CNPD Course:
Data Protection Basics

New aspects introduced by the General Data Protection Regulation

Esch-sur-Alzette (Belval)

4-6 July 2017

Georges Weiland

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**

Introduction

- Luxembourgish law of 2002/Directive of 1995
- **Issue** : No longer adapted to the current applications and technological evolutions
- The new European Data Protection Regulation (or "GDPR") **updates and strengthens the rights** of data subjects **and the duties** of data controllers and their processors.
- The GDPR aims to :
  - provide for a uniform legal protection
  - provide for uniform rules
  - ensure a strong, unique and consistent application
- Directly applicable throughout Europe
- Applicable from **25 May 2018**

Overview of the GDPR

The GDPR is divided into **11 chapters** :

- Chapter I: General provisions (articles 1 to 4)
- Chapter II: Principles (articles 5 to 11)
- Chapter III: Rights of the data subject (articles 12 to 23)
- Chapter IV: Controller and processor (articles 24 to 43)
- Chapter V: Transfer of personal data to third countries (articles 44 to 50)
- Chapter VI: Independent supervisory authorities (articles 51 to 59)
- Chapter VII: Co-operation and consistency (articles 60 to 76)
- Chapter VIII: Remedies, liability and sanctions (articles 77 to 84)
- Chapter IX: Specific data processing situations (articles 85 to 91)
- Chapter X: Delegated acts and implemented acts (articles 92 to 93)
- Chapter XI: Final provisions (articles 94 to 99)

General provisions

- Material scope
  - Processing by automated means and non-automated means
  - Exclusions
- Territorial scope
  - Applicability of the GDPR linked to the processing of data
  - Offering of goods and services related to individuals within the EU
  - Monitoring of behaviour of individuals within the EU
  - Possibility of Member States to legislate in certain areas
- New definitions
  - In line with current well-established practices

Principles

- Lawfulness of processing
  - More restrictive consent
  - Children's consent
- Sensitive data
  - New aspects to adapt to current practices
- Criminal convictions and offences
  - Specific provision
- Processing which do not require identification

Rights of the data subject

- More transparency
  - Public information related procedures and mecanisms
- Increased information to personal data
  - Diversification
- Strengthened right of access
  - New aspects
- Right to rectification
- Right to restriction (New aspect)
  - Limit instead of erasing

Rights of the data subject

- Right to erasure (New aspect)
  - « Right to be forgotten »
- Profiling
  - Precisions
- Right to data portability (New aspect)
  - « Improved » right of access, interoperability
- Right to object
  - Particular situation, marketing, profiling

Controller and processor

- General obligations
  - General rule of responsability
  - « Data protection by design » and « data protection by default »
- Joint controllers
  - Specific provision
- Representatives
  - Controllers and processors not established in the EU
- Processor(s)
  - Contract content extended/sub-processing regulated
  - Responsability of processors

Controller and processor

- Records of processing activities
  - Replace notification obligations with a documentary trace
  - 250 employees/high risk
- Security of personal data
  - Also applicable to processors
  - Before & after
- Notification of a data breach
  - General application/Exceptions
  - To the supervisory authority (72h)
  - To the data subjects (if « high risk »)

Controller and processor

- Data protection impact assessment (New aspect)
  - If processing of personal data is to result in a high risk
  - List of scenarios in the GDPR
- Prior consultation of the supervisory authority
  - If analysis shows that risk cannot be reduced by reasonable means
  - Supervisory authority can provide a list of processing activities which are subject or not to DPIA's
- Data protection officer
  - Tasks : opinions, advisor, supervision and point of contact
  - Independent, sufficient resources, access to data
  - Mandatory or voluntary appointment
  - Possibility to appoint a single DPO

Controller and processor

- Codes of conduct
  - Contribute to an effective application of the GDPR
  - Developed according to different sectors and companies
  - Possibility of developing by representing organisations
  - Publicity

- Certification
  - Certify compliance of processing with the GDPR
  - Issued for 3 years max (renewable)
  - Voluntary subjection
  - Cannot decrease responsability
  - Without prejudice to the tasks and powers of the supervisory authority

Transfer of personal data to third countries

- As under the 95 Directive, compliance with rules
- Data transfers governed with tools which ensure adequate protection
- New extension : subsequent transfers from a third country to another country or organisation also submitted to EU law (« protection in a row »)

Supervisory authorites

- Obligation to provide for independant supervisory authorities

- « One Stop Shop »
  - « Lead » authority
  - Local competence

Cooperation and consistency

- Cooperation
  - « Lead » authority must cooperate with « concerned » authorities
  - Aim : Find consensus
  - If disagreement→ « Consistency mecanism »
- Mutual assistance
  - Mandatory
  - Response within 1 month
- Joint operations
  - Joint investigations or joint enforcement measures
  - Obligation to invite and to respond to requests for participation
  - Delegation of powers possible

Cooperation and consistency

- Opinion of the European data protection board
  - **Opinion** on specific draft decisions prior to their adoption
  - **Binding decision** if dispute between supervisory authorities or if authority does not intend to follow opinion of the board

- Urgency procedure
  - Adopt an urgent and provisional measure in exceptional circumstances
  - Limited period (3 months)
  - Possibility to make it permanent

Remedies, liability and sanctions

- Right to lodge a complaint
  - Authority of habitual residence, of place of work, of place of the infringement
- Right to a judicial remedy against an authority
  - Against a « legally binding decision of a supervisory authority concerning them → [the data subjects]»
- Right to a judicial remedy against a controller or processor
  - Possible suspension procedure
- Representation of data subjects

Remedies, liability and sanctions

- Right to compensation
  - Compensation covers material and immaterial damages
- Corrective measures by the supervisory authority
  - GDPR provides for and lists corrective measures that supervisory authorites must have in place
- Administrative fines by the supervisory authority
  - Major Innovation for Luxembourg
  - In addition to, or instead of corrective measures
  - **Must be effective, proportionate and dissuasive**
  - Maximum **20.000.000.- Euros** or **4 % of the total worldwide turnover** of the preceding financial year

Thank you

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