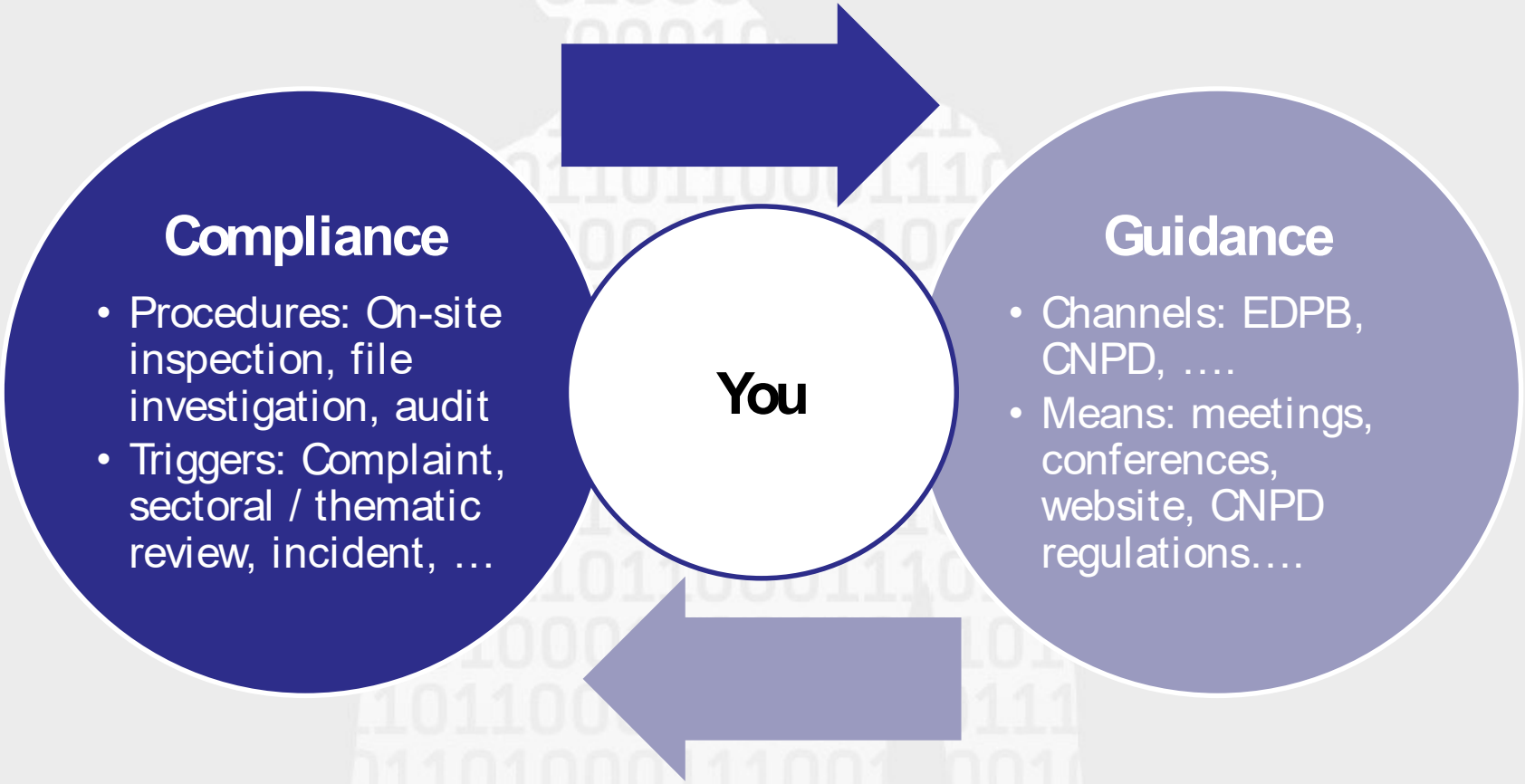
- Widening of competence to include processing activities in criminal / national security matters:
  - Currently: « Article 17 » Supervisory Authority (State Public Prosecutor + 2 members of the CNPD)
  - Draft bill n°7168 implementing Directive 2016/680:
    - Processing operations by competent authorities 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

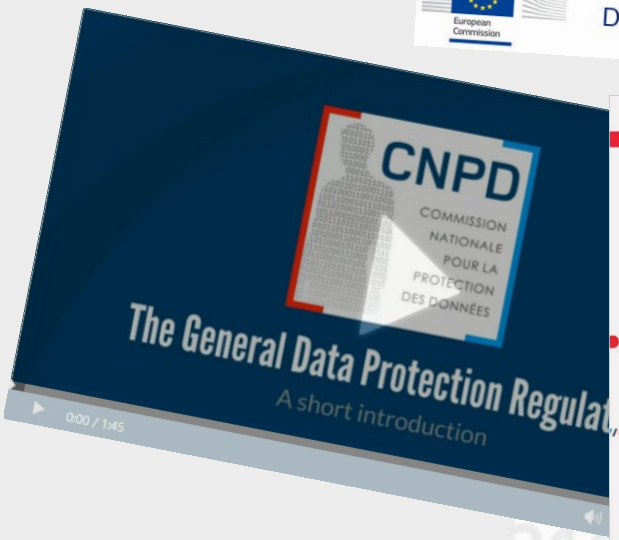
Article 58 Powers: Each supervisory authority shall have all have all of the following investigative powers:

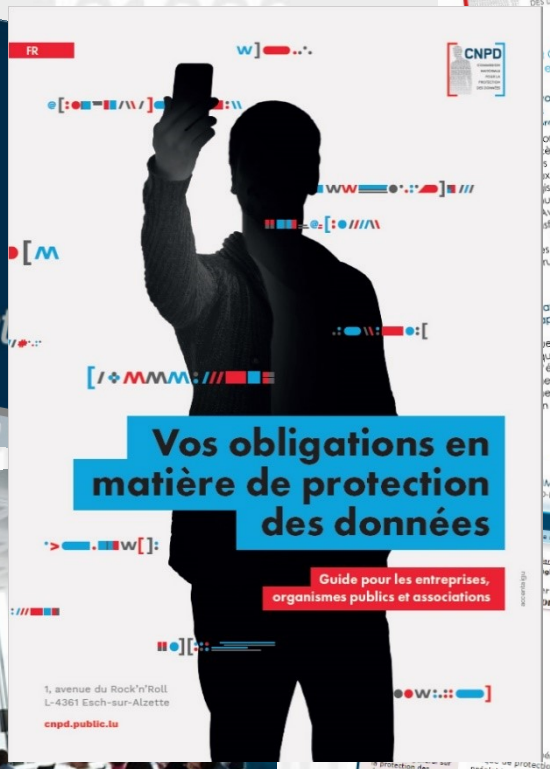
- to carry out **investigations** in the form of **data protection protection audits;**
- to obtain, from the controller and the processor, **access to all personal data** and to **all information necessary** for for the performance of its tasks;
- to obtain access **to any premises of the controller and and the processor,** including to any data processing equipment and means, in accordance with Union or Member State procedural law.
- …

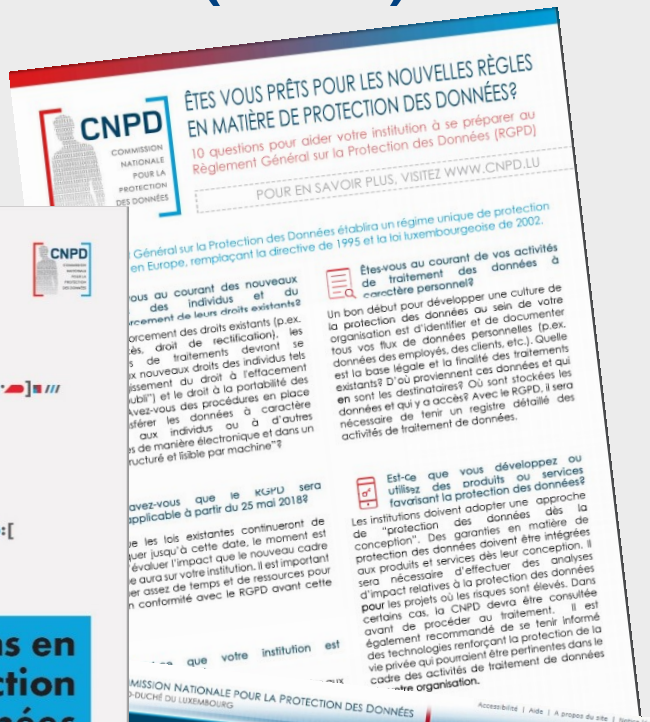
The right balance (1/3)

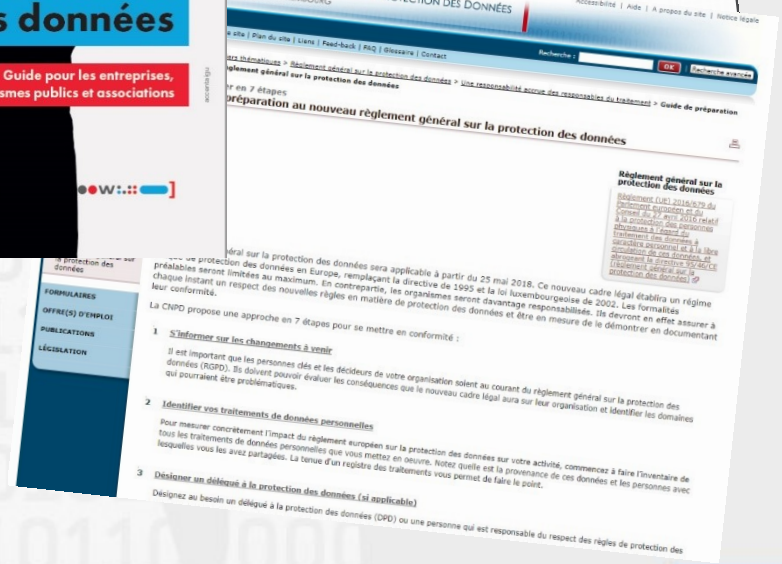


The right balance (2/3)

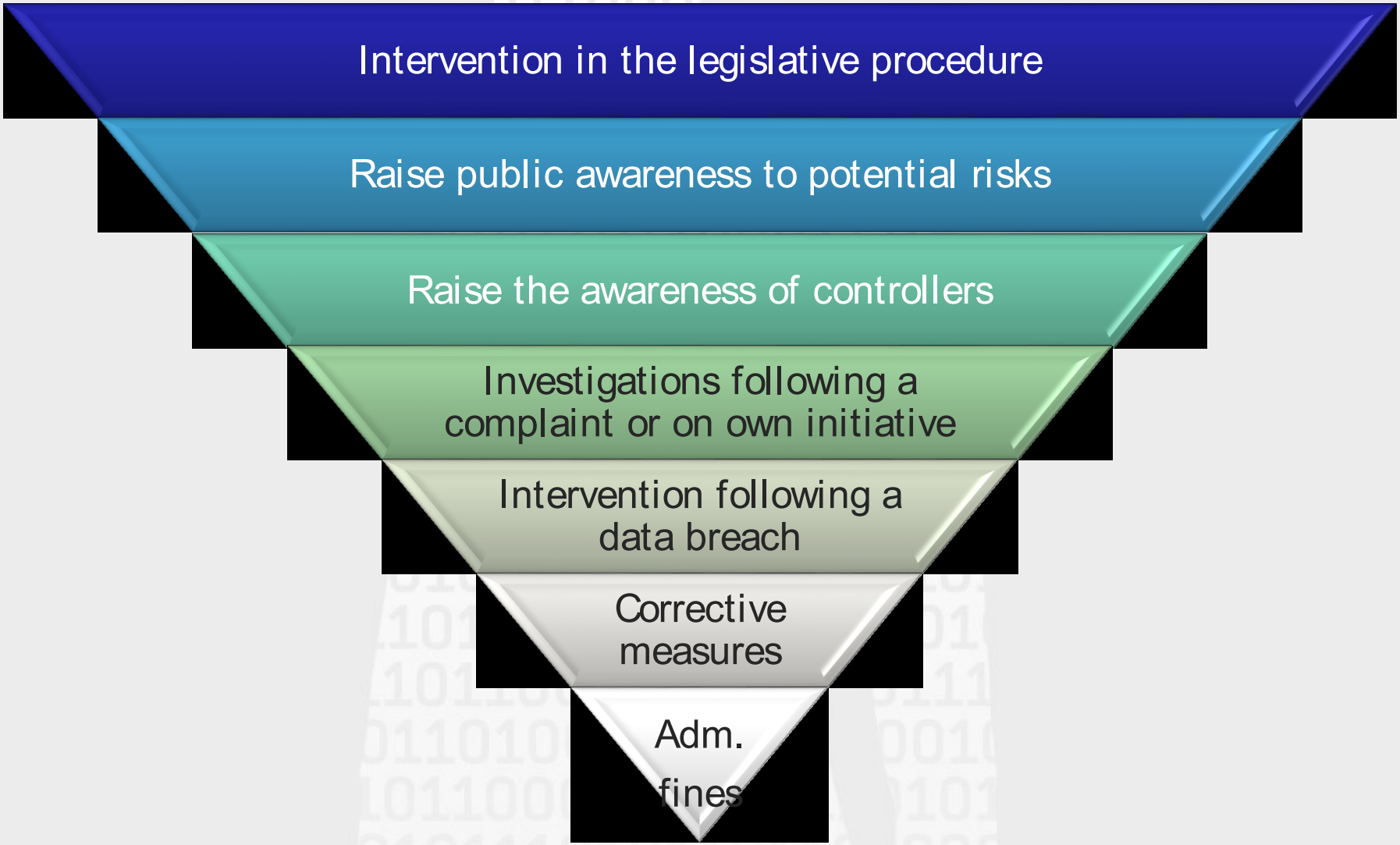








The right balance (3/3)



Different types of investigations

On-site inspection

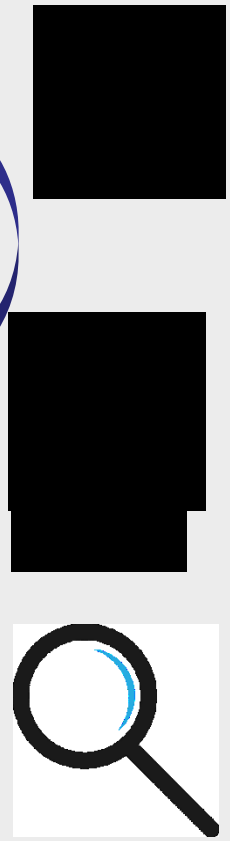
- Inspection at the premises of the controller / processor
- Specific/limited scope
- One-off visit – where applicable triggers a file inspection

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

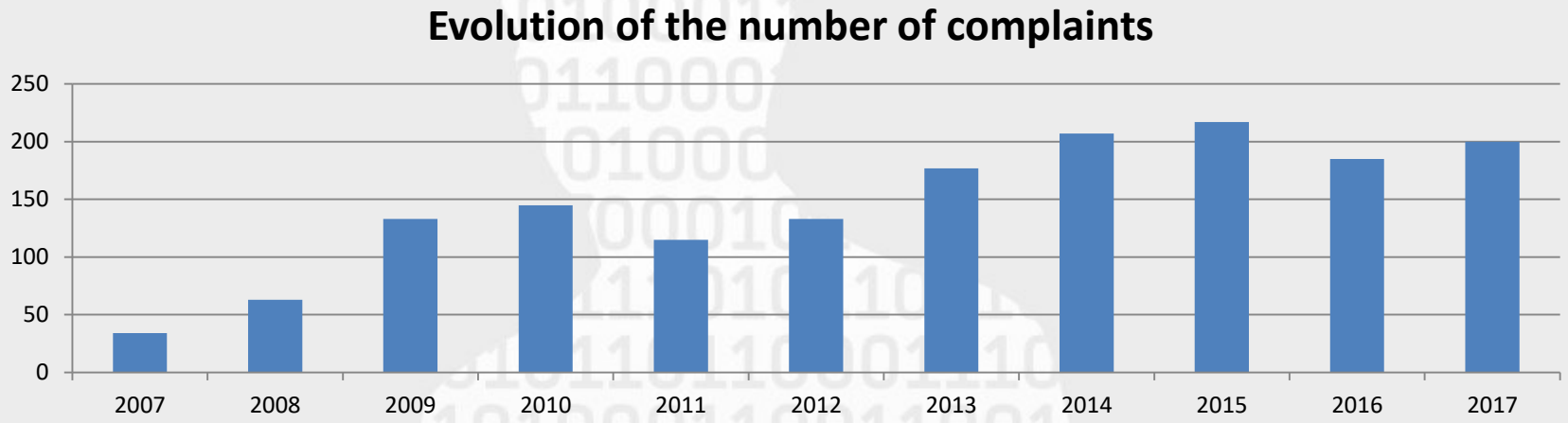
- Issue warnings and reprimands
- Order the controller/processor to bring processing operations into compliance with the GDPR
- Impose a temporary or definitive limitation, including a ban on processing
- Power to impose administrative fines:
  - Major innovation for the Grand Duchy
  - Imposed in addition,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

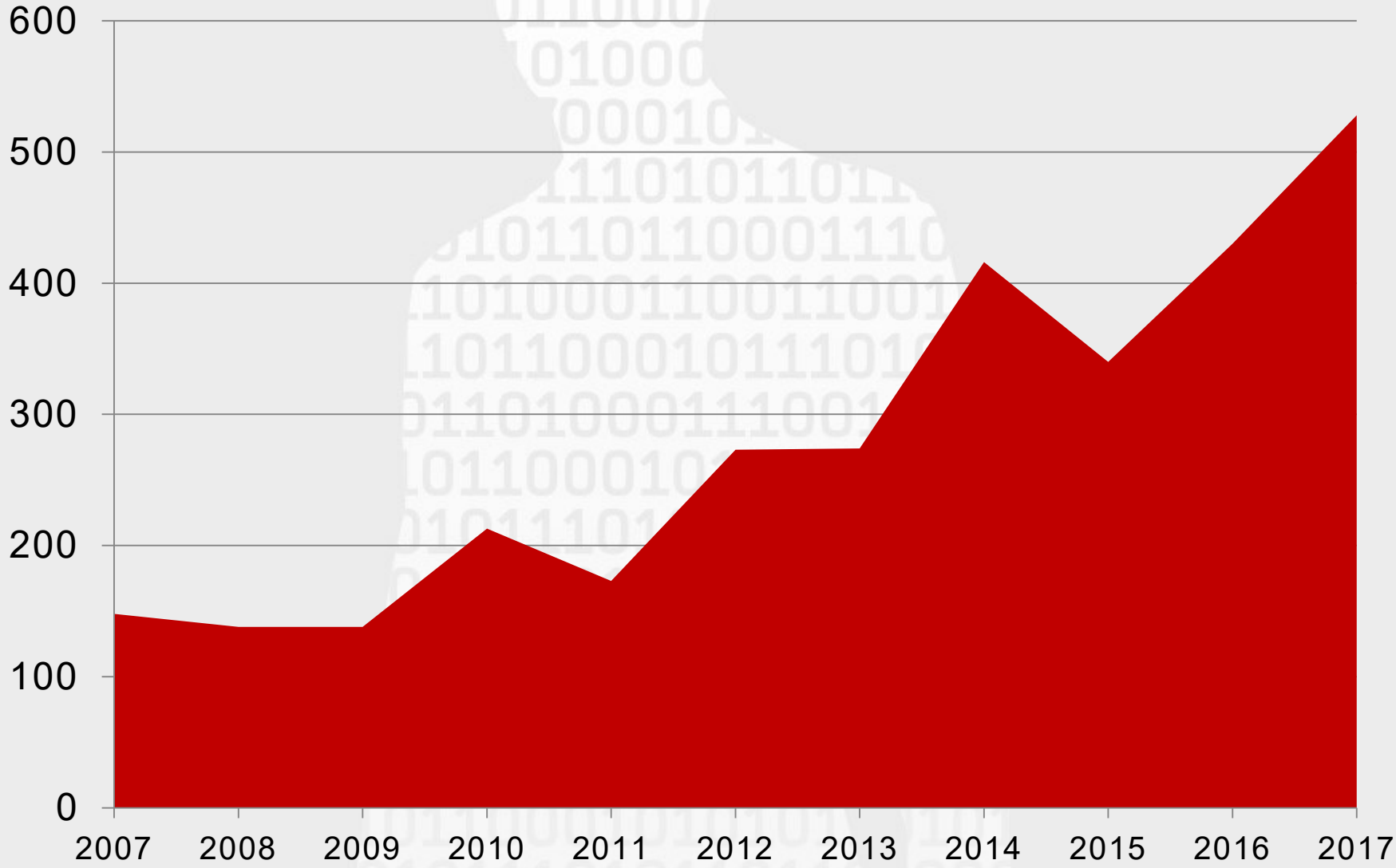
- Right for every data subject to lodge a complaint
  - with a supervisory authority of the MS of the data subject's habitual residence, place of work or place of the alleged infringement
- Right to an effective judicial remedy against a supervisory authority
  - against a legally binding decision concerning 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 "*Tribunal administratif*" deciding on the merits of the case

Increase of complaints (2017)

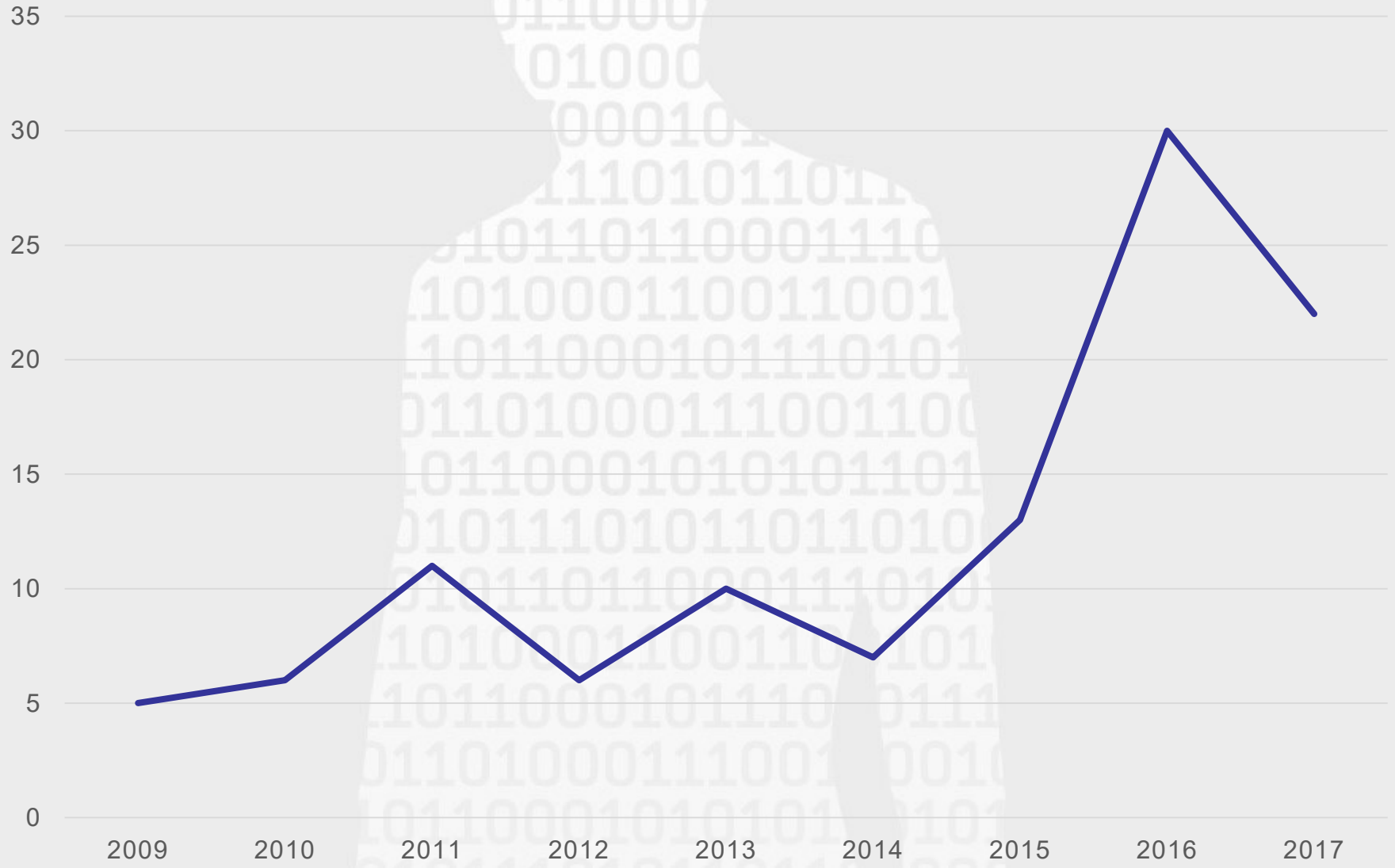


- Lawfulness of certain administrative/commercial practices (30%)
- Refusal of the data subject's right of access (13,5%)
- Illicit communication to third parties (18.5%)
- Supervision at the workplace / video-surveillance (12%)
- Requests of erasure or rectification of data (12%)
- Objection for marketing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

Increase of written information requests (2017)



Legal opinions (2017)



Thank you for your attention!

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