# CNPD Course: Data Protection Basics

The obligations of controllers



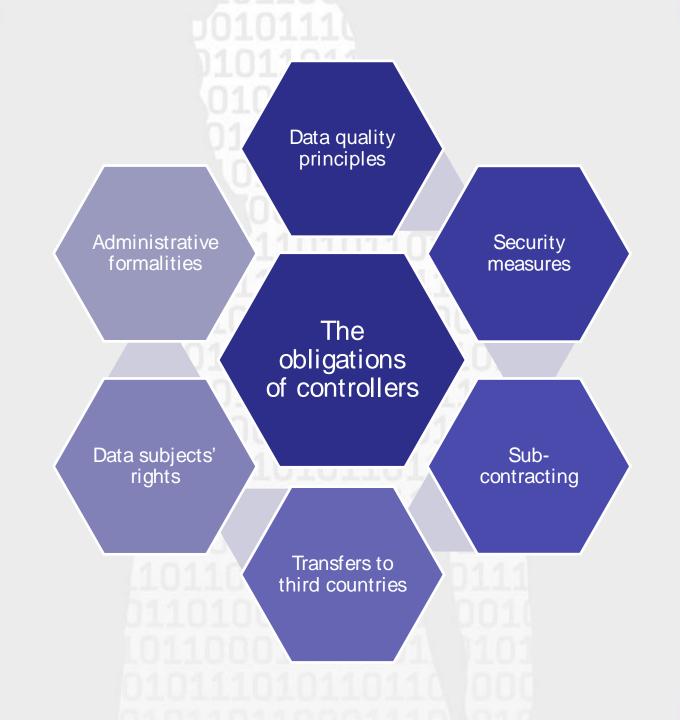
Esch-sur-Alzette (Belval)

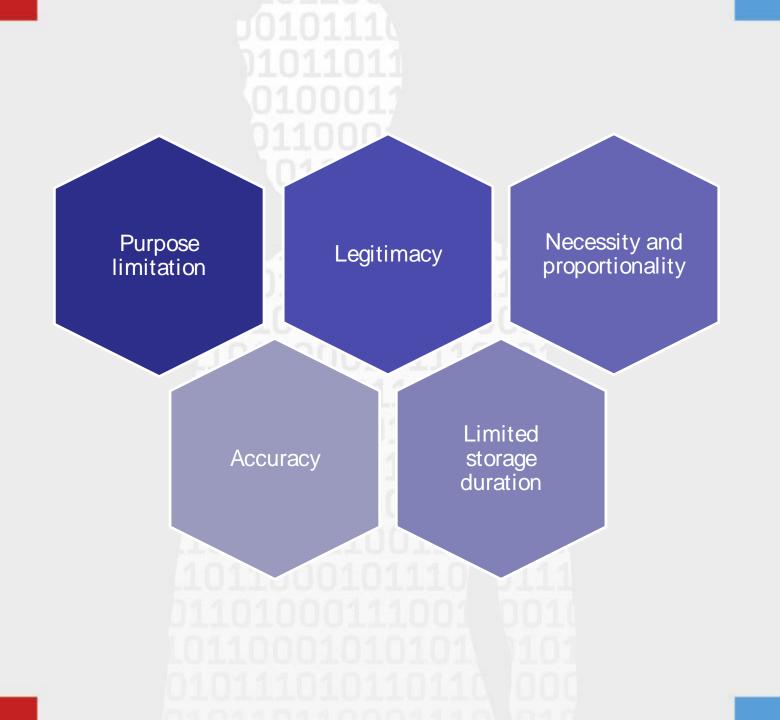
4-6 July 2017

Mathilde Stenersen Legal department

### Programme

- 1. Introduction
- 2. Basic concepts
- 3. The rights of data subjects
- 4. The role of the CNPD
- 5. The obligations of controllers
- 6. Main innovations introduced by the new European data protection regulation





#### A. Purpose limitation

- Purpose = objective pursued by the controller for the processing of personal data
  - Purpose(s) must be defined beforehand
  - 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
    - « compatible purposes », where the further processings activities are compatible with the initial purpose for which data had been collected (principle criterion = reasonable expectation of the data subject)

#### B. Legitimacy (1/2)

- = need to legitimise the processing on the restrictive criteria as provided for in the Act
  - Article 5 of the Act (« general regime »)
    - e.g. consent, legal obligation, necessary for the execution of a contract, public interest
  - Article 6 of the Act (sensitive data)
    - Principle: the processing of sensitive data is prohibited
    - Exceptions: f.ex. explicit consent, public interest, labour law obligation for the controller
  - Article 7 of the Act (data processed by health services)
    - e.g. medical reasons, healthcare/scientific research + explicit and written consent

#### B. Legitimacy (2/2)

- Article 8 of the Act (judicial data)
  - Principle: processing of judicial data prohibited
  - Exception: if foreseen by law
  - e.g. criminal records
- Article 10 and 11 of the Act (processing for surveillance purposes)
  - e.g. videosurveillance, surveillance of IT tools, recording of phone conversations, use of biometric systems, geolocalisation, surveillance of access to workplace and work schedules
  - → Restrictive conditions + prior authorisation from CNPD
  - N.B. Work place surveillance Article 11 of the Act and Article L.261-1 of the Labour Code (cf. brochure)

- C. Necessity and proportionality
- = only processing of necessary data and link to the purpose
  - Processing of adequate, relevant and non excessive data in relation to the purposes for which they are collected
  - → « Need to have, not nice to have »
    - Can the purpose be achieved without processing personal data or by processing less data?
    - → Are there other, less intrusive means that could be used?

#### D. Accuracy

- the data processed by the controller must be accurate and, where necessary, kept up to date
  - Inaccurate or false data can harm the data subject
  - Every effort must be made to ensure the data being processed are accurate and up to date
  - If this is not the case, the personal data must be rectified or erased

#### E. Limited storage duration

- process data for no longer than is necessary for the purposes for which the data were collected and processed
  - If the purpose is fully achieved, the data must either be (definitively) erased or (fully) anonymised
  - The adequate retention period of personal data is relative and depends on the purpose (ex.: prescription period) → case-by-case analysis
  - In any event: data cannot be retained forever solely because the data could perhaps be useful one day

# II. Security measures

- Technical and organisational measures in accordance with the "state of the art"
- Measures must be adapted to the context and particularities of each specific area
  - Analysis: nature of data, legal prescriptions, size of company or organisation, complexity of the system, risks incurred, etc.

# III. Sub-contracting / processors

- Mandatory written contract (controller processor) providing:
  - Processor will act only on instructions from the controller
  - Obligations of the controller (regarding security measures) are also incumbent on processor

#### IV. Transfers to third countries

- Free flow of data within the EU/EEA is permitted
- Transfer of personal data to third countries (= outside the EU) is prohibited, unless:
  - Adequacy decision for the country (or for a specific sector within a given country)
  - Adequate safeguards (in Luxembourg: BCRs or Standard Contractual Clauses, with a prior authorisation from the CNPD)
  - Derogations for occasional, specific transfers (e.g. consent, contract, etc.)

# V. Respecting data subjects' rights

#### = the data subjects must:

- be informed about the processing activities concerning them (before the data are processed);
- have access to the data about them that is being processed (on their request);
- be able to object on compelling legitimate grounds relating to their particular situation to the data about them being processed;
- be able to ask for the rectification of inaccurate or false data.
- N.B. Unsolicited communications and marketing specific rights and obligations → Act of 30 May 2005

# VI. Administrative steps (1/4)

#### 1. Prior authorisation

#### – When?

- Surveillance and surveillance in the workplace (including videosurveillance)
- Processing of genetic data
- Processing of biometric data
- Credit status and solvency (except for PSF and insurance companies → notification)
- Combination of data (interconnexion)
- Further processing/secondary use of data for historical, statistical or scientific purpose (≠ direct collection of data from data subject)
- Specific case: transfer of personal data to third countries

# VI. Administrative steps (2/4)

#### 1. Prior authorisation

#### - How?

- Videosurveillance, data transfers to third countries → form on CNPD website
- Surveillance of access to workplace and work schedules -> « engagement formel de conformité » (single decisions)
- Other processings: simple letter no predefined form

#### – What?

- Legal review of the processing by the CNPD
- Wait for the approval of the CNPD to begin the processing activities

# VI. Administrative steps (3/4)

#### 2. Prior notification

- When?
  - For any processing not subject to prior autorisation and for which no exemption has been foreseen
- How?
  - Notification form on CNPD website
- What?
  - Administrative formality (no legal review)

## VI. Administrative steps (4/4)

#### No administrative steps required if:

- No personal data
- Personal data are fully anonymised (strict definition)
- Exemption of notification for "daily" and non-sensitive processing activities
  - e.g. Human resources and management of applications (recruitment), Salary Administration, Bookkeeping, Client and supplier administration, ...
- Nomination of a data protection officer (DPO) → register
  - Except for processing subject to authorisation → authorisation still needed

# VII. In the future (GDPR)

- Current obligations (e.g. data quality principles) remain valid
  - → some have been strengthened or become more detailed
- New obligations have been added
  - e.g. accountability principle → the controller must be able to demonstrate compliance with the GDPR

#### but:

 Administrative steps will be removed (authorisation, notification)

# Thank you for your attention!

**Questions?** 



#### 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