BONN & SCHMITT
AVOCATS

In the perspective of the E.U. Regulation: How to ensure compliance and traceability (The principle of Accountability)

Alain GROSJEAN

Definition of Accountability

Implementation of a data protection program: Global vision

Abandoning the preliminary formalities in relation to notifying the regulatory authorities.

In exchange for the implementation of the principle of Accountability.

An economy of 2.3 billions euros.

Definition

The new principle of accountability consists, for controllers, of implementing concrete measures in order to ensure that legislation on personal data protection is respected, including the obligation of transparency and traceability, which allows for the documentation of measures, which have been taken.

Implementation of the principle of accountability

Article 24 of the European Regulation: "*Taking into account the nature, scope context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in compliance with this Regulation. Those measure shall be reviewed and updated where necessary.*"

These measures must be proportionate to the processes.

Adhering to Codes of Conduct or a mechanism of certification.

Accountability goes further than simple compliance.

It takes in account the context – the environment– of the processing in every field of a specific activity.

Collaborative work.

Controllers, data protection staff, regulatory authorities, public or private actors, professional associations etc.).

Co-regulation

We are talking about a system by which a public body, for instance an independent regulatory authority, establishes a framework which different actors are trying to define measures aimed at remedying a market failure.


Internal rules
Notification of personal data breaches
Internal documentation
Accountability
Data protection officer
Data protection impact assessment
Privacy by design

IMPLEMENTATION OF THE PRINCIPLE OF ACCOUNTABILITY

A. IMPLEMENTATION OF A PROGRAM OF THE DATA PROTECTION MANAGEMENT ACCORDING TO RISKS.

Privacy by Design & importance of the personal data officer

B. INTERNAL RULES AND CODE OF CONDUCT

C. DOCUMENTATION

D. RISKS ANALYSIS

E DATA PROTECTION OFFICER

F. BREACH NOTIFICATIONS

The Implementation of this program lies on several axes of development :

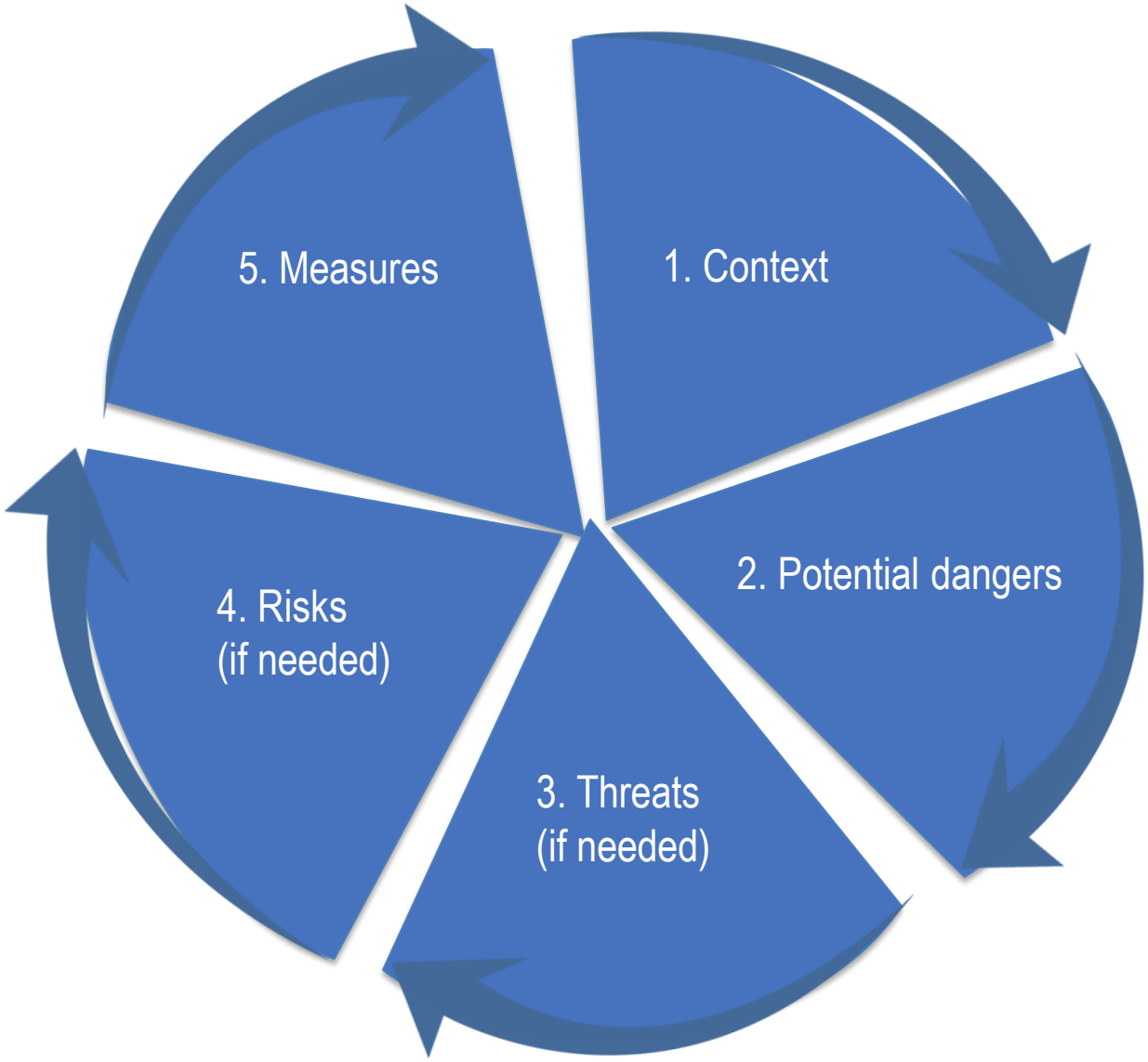
Governance : the company must define the programs functions and governance in order to ensure its proper conduct and maintenance. One or several managers of the data protection program must be appointed.

Control : A control program must be implemented: precise procedures in order to comply with the Regulation requirements. A set of politics, resources and procedures must be drafted in order to face the risks related to personal data protection.

The program must be periodically reviewed : A company must be able to update the program, in order to adapt to changing circumstances. A plan in order to overview and review the program must be developed. The control program must also be evaluated and reviewed.

The controller must implement measures, taking into account the nature, scope, context, goals and risks of processes.

The National Commission for Information Technology and Civil Liberties (CNIL) considers the EBIOS method to be relevant.


1. Context
2. Potential dangers
3. Threats
(if needed)
4. Risks
(if needed)
5. Measures

Risk analysis : Context study

The First Step is the one of the context study. It must allow the controller (or the processor) to get a "clear vision of the perimeter by identifying every useful element for the risks management".

It is also an opportunity for the controller or the processor to collect impacted data and to check that each peace of data is essential to the process considered.

Risks analysis

Step one : identify the potential dangers.

These potential dangers must be analyzed in relation with their potential impact on the concerned persons' rights.

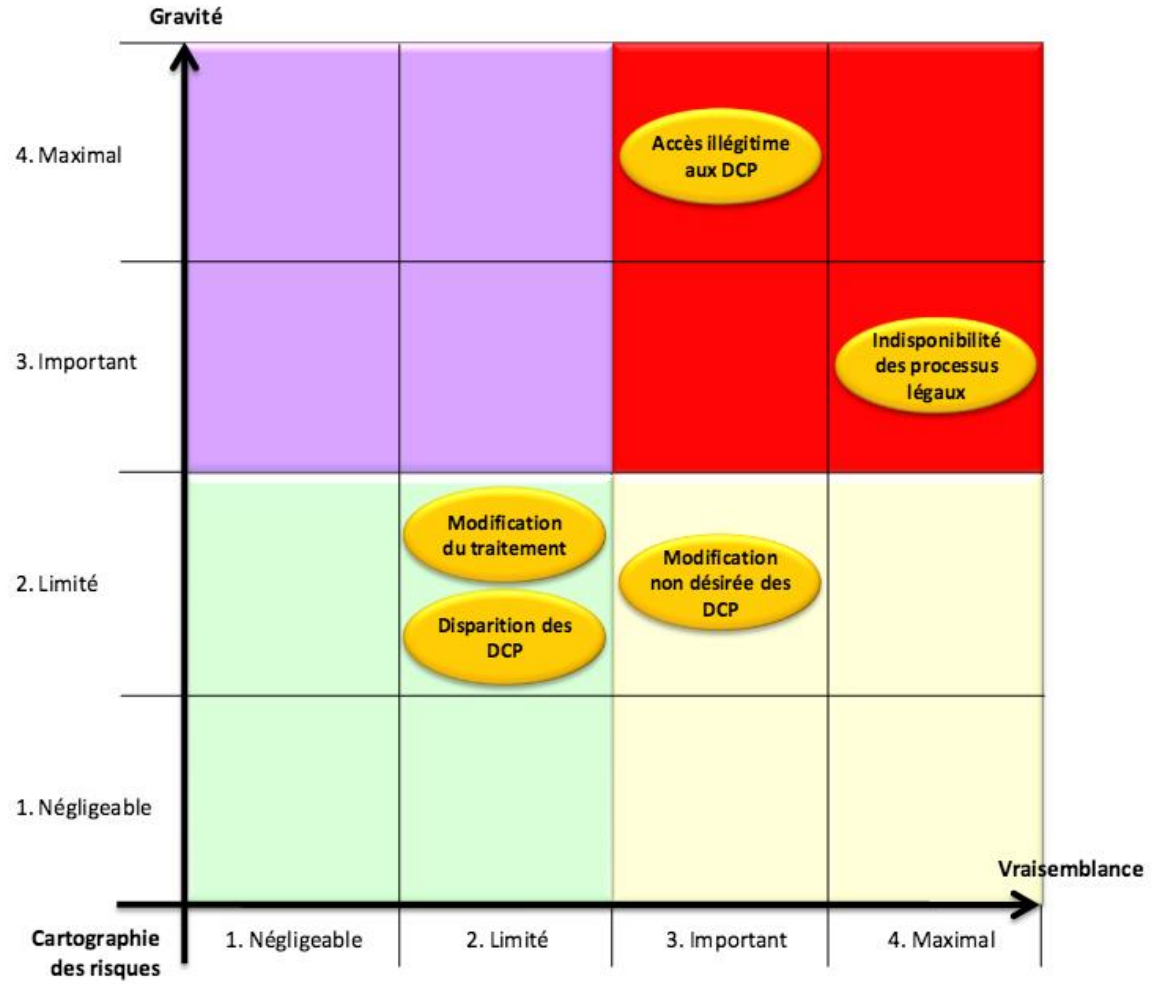
The seriousness of the risk is determined by evaluating the value of the process and the harmfulness character.

Risks analysis

Step one: establishing an explicit list which create a hierarchy of each threat.

Mapping risks with respect to their seriousness and the likelihood or their occurrence in order to establish priorities.

Once the risks have been evaluation and identified, we can process to establish adequate means in order to reduce them.


Gravité
4. Maximal
3. Important
2. Limité
1. Négligeable
Accès illégitime aux DCP
Indisponibilité des processus légaux
Modification du traitement
Disparition des DCP
Modification non désirée des DCP
Vraisemblance
Cartographie des risques
1. Négligeable
2. Limité
3. Important
4. Maximal

Security failure management

Security failure and incident management protocols must be implemented. A set of preparatory actions which define the strategy that the company has to adopt in order to effectively control the threats and incidents in the area of personal data must be in place.

The human factor: It may be the most important aspect of a data protection policy because it is the one on which we have the least ability to control.

Notification of Personal data breaches

The controller has to notify the breach to the regulatory authority within 72 hours after the breach has occurred in case of high risk for the data subjects.

The controller will also have to inform, without delay, the people affected by the breach. This obligation does not exist if the controller implemented measures to render the data incomprehensible (like encryption).

Accountability and privacy by design.

The principle of accountability requires choosing sufficient technologies and architectures.

The implementation and continued updating of sustainable systems to data protection by IT services by applying the principle of Privacy by design is required.

Privacy by design :

Since the conception of the processing and during the processing, the controller must apply "*technical and organizational measures appropriate to the processing activity being carried out and its objectives, such as pseudonymisation, which are designed to implement data-protection principles (…)*" (Article 25 of the EU Regulation).

Accountability measures :

Codes of conduct (Article 40 of the European Regulation)

Documentation (Article 30 of the European Regulation)

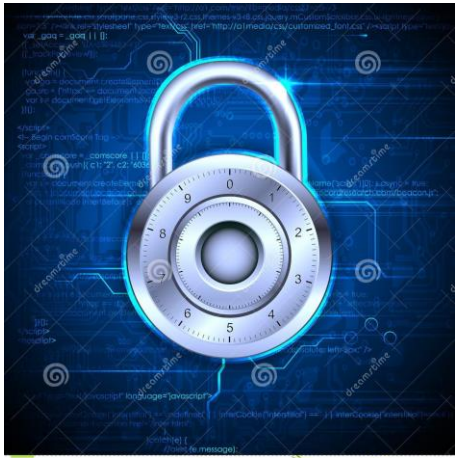
Risks analyses (Article 35 of the European Regulation)

Awareness, training, complaints management and internal audit.

Accountability creates an improved awareness and training on the mechanism of data protection (this shall be an initiative of Human Resources), a complaints procedure, an internal audit scheme and also corrective measures plans in case of incidents, attacks, failures etc.

Code of conduct, good practice, charters and labels, will be tools toward an improved awareness in order to improve staff training in relation to personal data protection rules.

The controller will have to implement internal transparency rules, which should be concise and clear, and easily accessible in relation to personal data protection process and in relation to the exercise, by the concerned persons of their rights (Article 12).



Sanctions, increased liability of the controller and processor.

Administrative fines up to 20 000 000 EUR or in case of an undertaking, up to 4 % of the total worldwide annual turnover

Anonymisation techniques or coding offer guarantees annihilating or reducing accountability obligations.

Regulatory authorities guidance.

Establishment by regulatory authorities of simplified procedures, rules and good practice, and practical sheets anticipating concrete scenarios for companies.

Packs aimed at specific activities (finance, pharmacy, energy)

Regulatory authorities will also have to deliver labels.