

CNPD Course: Data Protection Basics

*Presentation of Luxembourg's
data protection authority*



Esch-sur-Alzette

7-8 February 2018

Dani Jeitz

Service juridique

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)

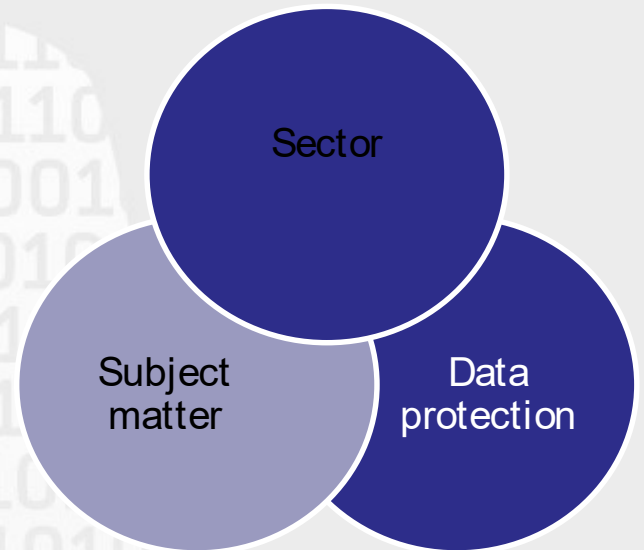
CNPD

Compliance

Guidance

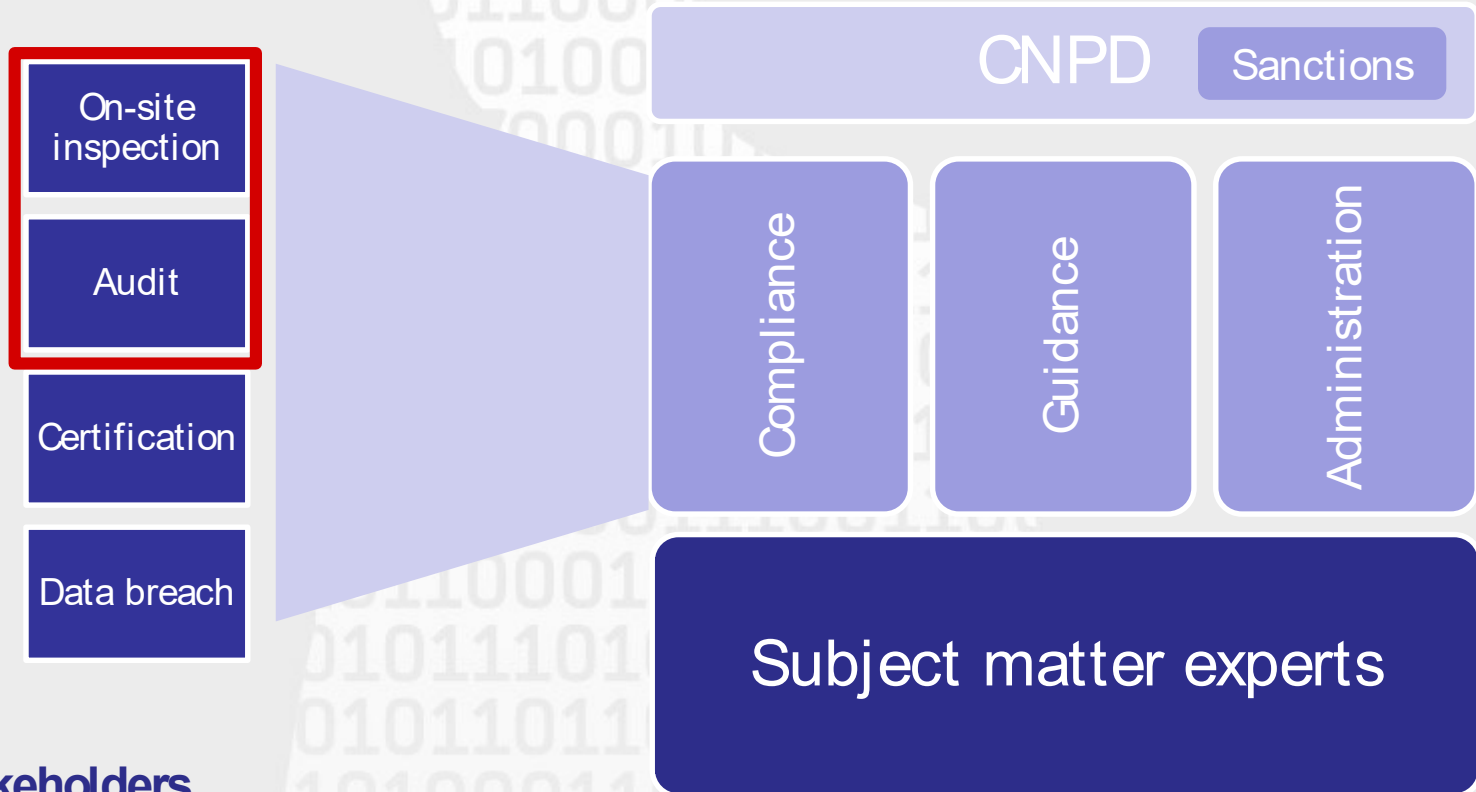
Administration

Subject matter experts



Collaboration

New organizational setup (2/2)



Stakeholders



Commissioners



Head of investigation



Investigator



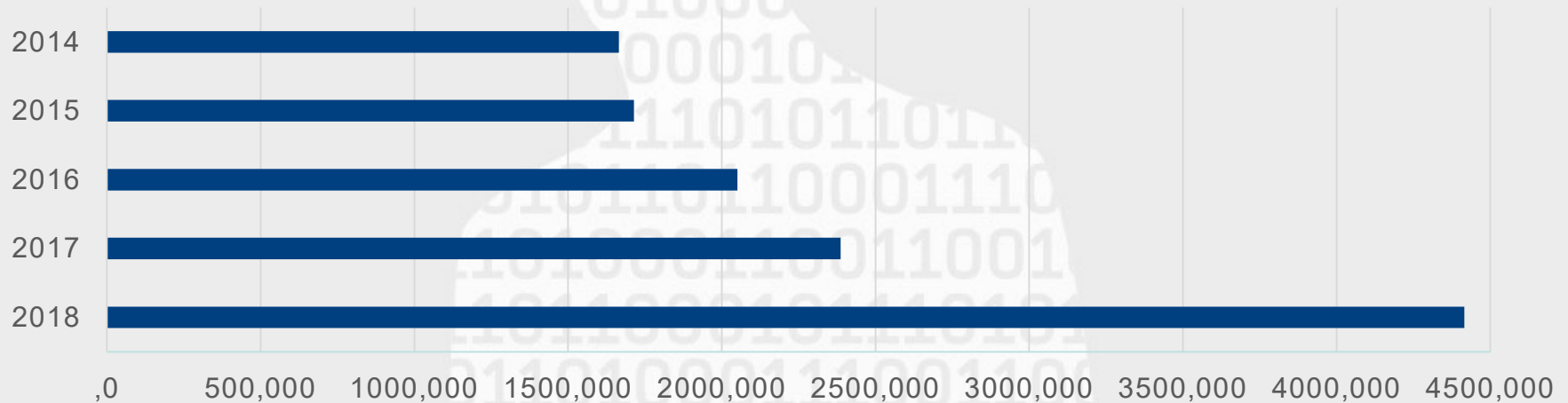
Expert



European cooperation

Evolution of the CNPD

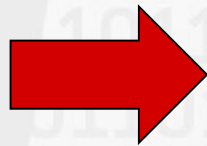
Annual funding



Staff

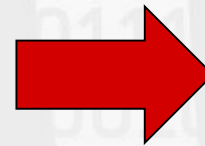
2014

15



2017

25



2018

35

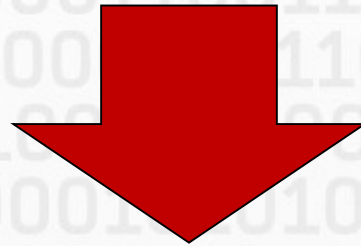
Territorial jurisdiction of the CNPD

- 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
- Accredite the certification bodies
- Cooperate with other supervisory authorities
- Write and publish an annual activity report

Tasks

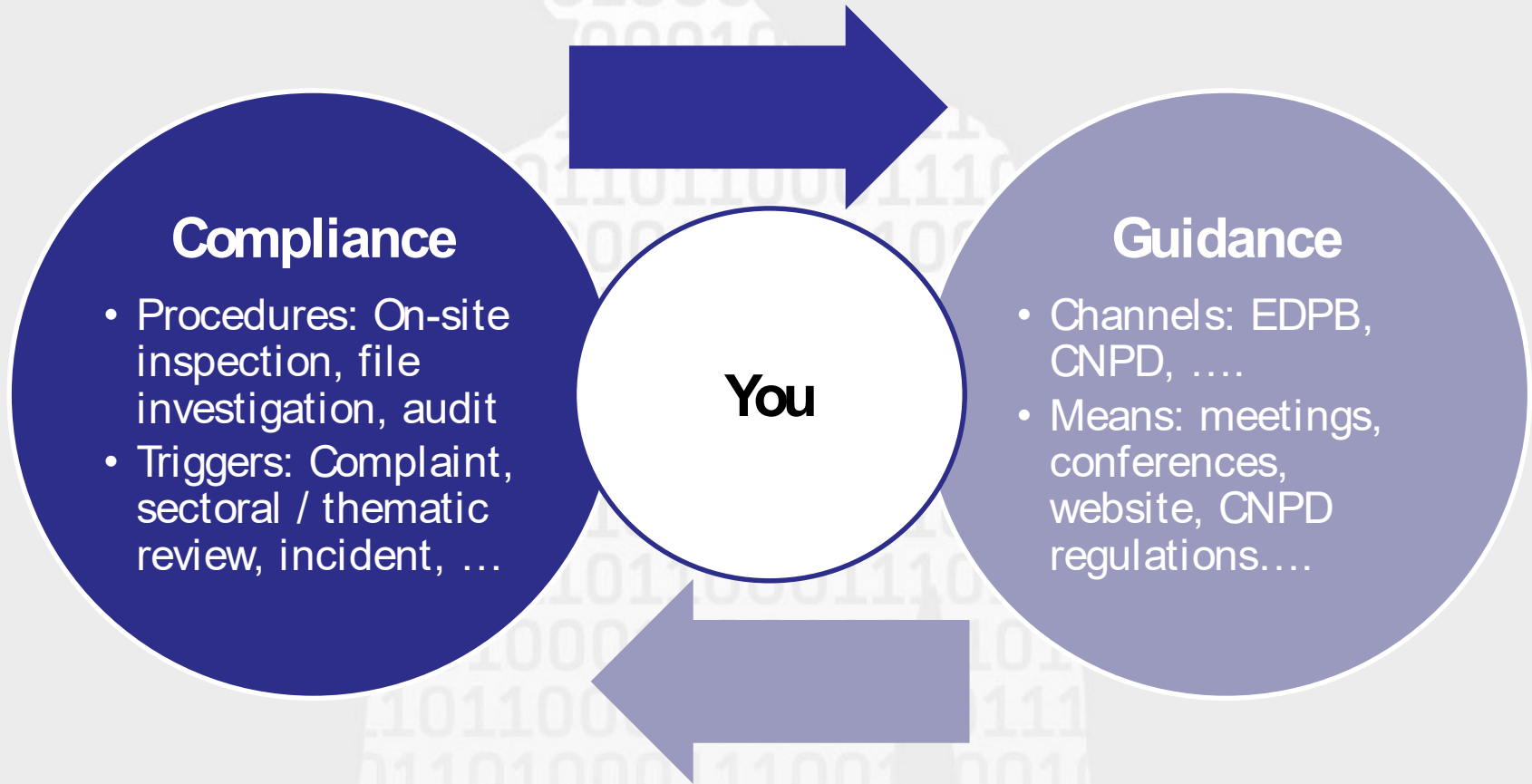
- Widening of competence to include processing activities in criminal / national security matters:
 - Currently: « Article 17 » Supervisory Authority (State Public Prosecutor + 2 members of the CNPD)
 - Draft bill n°7168 implementing Directive 2016/680:
 - Processing operations by competent authorities 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 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** and to **all information necessary** for the performance of its tasks;
- to obtain access **to any premises of the controller and the processor**, including to any data processing equipment and means, in accordance with Union or Member State procedural law.
- ...

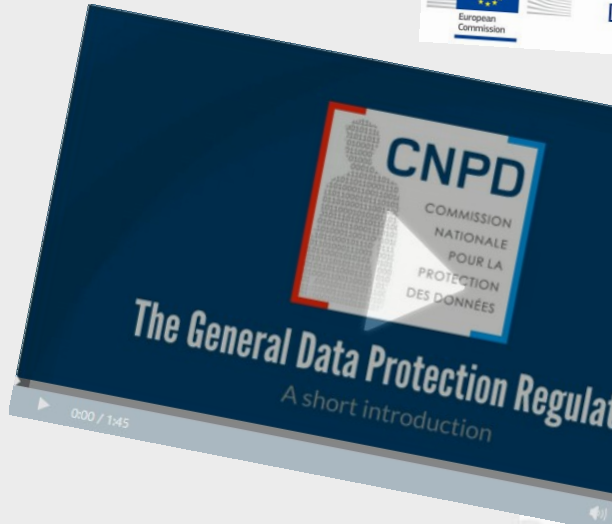
The right balance (1/3)



The right balance (2/3)



ARTICLE 29
Data Protection Working Party



ÉTES VOUS PRÊTS POUR LES NOUVELLES RÈGLES EN MATIÈRE DE PROTECTION DES DONNÉES?

10 questions pour aider votre institution à se préparer au Règlement Général sur la Protection des Données (RGPD)

POUR EN SAVOIR PLUS, VISITEZ WWW.CNPD.LU

Général sur la Protection des Données établit un régime unique de protection en Europe, remplaçant la directive de 1995 et la loi luxembourgeoise de 2002.

Vous ou courant de nouveaux des individus et du traitement de leurs droits existants? (p.ex. droit de rectification), les traitements devront se conformer aux nouveaux droits des individus tels que le droit à la portabilité des données et le droit à l'effacement des données. Avez-vous des procédures en place pour garantir les données à d'autres personnes de manière électronique et dans un format lisible par machine?

Êtes-vous au courant de vos activités de traitement des données à caractère personnel?

Un bon début pour développer une culture de la protection des données ou sein de votre organisation est d'identifier et de documenter tous vos flux de données personnelles (p.ex. données des employés, des clients, etc.). Quelle est la base légale et la finalité des traitements des données et qui y ont accès? Où sont stockées les données et qui y a accès? Avec le RGPD, il sera nécessaire de tenir un registre détaillé des activités de traitement de données.

Est-ce que vous développez ou utilisez des produits ou services favorisant la protection des données?

Les institutions doivent adopter une approche de "protection des données dès la conception". Des garanties en matière de protection des données doivent être intégrées aux produits et services dès leur conception. Il sera nécessaire d'évaluer les impacts des données et d'effectuer des analyses de risque relatives à la protection des données pour les projets où les risques sont élevés. Dans certains cas, la CNPD devra être consultée avant de procéder au traitement. Il est également recommandé de se tenir informé des technologies pertinentes dans le cadre des activités de traitement de données de votre organisation.

1. S'informer sur les changements à venir

Il est important que les personnes clés et les décideurs de votre organisation soient au courant du règlement général sur la protection des données (RGPD). Ils doivent pouvoir évaluer les conséquences que le nouveau cadre légal aura sur leur organisation et être en mesure de le démontrer en documentant ce qui pourrait être problématiques.

2. Identifier vos traitements de données personnelles

Pour mesurer concrètement l'impact du règlement européen sur la protection des données sur votre activité, commencez à faire l'inventaire de tous les traitements de données personnelles que vous mettez en œuvre. Notez quelle est la provenance de ces données et les personnes avec lesquelles vous les avez partagées. La tenue d'un registre des traitements vous permet de faire le point.

3. Désigner un délégué à la protection des données (si applicable)

Désignez au besoin un délégué à la protection des données (DPO) ou une personne qui est responsable du respect des règles de protection des données.

Vos obligations en matière de protection des données

Guide pour les entreprises, organismes publics et associations

1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette
cnpd.public.lu



The right balance (3/3)

Intervention in the legislative procedure

Raise public awareness to potential risks

Raise the awareness of controllers

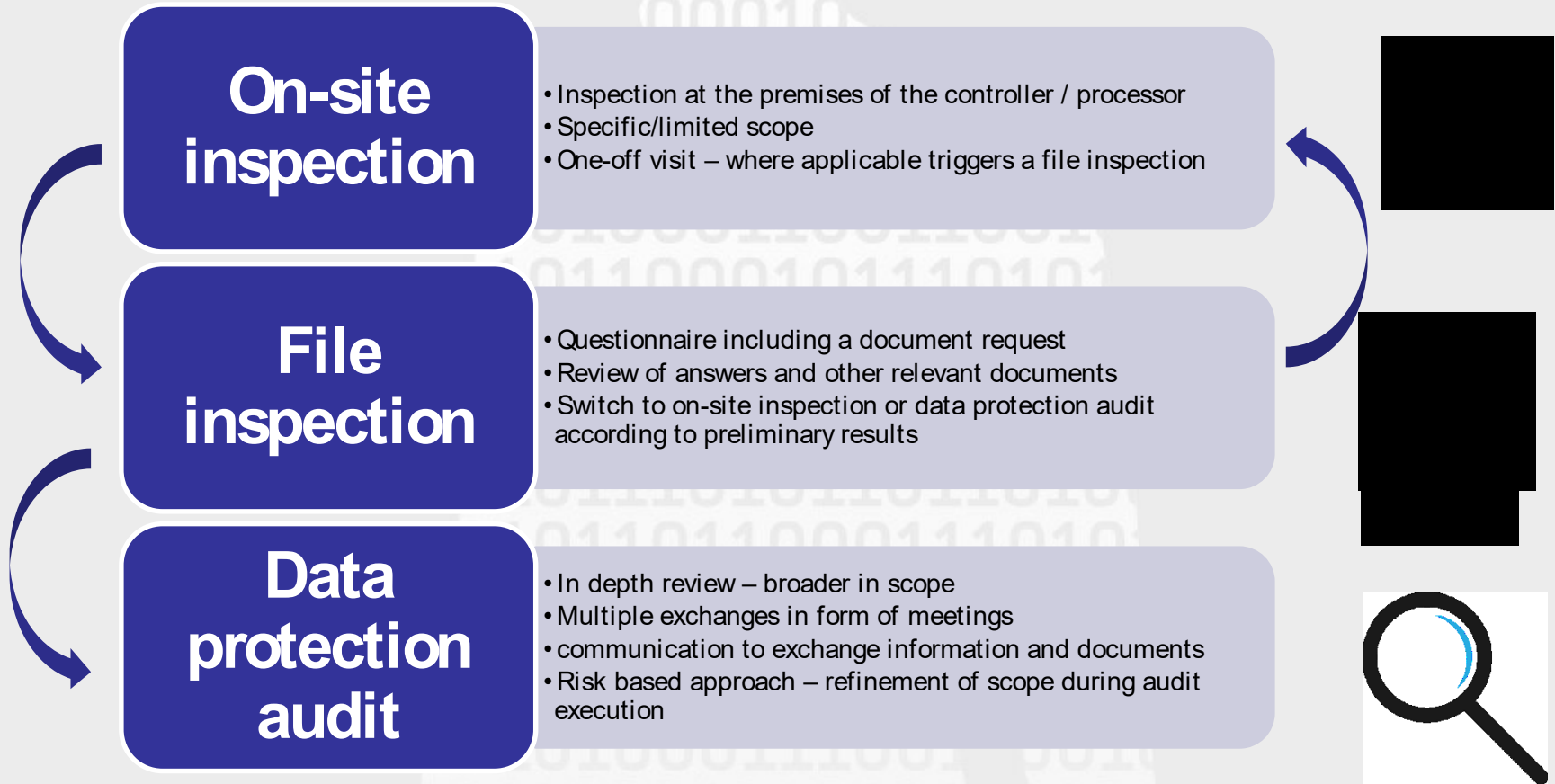
Investigations following a complaint or on own initiative

Intervention following a data breach

Corrective measures

Adm.
fines

Different types of investigations



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

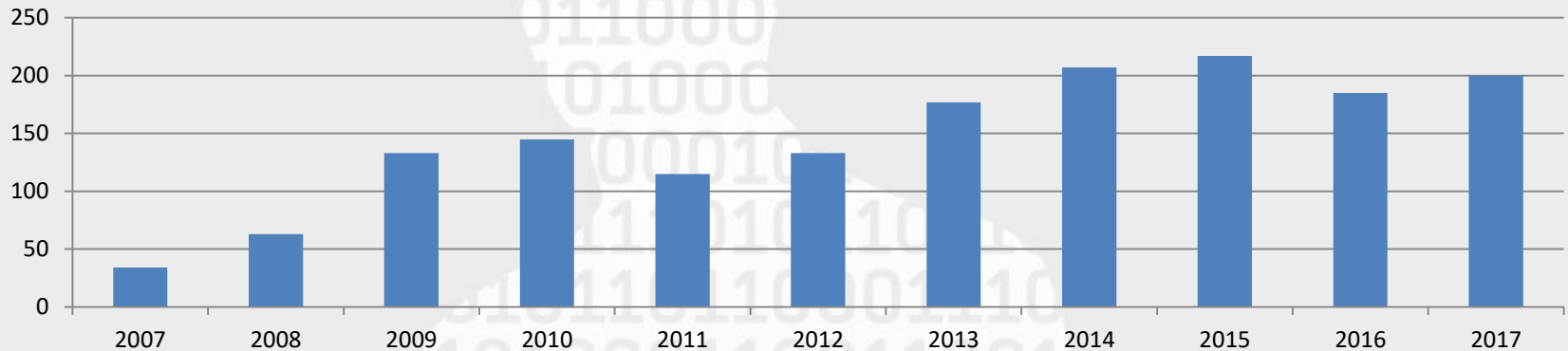
Infringements can be subject to a max. administrative fine of up to 20 million EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year.

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

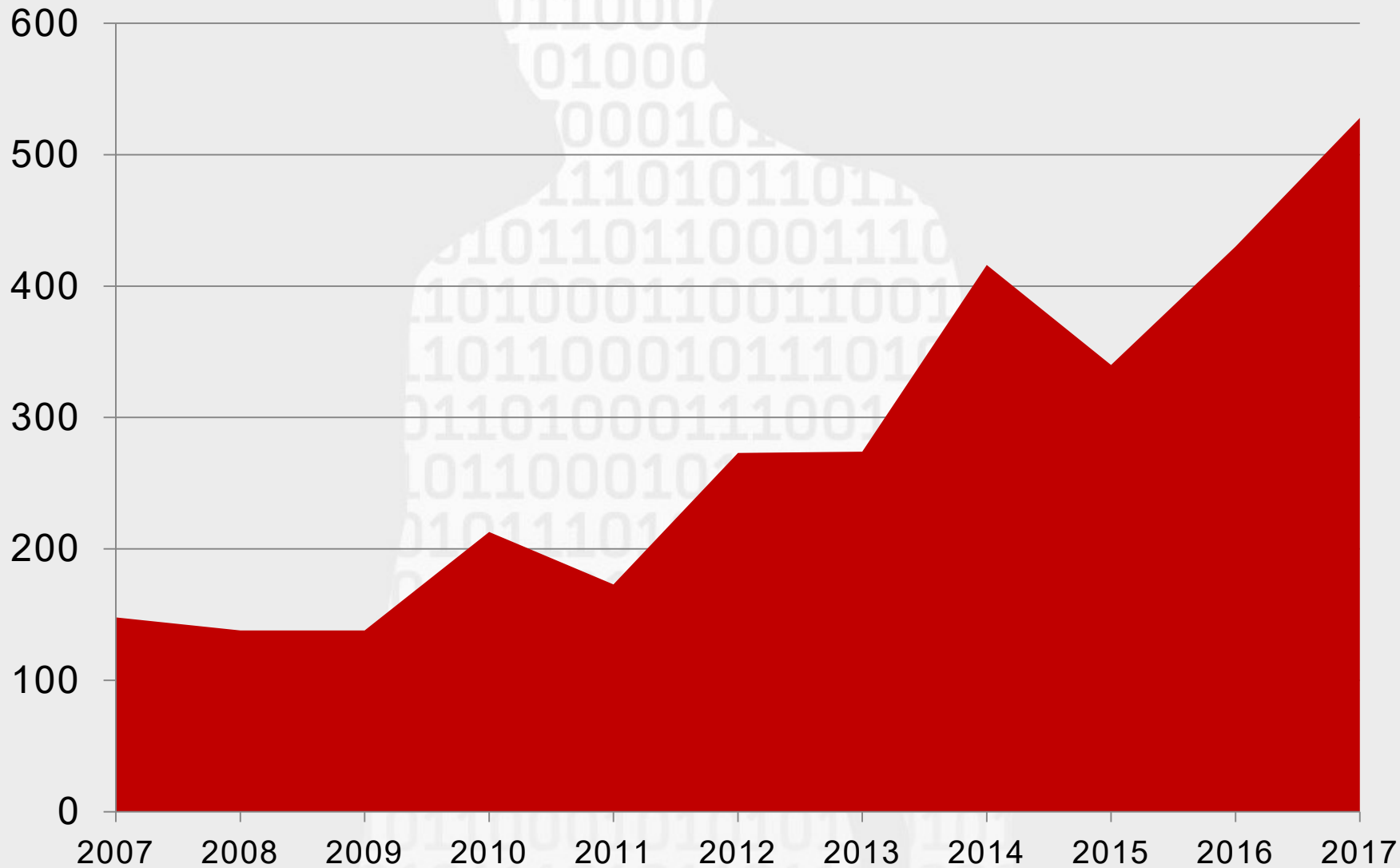
Increase of complaints (2017)

Evolution of the number of complaints

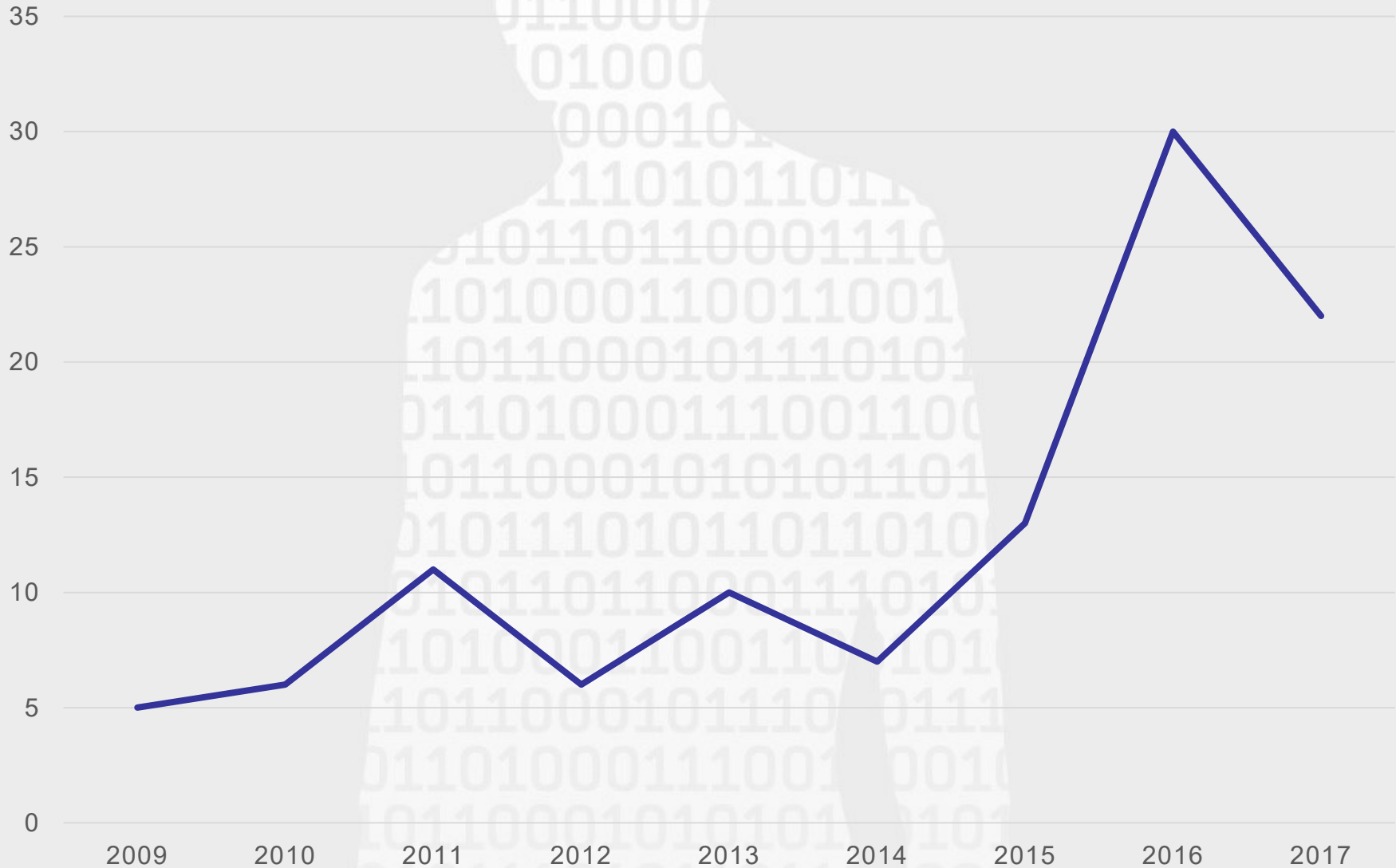


- Lawfulness of certain administrative/commercial practices (30%)
- Refusal of the data subject's right of access (13,5%)
- Illicit communication to third parties (18.5%)
- Supervision at the workplace / video-surveillance (12%)
- Requests of erasure or rectification of data (12%)
- Objection for marketing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

Increase of written information requests (2017)



Legal opinions (2017)



Initiation to data protection – 06-07/01/2018

0101110
01011011



10110001010101
010111010110110
010110110001110

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