Specialised information session: The new European general data protection regulation.

The future role of the CNPD and the impact on various stakeholders.

Guillaume Byk

Juriste – Chargé de Mission

CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

14-17 November 2016, Chambre de Commerce & 18 November 2016, Technoport (Belval)

1. A brief history

- The current law is based on a directive from 1995.
- The current legal framework is no longer suited to current technological evolutions (big data, smart phone, cloud computing…).
- The new regulation **updates and strengthens** the rights of data subjects and the obligations of data controllers and processors.
- The regulation being applicable everywhere in Europe, it will harmonise the legislation at the European level and will contribute to the advent of a European digital market.
- The regulation will be applicable from the **25th of May 2018.** Before this date, the current law is still applicable.

Main stakeholders affected by the GDPR

Data subjects (DS)

(Individuals whose personal data are being processed)

The GDPR gives DS an enhanced set of rights which they can enforce against data controllers and/or processors.

Data controllers (DC) & processors (DP)

(Private companies and public authorities which process personal data of individuals)

DC and DP are subject to a series of new obligations to the data subjects and/or supervisory authorities.

Supervisory Authority (SAs)

SAs help DS in protecting their rights and DC and DP in fulfilling their obligations as set out in the regulation. The GDPR strengthens their supervisory powers.

2a. Supervision after the GDPR

Overview

- Data controller and/or processor

  Accountability = implementation of compliance & the ability to demonstrate it at any time (Art. 5.2)

  - Reduced reporting tasks to the SA after the suppression of prior formalities,
  - Increased internal compliance measures for the DC/DP,
  - Freedom in the implementation of compliance, but also increased responsibilities for the DC and/or DP.

- Supervisory Authority
  - **A posteriori control** instead of prior examination.
  - Prior formalities (notification and autorisation request) are replaced by controls and investigations.
  - The goal is to ensure that DC/DP abide by their new obligations and assume their responsabilites, with a particular focus on ex-post controls of non-compliant DC/DP.

2b. Supervision after the GDPR
Enhanced missions (Art. 57)

- Some current missions are maintained
  - Awareness and guidance of all the players i.e. the DC/DP and the public,
  - Advice and counsel to the government, companies and citizens,
  - Monitor the evolution of new information technologies.
- Some missions are specified or strengthened
  - Compulsory cooperation with the other European SAs,
  - Investigation of complaints and claims lodged with the CNPD,
  - Encourage the development of codes of conduct, the adoption of contractual clauses and the approval of binding corporate rules.
- New missions
  - Prior consultation in some cases,
  - Encourage the implementation of certification and labelling mechanisms,
  - Manage an internal register of infringements of this regulation as well as the according remedial measures,
  - Participate in the activities of the European Data Protection Board.

2c. Supervision after the GDPR
Strengthening of powers (Art.58)

- Some current powers are specified or strengthened
  - Investigation and enquiry powers with regard to the DC/DP,
  - Power to impose sanctions / to adopt correctives measures (financial sanctions),
  - Authorisation power and advisory power.

- New powers
  - Enforce the DC/DP to comply with new DS's rights,
  - Withdrawal of certifications,
  - Request the DC to communicate a personal data breach to DS,
  - Impose an administrative fine (max. 10/20 millions Euros or 2/4% of the total worldwide annual turnover of the preceding financial year) according to the nature, scope, duration of the infringement etc. . The fine must be effective, proportionate and dissuasive.

- Additional powers can be granted to the CNPD by the national law

3a. The one-stop-shop and the consistency mechanism
Overview

- In cross-border cases, the DC/DP has a unique contact point named the lead SA linked to the DC/DP's main establishment (Art. 4.16) or its only establishment (Art. 56.1).
- The lead SA and the concerned SAs collaborate with each other through the one-stop-shop mechanism in order to reach a consensus (Art. 60).
- With the involvement of the European Data Protection Board (having legal personality) through the consistency mechanism (Art. 63).
- Appeal against the decisions of the EDPB is possible within 2 months directly to the CJEU in application of art. 263 TFEU.

3b. The one-stop-shop mechanism
Overview

- New regulation system in relation to cross-border processings:
  - Processing of personal data which takes place in the context of the activities of establishments of the DC/DP based in more than one Member State,

  or
  - Processing of personal data which takes place in the context of the activities of a single establishment of the DC/DP but which substantially affects or is likely to substantially affect DS in more than one Member State.

- Advantages:
  - For DS: better defence of their rights since they can directly complain to their country's SA (proximity, unique point of contact).
  - For DC/DP: simplicity/reduced administrative burden (unique point of contact) and enhanced legal certainty.

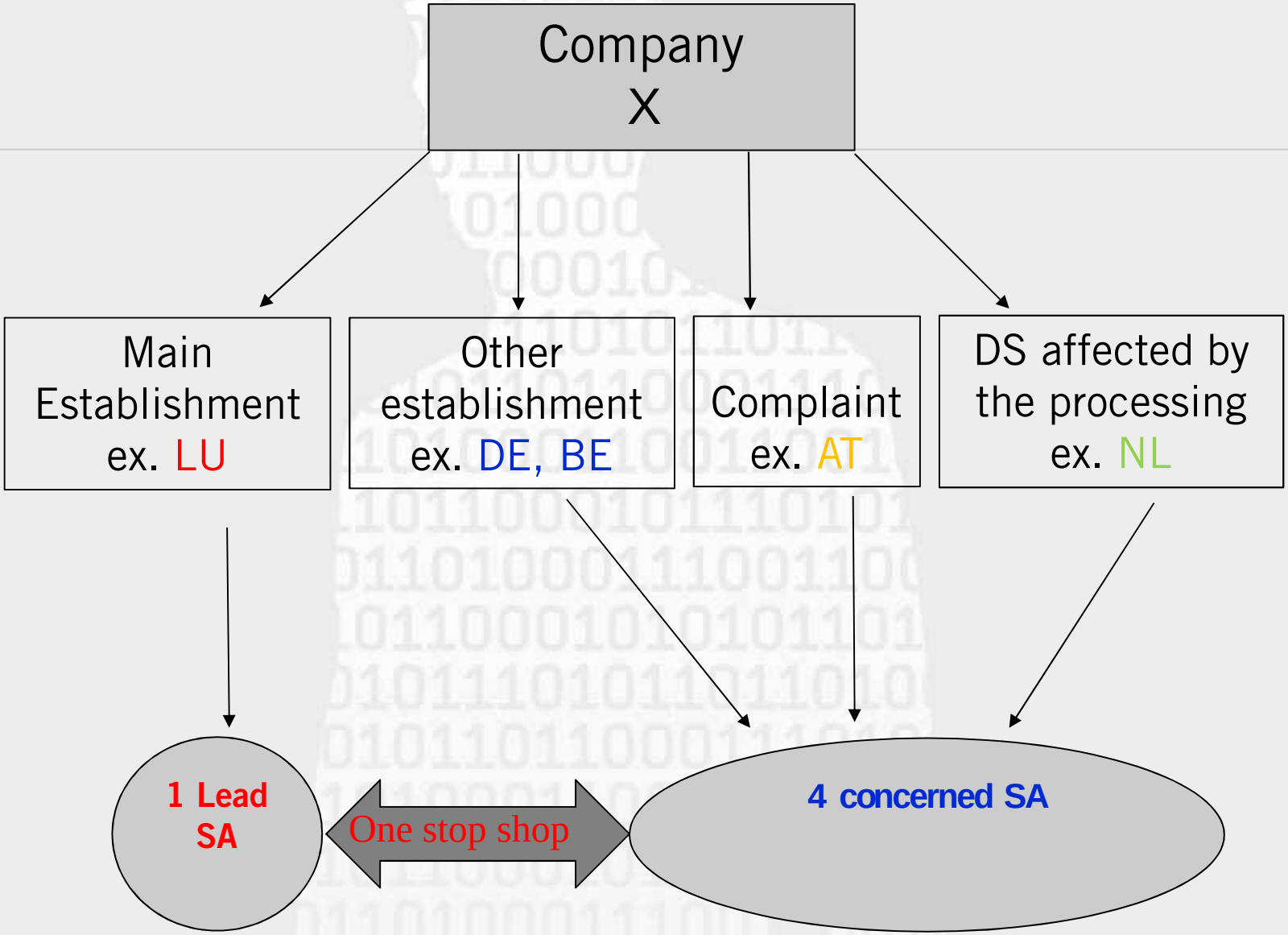
3c. The consistency mechanism

Overview

- **Central role of the EDPB** within the consistency mechanism. It contributes to the consistent implementation of the GDPR through:
  - Compulsory opinion when the SA wishes to adopt certain measures (Art. 64.1) (eg.: list of processings requiring a DPIA)
  - Binding decision when the EDPB plays its role in the resolution of conflicts (Art. 65.1)
  - Urgency procedure (Art. 66), derogatory procedure to the one-stop-shop and consistency mechanism

- Advantages:
  - For DS: common interpretation within the entire EU of the rights provided by the GDPR
  - For DC/DP: common interpretation within the entire EU of the obligations imposed by the GDPR

Example with 5 SAs



4a. Evolution of national law
National provisions

- The regulation grants a certain leeway in the implementation of national provisions related to specific sectors or aspects (research, employment law…).
- There will be an evolution of the national law in order to align it with the provisions of the regulation.
- Information regarding these exclusively national aspects will be provided depending on the progress of the work related to the modification of the national legislation.

4b. Evolution of national law

Interim measures

- Filing in August of a draft bill (projet de loi) in order to simplify the current administrative procedures (Projet de loi n°7049).

- This draft bill removes the requirement of an autorisation for processings related to:
  - Surveillance,
  - Credit and solvency,
  - Interconnection of data,
  - Data transfer to third countries.

- A notification will still be required.

5a. Work of article 29 Working Party

- In February 2016, the article 29 Working Party published its priorities in relation to the implementation of the new regulation.

- 3 main actions were defined:
  - Setup of a task force for the creation of the EDPB,
  - Preparation of the one-stop-shop and consistency mechanism,
  - Publication of guidance for DC/DP.

5b. Work of article 29 Working Party

- For guidance, the following 4 themes were selected:
  - The new right to portability,
  - The concept of high risk and data protection impact assessment (DPIA),
  - Certification,
  - The Data Protection Officer (DPO).

- The cooperative work between the various supervisory authorities on these guidance documents has made considerable progress, but they are still under review. They will probably be released by the end of this year or in the beginning of next year.

For more information

- The presentations (mostly in French) given during the conference of 11th October 2016 can be downloaded from:

- http://www.cnpd.public.lu/en/actualites/national/2016/10/conference-CNPD-SMC-1110/index.html

- Our thematic section on this subject:

- http://www.cnpd.public.lu/en/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees/Reglement-general-sur-la-protection-des-donnees/index.html

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