GDPR, A NEW PARADIGM FOR DATA PROTECTION

Didier MARTIN
Délégué à la protection des données

DATA PROTECTION, FOUNDING PRINCIPLES

LIL Law 78/17 of jan. 6th 1978 modified

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la loi.

Information technology should be at the service of every citizen. Its development shall take place in the context of international cooperation. It shall not violate human identity, human rights, privacy, or individual or public liberties.

Everyone has the right to decide and control the uses that are made of personal data concerning him, under the conditions set by law.

REGULATION WITH ADMINISTRATIVE, CIVIL AND CRIMINAL PROVISIONS

Beyond enhaced sanctions powers of supervisory authority - CNIL in France -

GDPR and LIL recognise **group actions** before administrative and civiles courts in cessation and **redress** for personal data breaches.

French Penal Code Arts. 226-16 to 226-24 may punish data protection principles non-compliance :

€ 300,000 and 5 years imprisonment

THREE ESSENTIAL DEFINITIONS FROM GDPR ART 4

- **Personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified either directly or indirectly.

- **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration.

- **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

THE SIX PRINCIPLES OF PERSONNAL DATA PROCESSING ART 5

- Lawfulness, fairness and transparency
- Purpose limitation: *specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*
- Data minimisation : *adequate, relevant and limited to what is necessary*
- Data accuracy
- Storage limitation
- Ensures appropriate security: *intégrity, confidentiality, using appropriate technical or organisational measures*

THE **CONTROLLER** SHALL BE **RESPONSIBLE** FOR

AND BE ABLE TO DEMONSTRATE COMPLIANCE WITH THIS PRINCIPLES

ACCOUNTABILITY, A KEY PRINCIPLE

Accountability is THE essential novelty of the GDPR,

it substitutes, to a system of **prior declaration** imposing **obligations of means**,

a **regulated self-regulation mechanism** that is more fluid

but imposes **result obligations**

For any processing the controller must :

- ✓ Taking into account the nature, scope, context and purposes
- ✓ Evaluate associated risks
- ✓ Determine appropriate mesures to respect and demonstrate RGPD compliance
- ✓ Implément thoses mesures and law requirements
- ✓ Verify operational compliance of processing
- ✓ Take into account any nonconformities and evolutions

THE SIX LEGAL BASES - OR LAWFULNESS - OF A TREATMENT ART 6

- Consent
- Performance of a contract
- Compliance with a legal obligation
- Protect the vital interest of the data subject
- Performance of a task carried out in public interest
- Legitimate interest pursued by the controller

⚠ not provide a valid legal ground in a specific case where there is a clear imbalance between the data subject and the controller
(RGPD Consid. 43)

⚠ Shall not apply to processing carried out by public authorities
(GDPR Art. 6-1.)

CATEGORIES OF DATA WHOSE PROCESSING IS PROHIBITED, EXCEPT SPECIFIC RULES ART 9

- racial or ethnic origin
- political opinions, religious or philosophical beliefs, or trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

⚠ GDPR extends the data heath scope
Consid. 35, Art. 4-15

... And personal data relating to criminal convictions and offences Art 10

INCRERASED FUNDAMENTAL RIGHTS

- Information to be provided art 13 & 14 increrased
- Right of access art 15
- Right to rectification art 16 & 19 increrased
- Right to erasure ‘right to be forgotten’ art 17 & 19 created
- Right to restriction of processing art 18 & 19 created
- Right to data portability art 20 created
- Right to object art 21 & 22 The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. increrased

INFORMATION OF NATURAL PERSONS

- Identity and the contact details of the controller and the DPO
- The purposes of the processing and its legal basis
- *The right to **withdraw consent** at any time*
- The rights of concerned persons
- Catégories of personal data and period for which will be stored
- ***Meaningful information about the logic involved** if automated decision-making, including profiling*
- *Possibles **consequences** of **failure** to **provide** such **data***
- *The recipients or categories of recipients of personal data, if any*
- ***Purpose of others processings** on collected data*
- The right to lodge a **complaint** with a supervisory authority

RECORD OF PROCESSING ACTIVITIES, THE BASIS OF CONFORMITY DOCUMENTATION

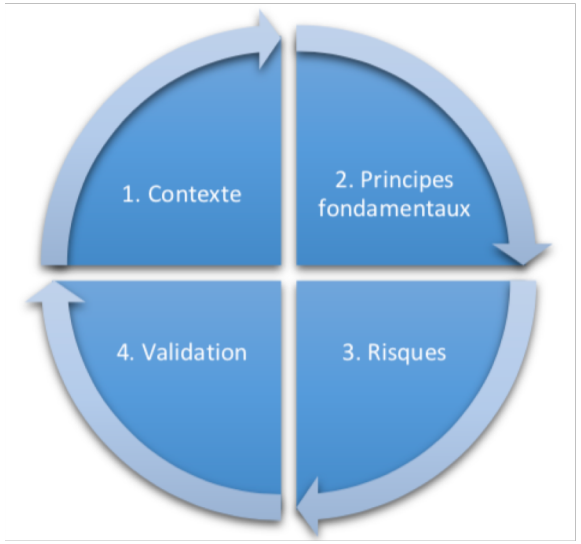
an obligation for controlers, he lists for each processing :

- Identity and the contact details of the controller and the DPO
- The purposes of the processing and those legal basis
- Categories of natural persons concerned
- Catégories of personal data and period for which will be stored
- Catégories of recipients
- Where applicable, transfers of personal data to a third country and adequate level of protection guaranties
- Where possible, the envisaged time limits for erasure of the different categories of data
- Where possible, a general description of the technical and organisational security measures

DATA PROTECTION IMPACT ASSESSMENT - DPIA -

An essential tool for documenting the compliance of personal data processing likely to create high risks, the DPIA - Data Protection Impact Assessment - consists of :

- A **systematic description** of the envisaged **processing operations** and the **purposes** of the processing
- An **assessment** of the **necessity** and **proportionality** of the **processing operations** in relation to the purposes
- An **assessment** of the **risks** to the rights and freedoms of data subjects
- The **measures** envisaged to **address the risks**, including safeguards, security measures and mechanisms to ensure the **protection of personal data** and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.



Source CNIL, PIA la méthode Ed. fév. 2018

INCREASED TRANSPARENCY AND MORE DISTRIBUTED RESPONSIBILITIES

Extensive transparency against data breaches

- In the case of a personal **data breach**, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, **notify** the personal data breach **to the supervisory authority**.
- When the personal **data breach** is likely to result in a **high risk** to the rights and freedoms of natural persons, the controller shall communicate the personal data breach **to the data subject** without undue delay.
- The **supervisory authority**, having considered the likelihood of the personal data breach resulting in a high risk, **may require controller to communicate** the personal data breach to the data subject.

More distributed responsibilities

- Where two or more **controllers jointly determine** the **purposes** and **means** of processing, they shall be **joint controllers**
- GDPR gives the **Processors** a legal responsabilities. Processor must document GDPR respect, maintain a record of processing activities and provide technical and organizational guarantiees.