

The General Data Protection Regulation

Data Protection Impact Assessment (DPIA)



19th October 2017

Esch-sur-Alzette (Belval)

Alain Herrmann

IT department

Agenda



Goals



Basic principles and
criteria



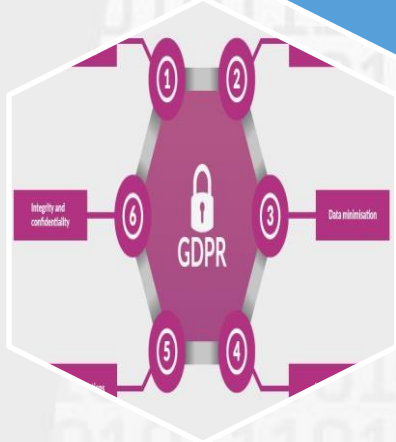
Steps of a DPIA

Goals of DPIA



Setup processings / products/ services that respect privacy

Assess the impacts on private life for the data subjects



Demonstrate the respect of the GDPR's fundamental principles

Examples of impacts on individuals



Physical impacts

Damage to the enjoyment of life, to the aesthetics or economic linked to the physical integrity.

Suffered loss or missed profit on assets of individuals.

Material impacts



Moral impacts

Physical or moral suffering, harm to the aesthetic or enjoyment of life



Examples of physical impacts



Headaches



Defamation that lead to physical or psychological reprisals

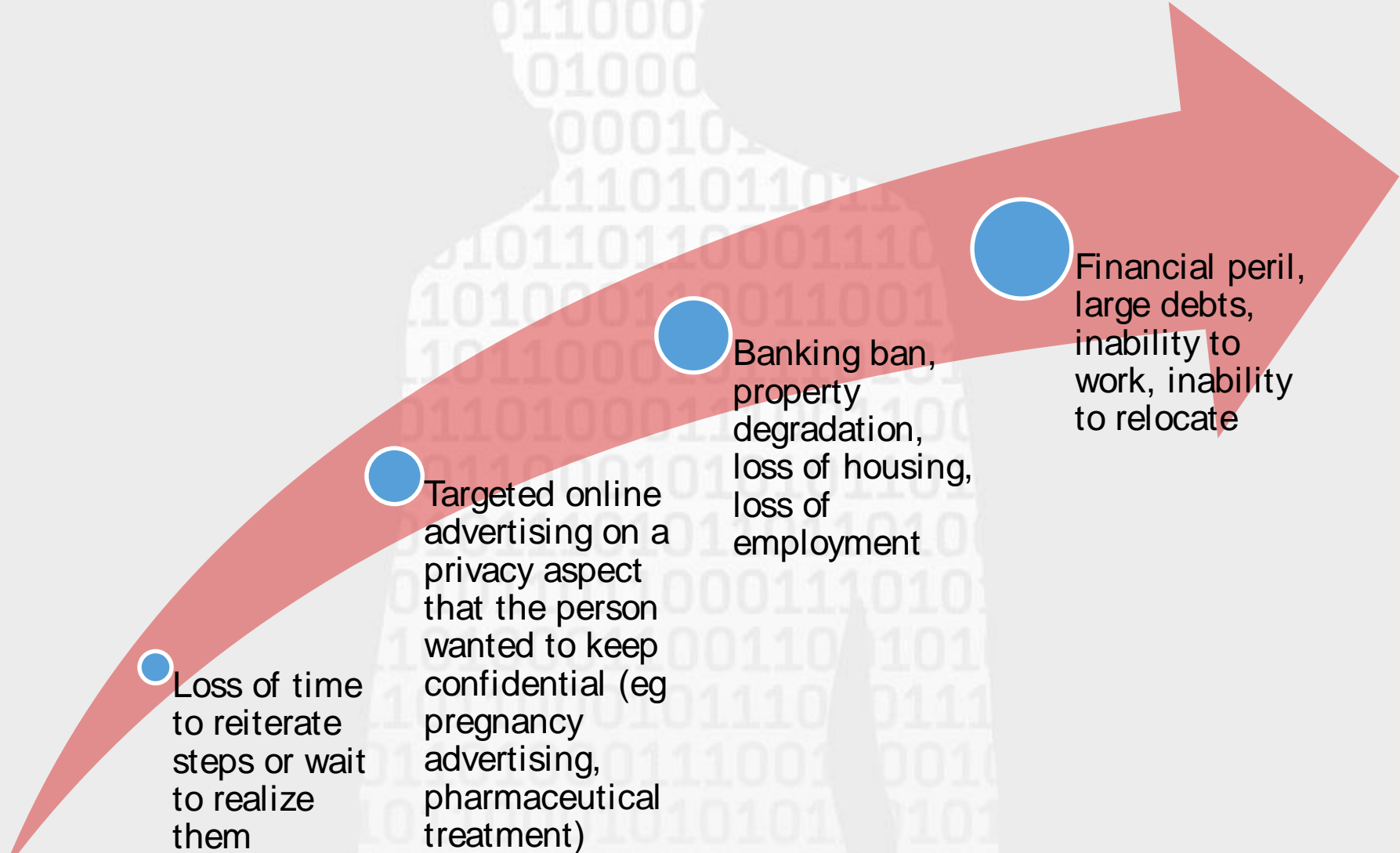


Impairment of bodily integrity, for example, as a result of aggression, domestic accidents, work, etc.



Death (ex: murder, suicide, fatal accident)

Examples of material impacts



Loss of time to reiterate steps or wait to realize them

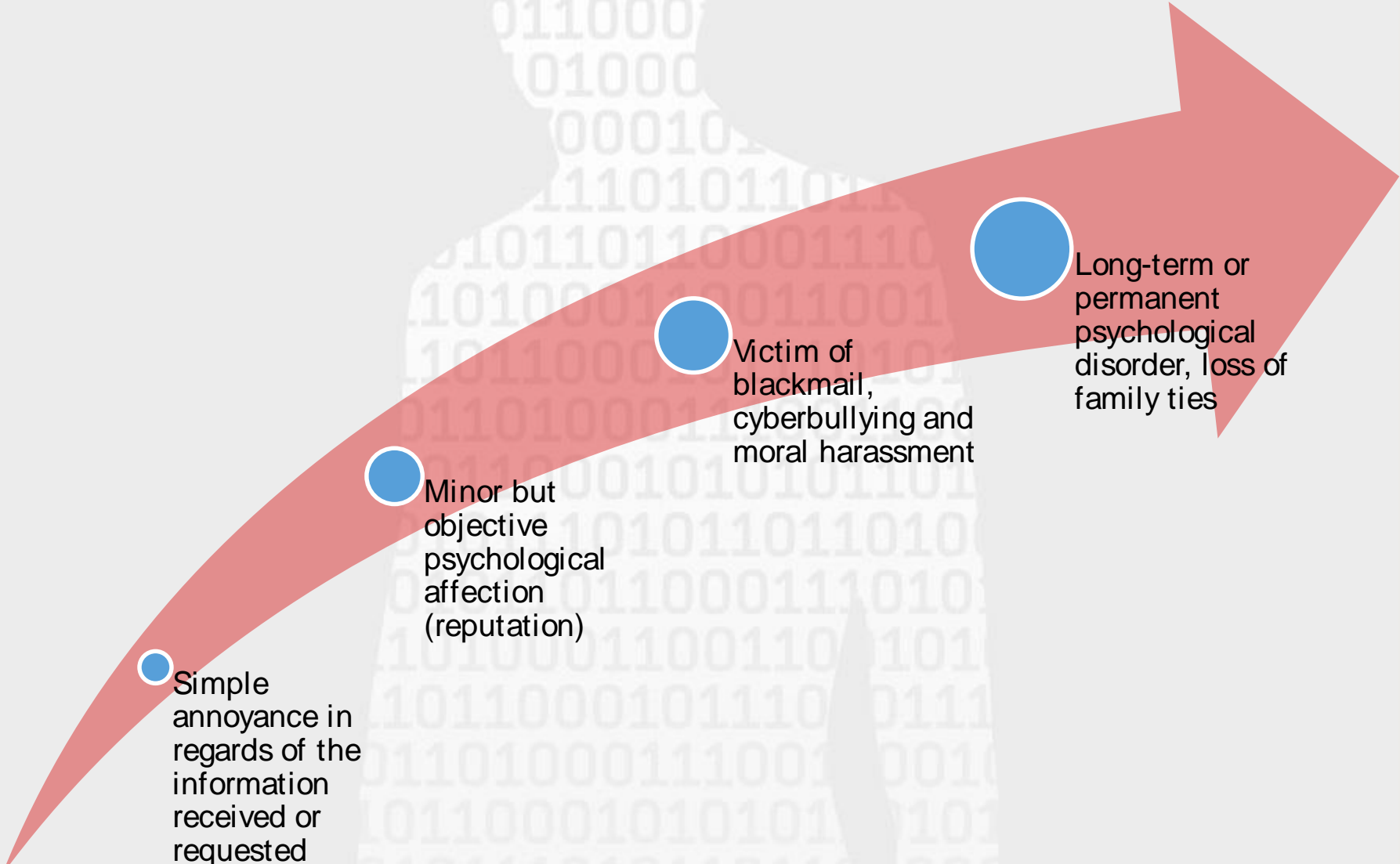
Targeted online advertising on a privacy aspect that the person wanted to keep confidential (eg pregnancy advertising, pharmaceutical treatment)

Banking ban, property degradation, loss of housing, loss of employment

Financial peril, large debts, inability to work, inability to relocate

(Source: CNIL)

Examples of moral impacts



Simple annoyance in regards of the information received or requested

Minor but objective psychological affection (reputation)

Victim of blackmail, cyberbullying and moral harassment

Long-term or permanent psychological disorder, loss of family ties

(Source: CNIL)

What does a DPIA assess?

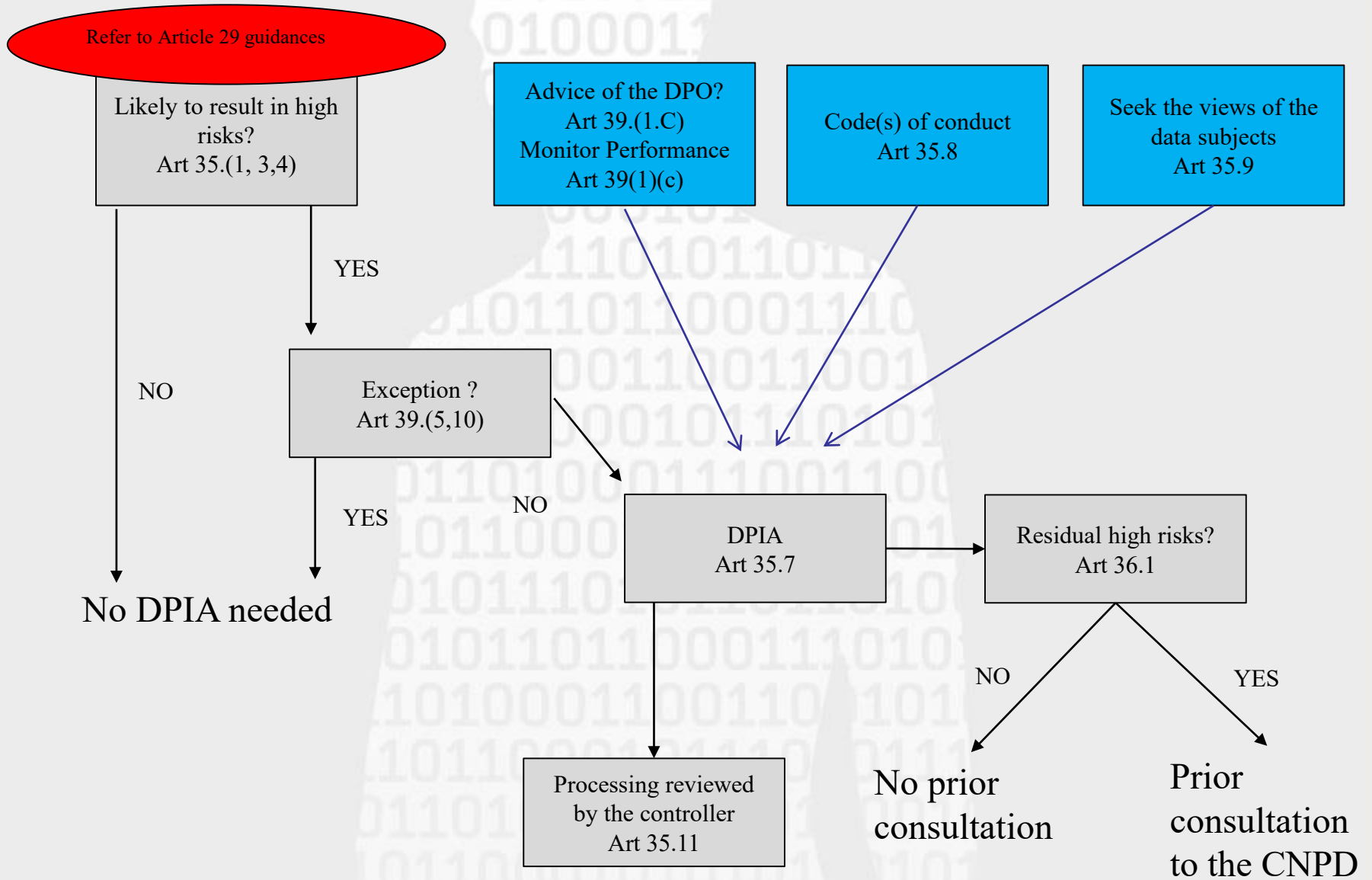
One processing or a set of similar processing operations



- A « *single assessment may address a set of similar processing operations that present similar high risks* »
- « *there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a simple project* »

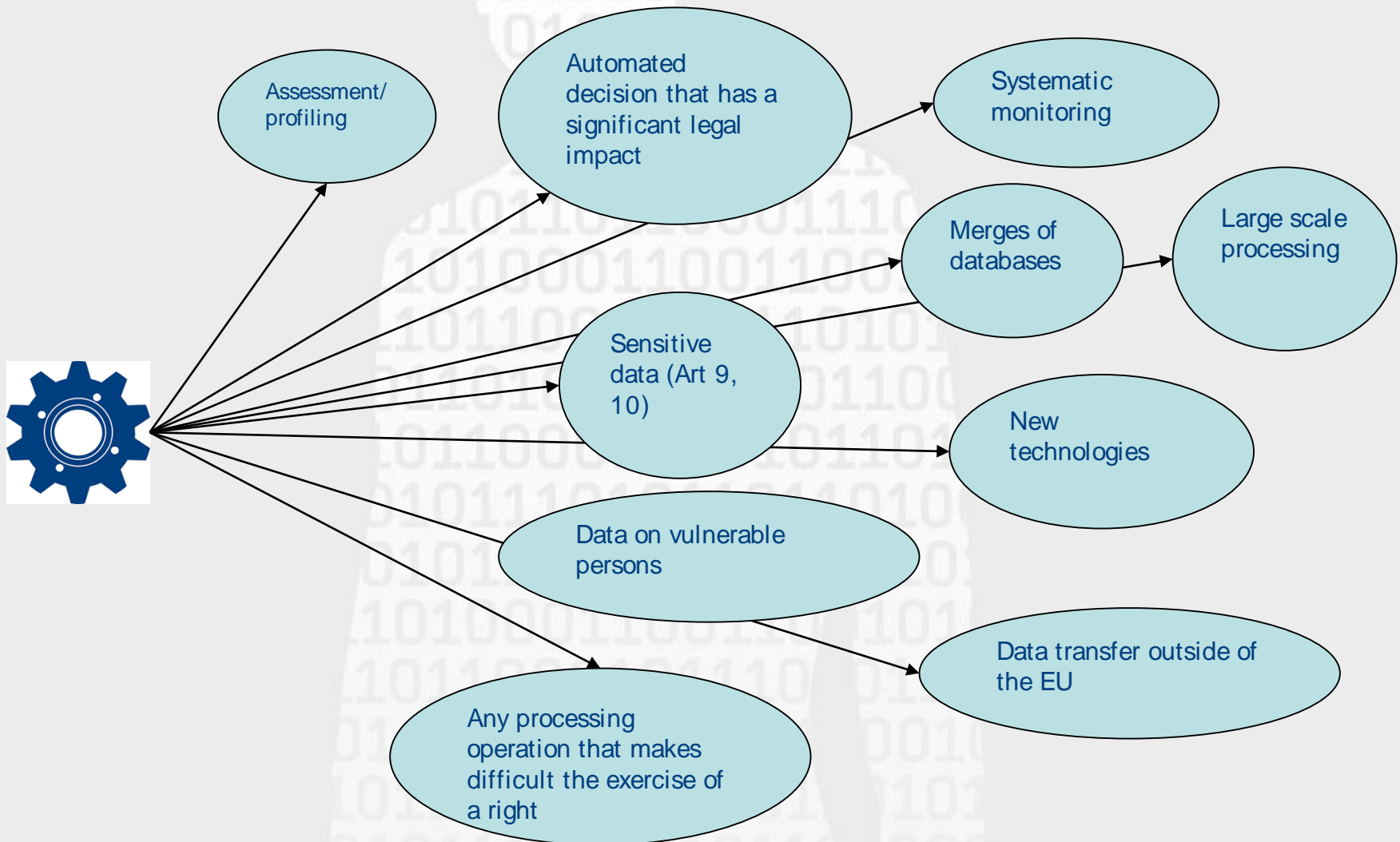


Basic principles



Criteria to perform a DPIA

One processing operation or a set of similar processing operations



Examples

Processing operations	Possible criterias	DPIA needed ?
An hospital processes genetic and health data of its patients	<ul style="list-style-type: none"> - Sensitive data - Data belonging to vulnerable people 	YES
Usage of a video-monitoring system, to monitor the behaviour of drivers on the highway. Usage of intelligent analysis is planned to read the car numbers	<ul style="list-style-type: none"> - Surveillance systématique - Nouvelles technologies 	
Internet site using a mailing list to send a newsletter	None	NO
E-commerce website that displays targeted advertisements based on their visitors consumer habits.	Evaluation / Profiling but not systematic and extensive	

When is a DPIA not needed?



The risk (for the data subjects) is not high



A similar DPIA exists: apply the measures

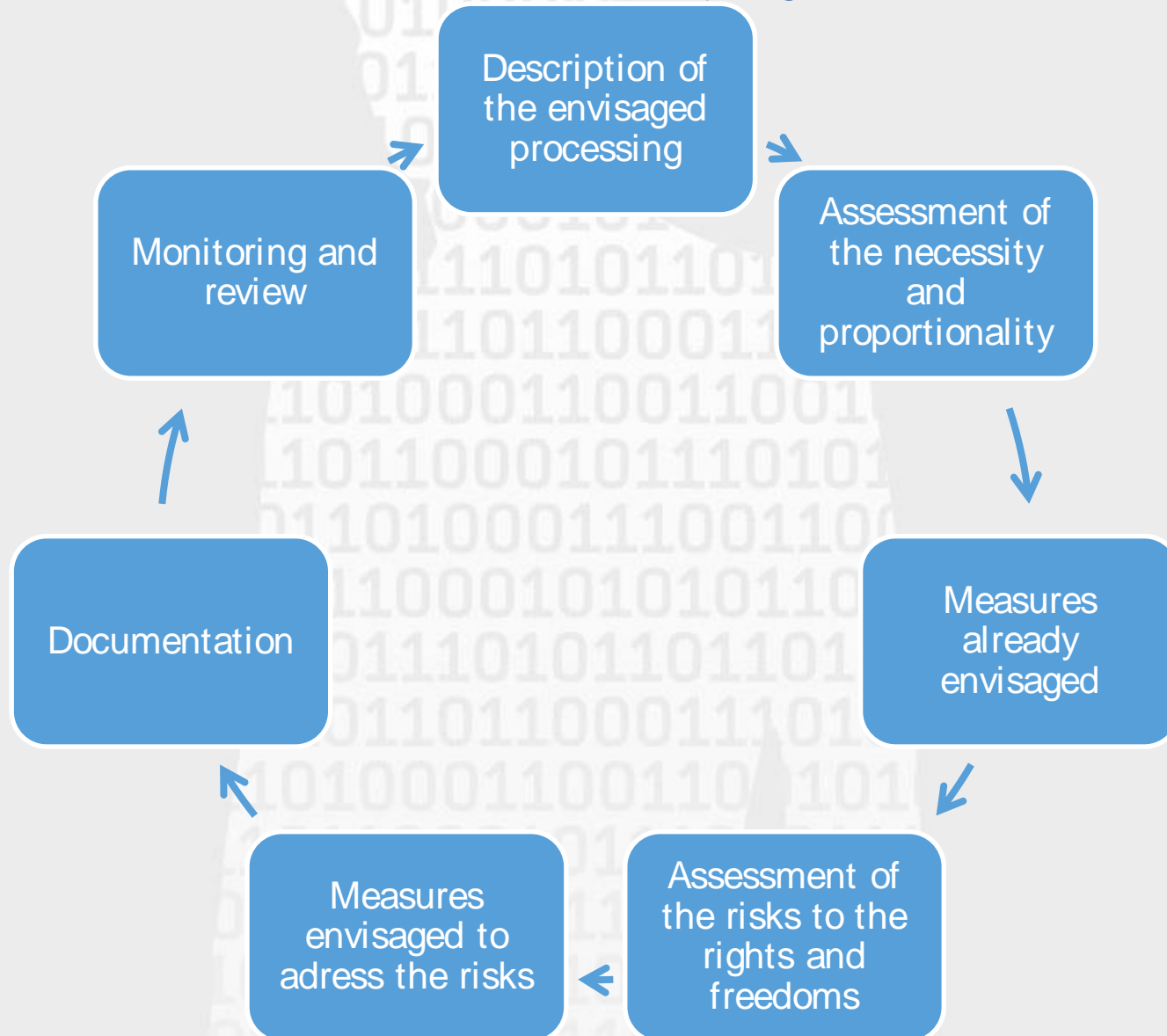


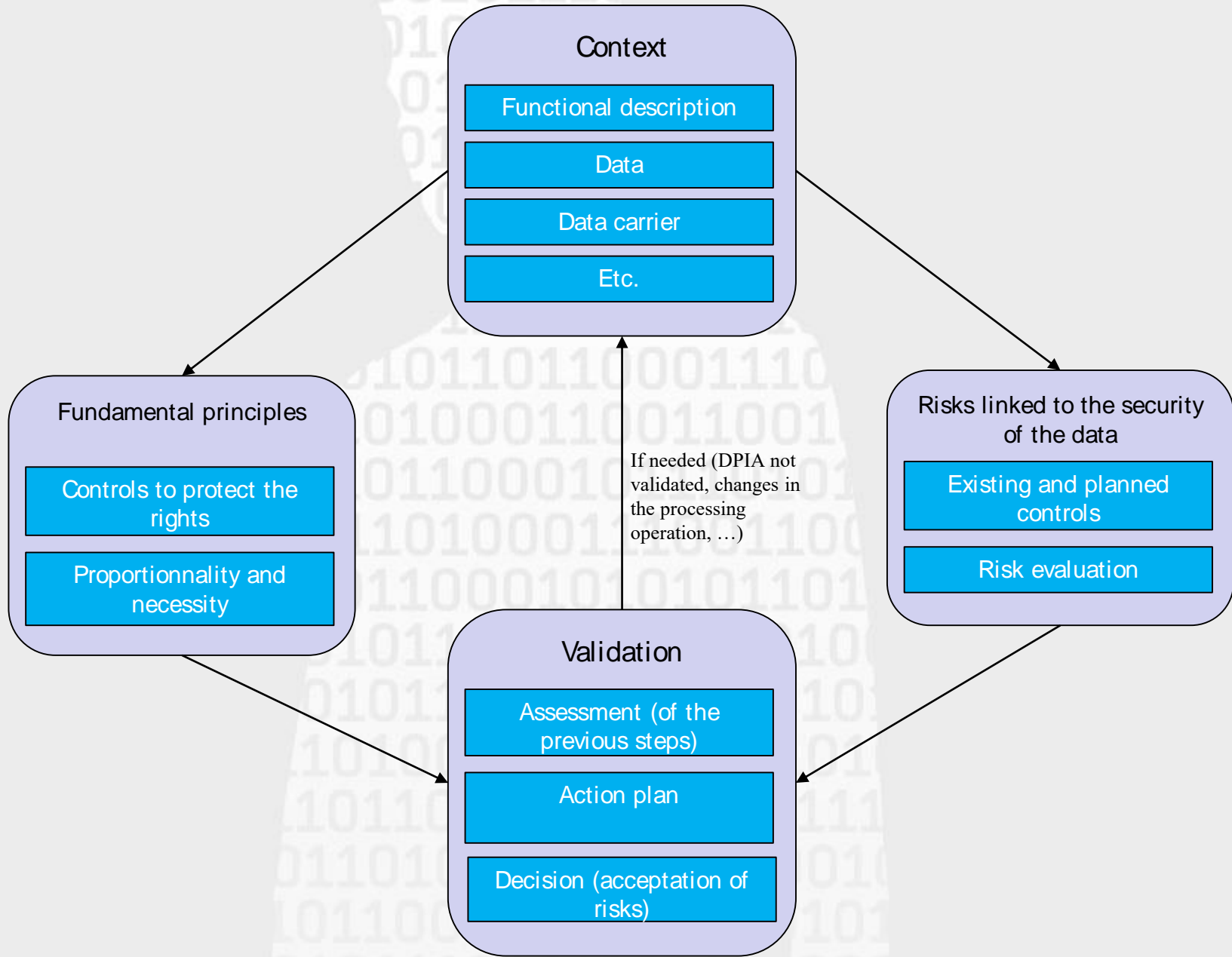
The law regulates the operation and the DPIA is included in it



The processing operation is part of the list of DPIA's exempted processing operations, provided by the CNPD

Iterative process for carrying out a DPIA





Publication and consultation

Prior consultation
to the CNPD

**Needed in case of
residual high risk**

Transparency: a
summary of the
DPIA can be made
public

The DPIA can be
request during a
conformity check
from the CNPD

The players of a DPIA

The data controller



Data Protection Officer



Chief Information Security Officer



'Business' experts



Sectorial experts: legal, ethic, economic



Define and document roles and responsibilities of the actors involved in a DPIA.

Additional information



DPIA and codes of conduct



Tools to help you

29

Guidances of the article
29 working group

Data Protection Governance : exercise of accountability

