CNPD Training: Data Protection Basics

The obligations of controllers and processors

Esch-sur-Alzette

11 June 2018

Mathilde Stenersen

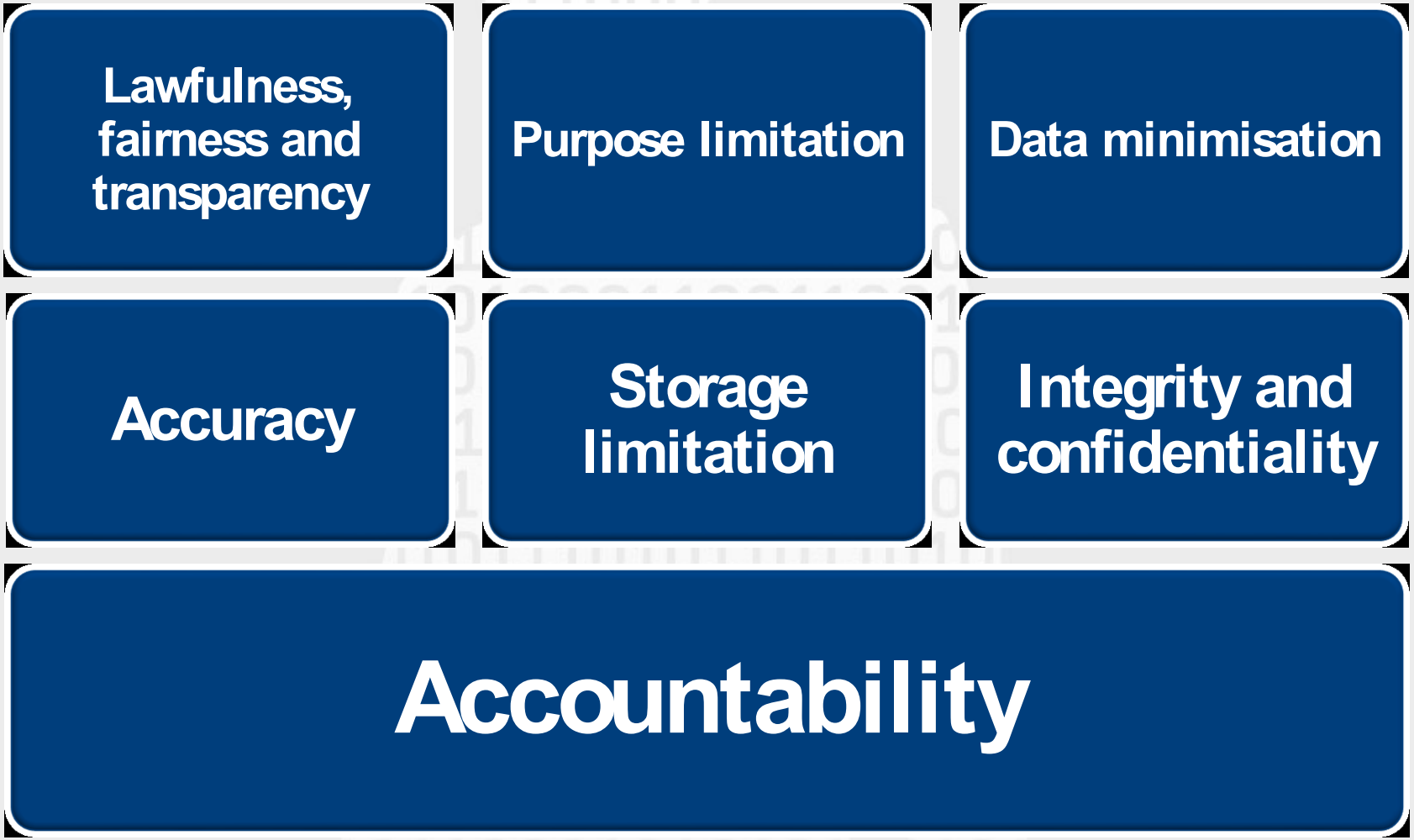
Legal service

Outline

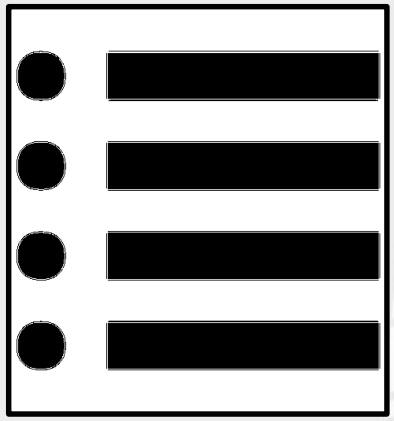
1. Introduction
2. Basic elements
3. The rights of the data subjects
4. **The obligations of controllers and processors**
5. The role of the CNPD


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:

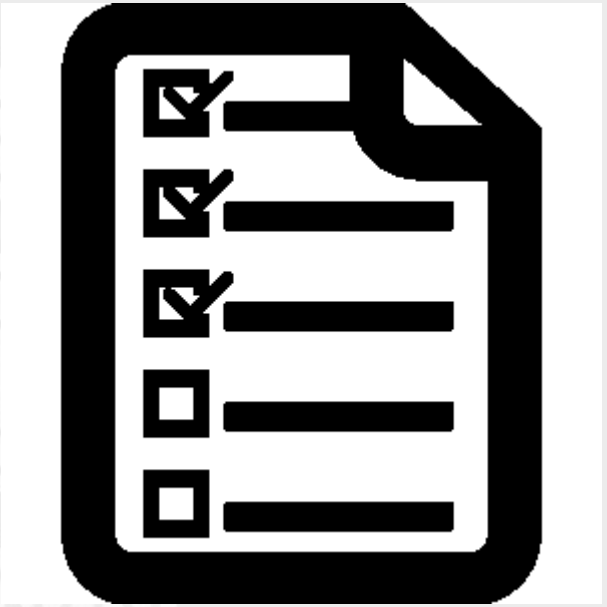
- « Compliance Support Tool » of the CNPD which also contains a register
- Other tools: CPVP (Belgian authority), CNIL (French authority)

Format: 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

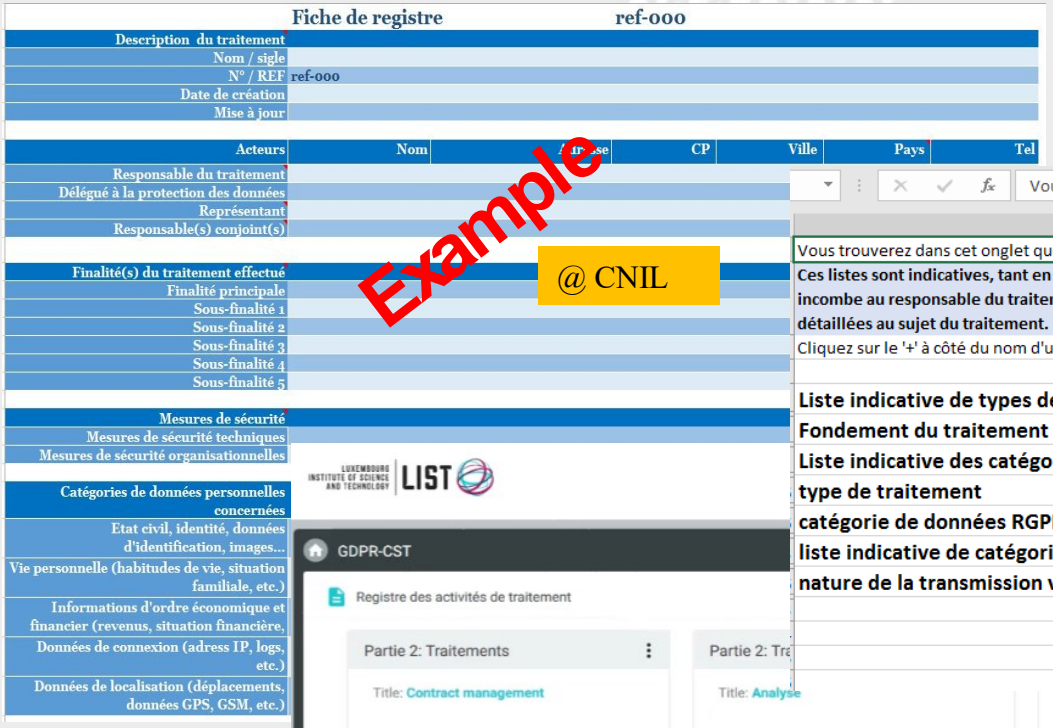
This document is based on the information that must be contained in the register, as required by Article 30 GDPR.

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 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)						

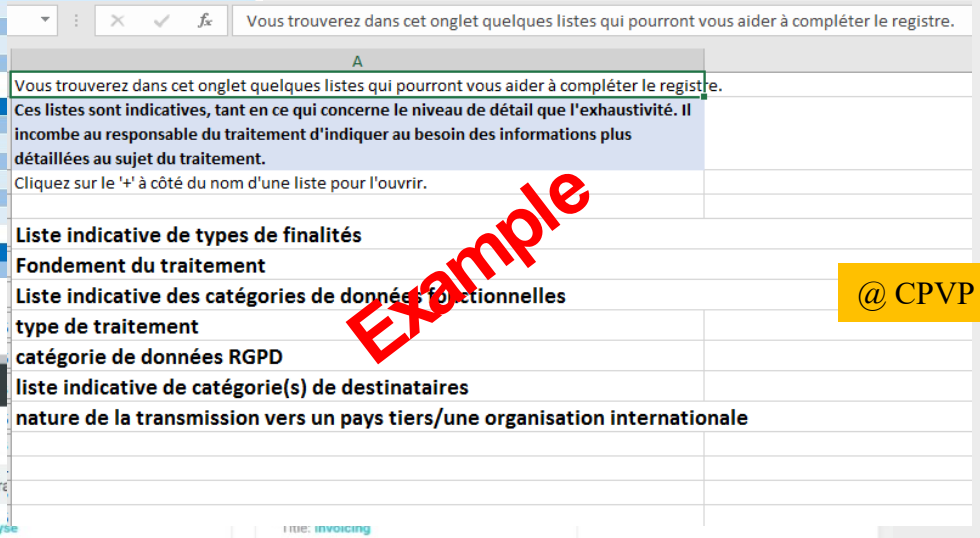
Finalité(s) du traitement effectué
Finalité principale
Sous-finalité 1
Sous-finalité 2
Sous-finalité 3
Sous-finalité 4
Sous-finalité 5

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

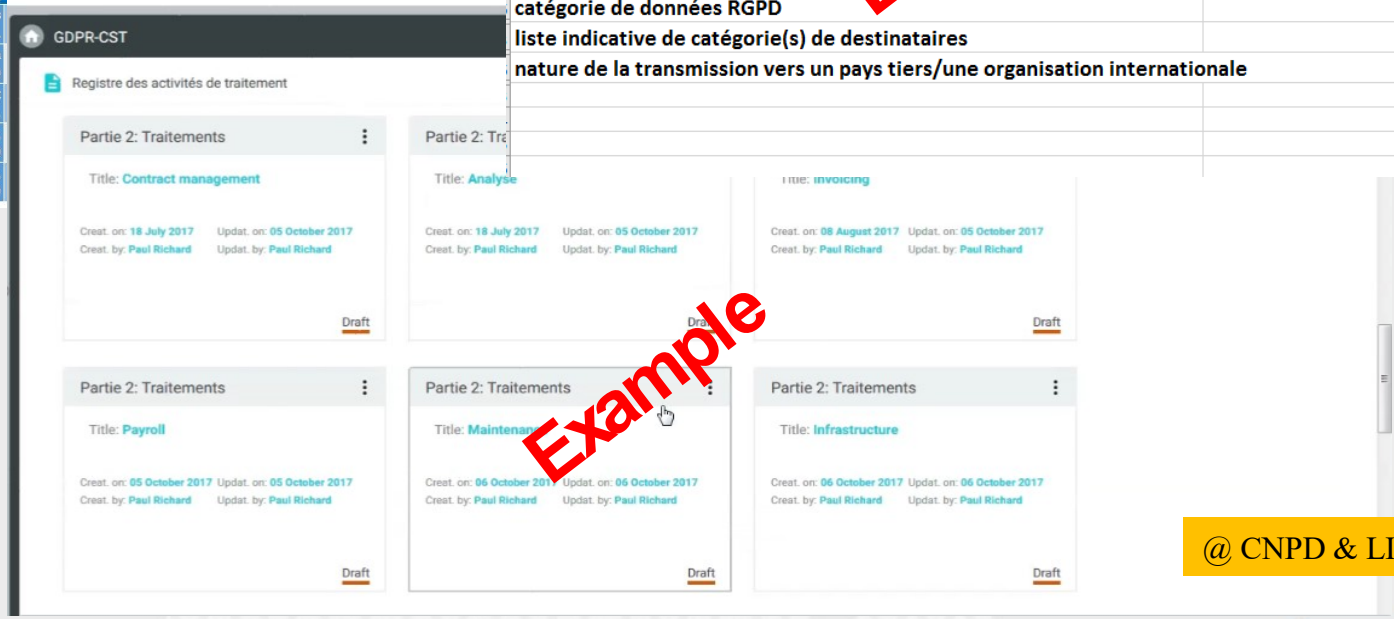


Vous trouverez dans cet onglet quelques listes qui pourront vous aider à compléter le registre.

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



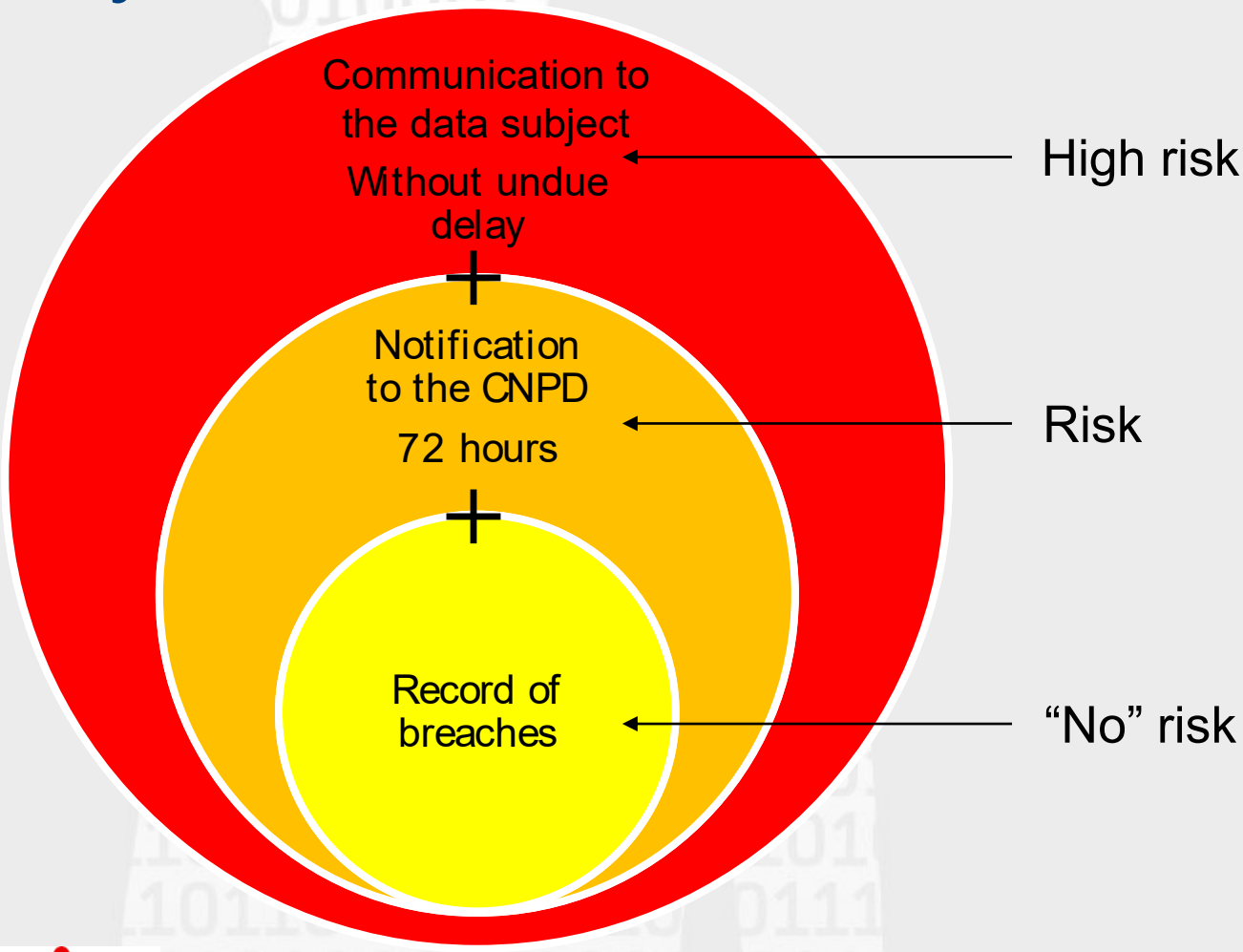
Example

@ 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)

Role: 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:

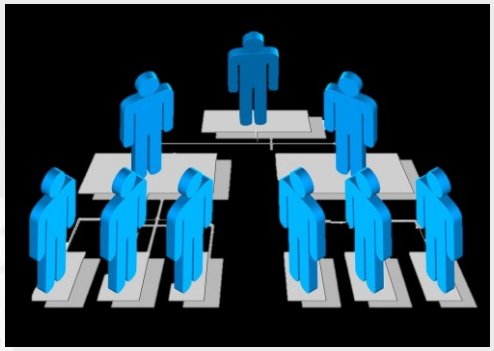
The processors only processes the personal data on documented instructions of the controller

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)

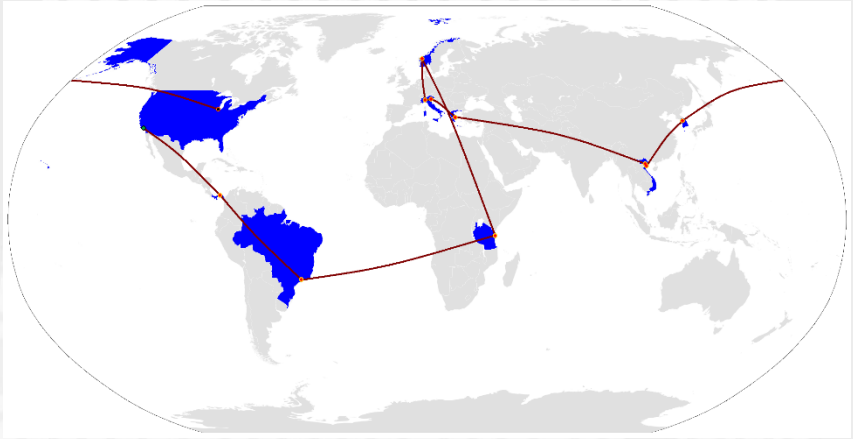
6. Processing

- 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

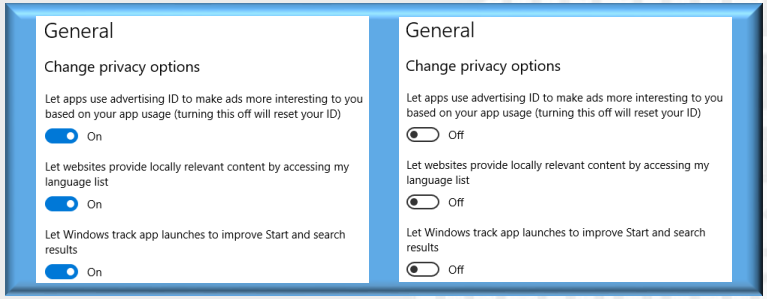
- Free flow of data within the EU/EEA
- Transfer of personal data to third countries (= outside the EU) only possible, if:
  - Adequacy decision
  - Adequate safeguards (e.g. BCRs or Standard Contractual Clauses, etc.)
  - Derogations for specific transfers (e.g. consent, contract, etc.)



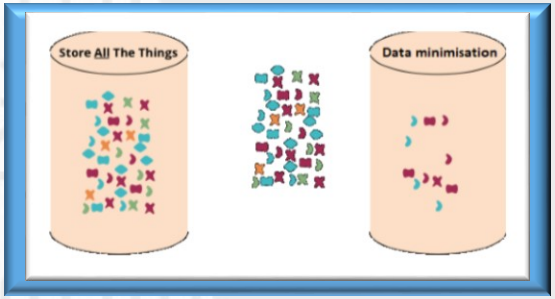
8. The rights of data subjects

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*)

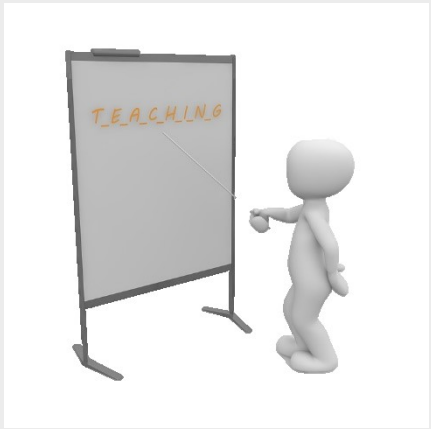


(*Privacy by default*)

- **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