Privacy Impact Assessment

February 2021

Claude Castelluccia

Objectives of a Privacy Impact Assessment

- A Privacy Impact Assessment (PIA) is a systematic process to evaluate the impact and risks of collecting, using, and disseminating personally identifiable information in a project, product, service, or system.
- The **goal is to identify privacy risks**; ensure compliance with national or local laws, contractual requirements, or company policy; and put risk mitigation strategies in place.
- The recently passed EU General Data Protection Regulation requires PIAs when data processing is “likely to result in a high risk for the rights and freedoms of individuals
- Performed by data controller (with help of Data Privacy Officer)

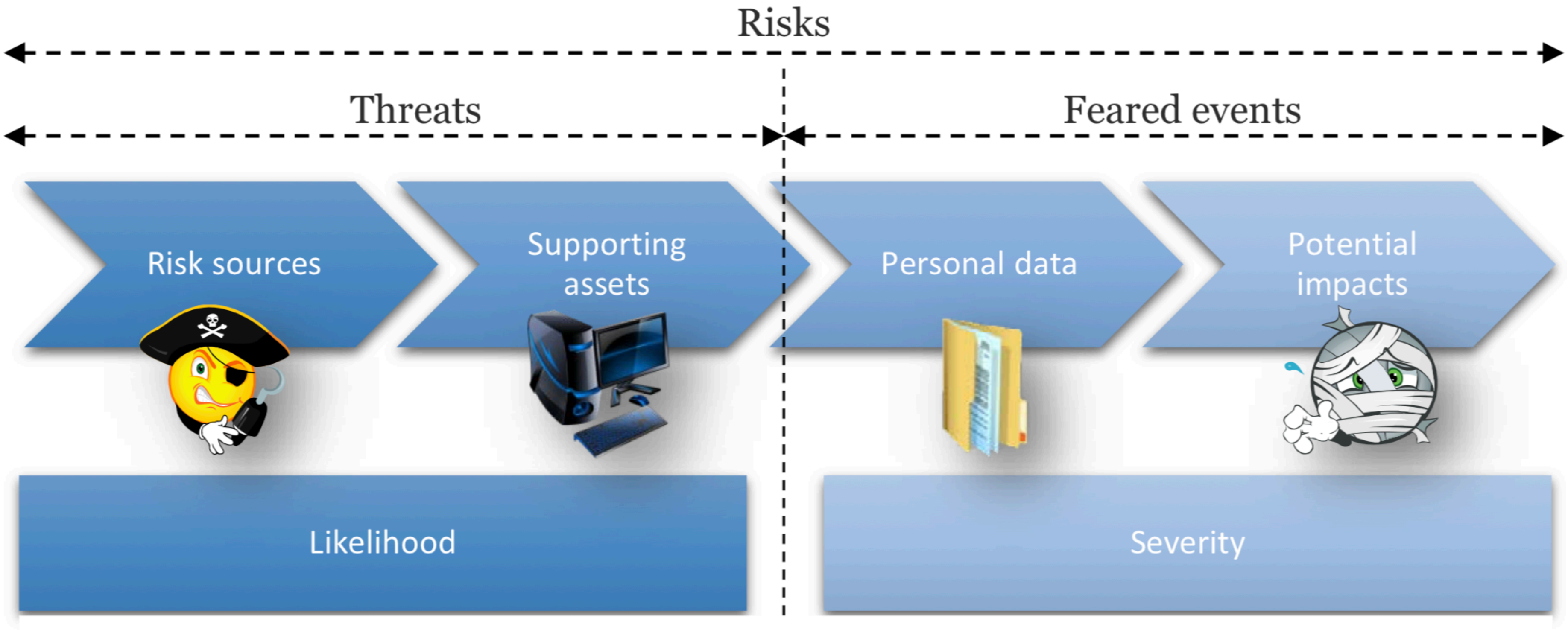
What is a Privacy Risk?

A risk is a hypothetical scenario that describes a feared event and all the threats that would allow this to occur. More specifically, it describes:

- how risk sources (e.g.: an employee bribed by a competitor)
- could exploit the vulnerabilities of supporting assets (e.g.: the file management system that allows the manipulation of data)
- in a context of threats (e.g.: misuse by sending emails)
- and allow feared events to occur (e.g.: illegitimate access to personal data)
- on personal data (e.g.: customer file)
- thus generating impacts on the privacy of data subjects (e.g.: unwanted solicitations, feelings of invasion of privacy, personal or professional problems).

What is a Privacy Risk?

The following diagram summarises all the concepts above:



What is a Privacy Risk?

The risk level is estimated in terms of severity and likelihood:

- **severity** represents the magnitude of a risk. It primarily depends on the prejudicial nature of the potential impacts[15] ;
- **likelihood** expresses the possibility of a risk occurring. It primarily depends on the level of vulnerabilities of the supporting assets when under threat and the level of capabilities of the risk sources to exploit them.

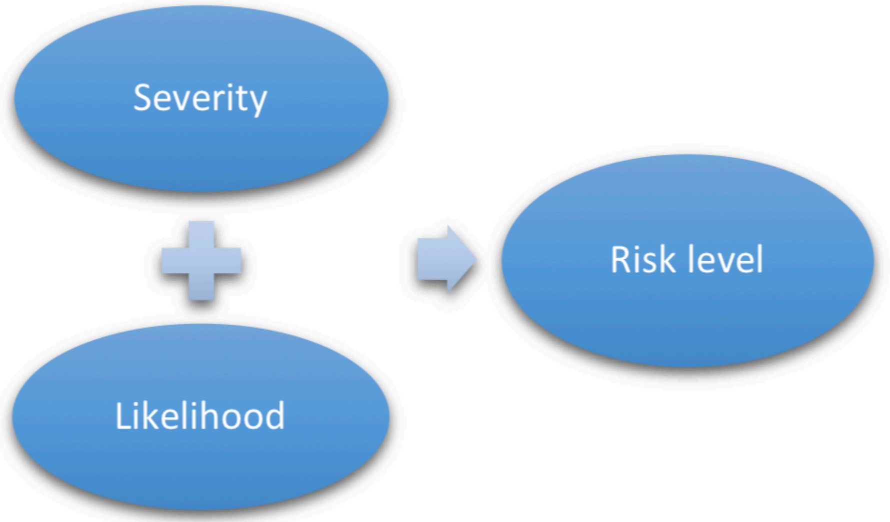
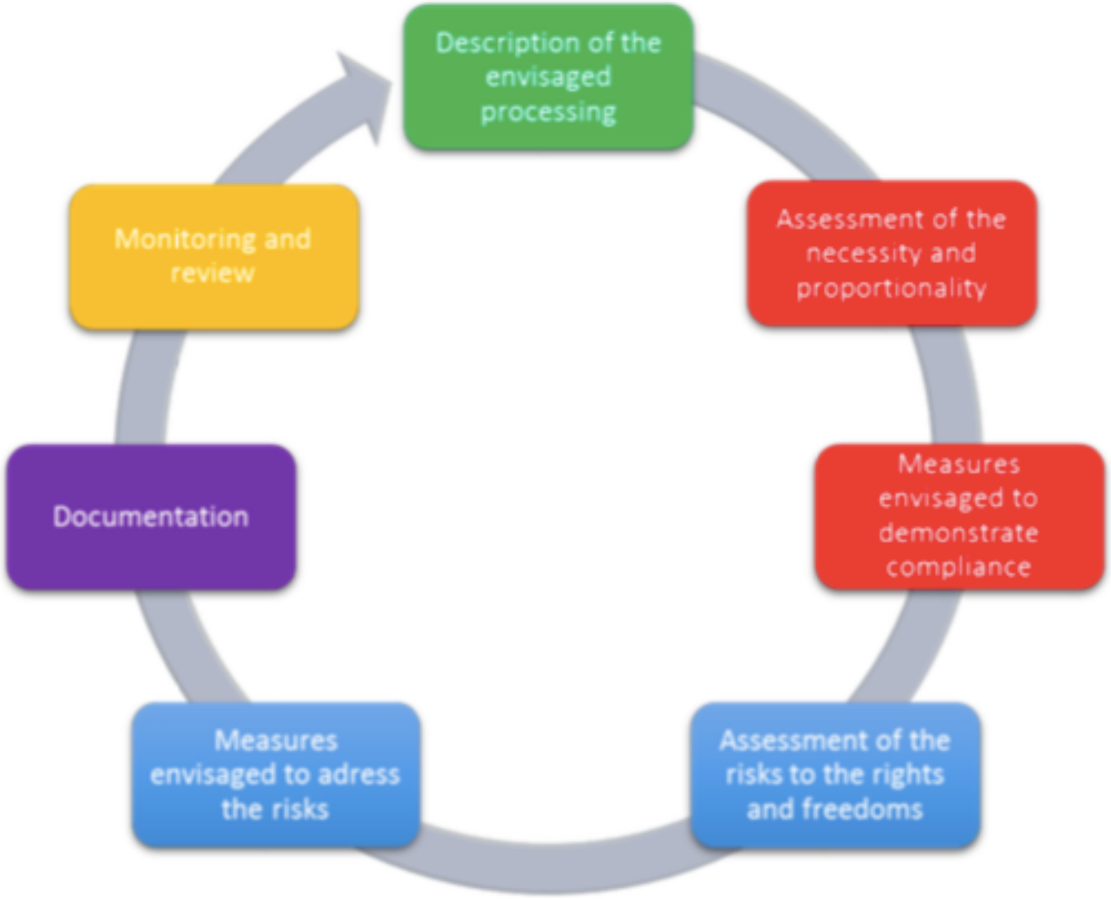


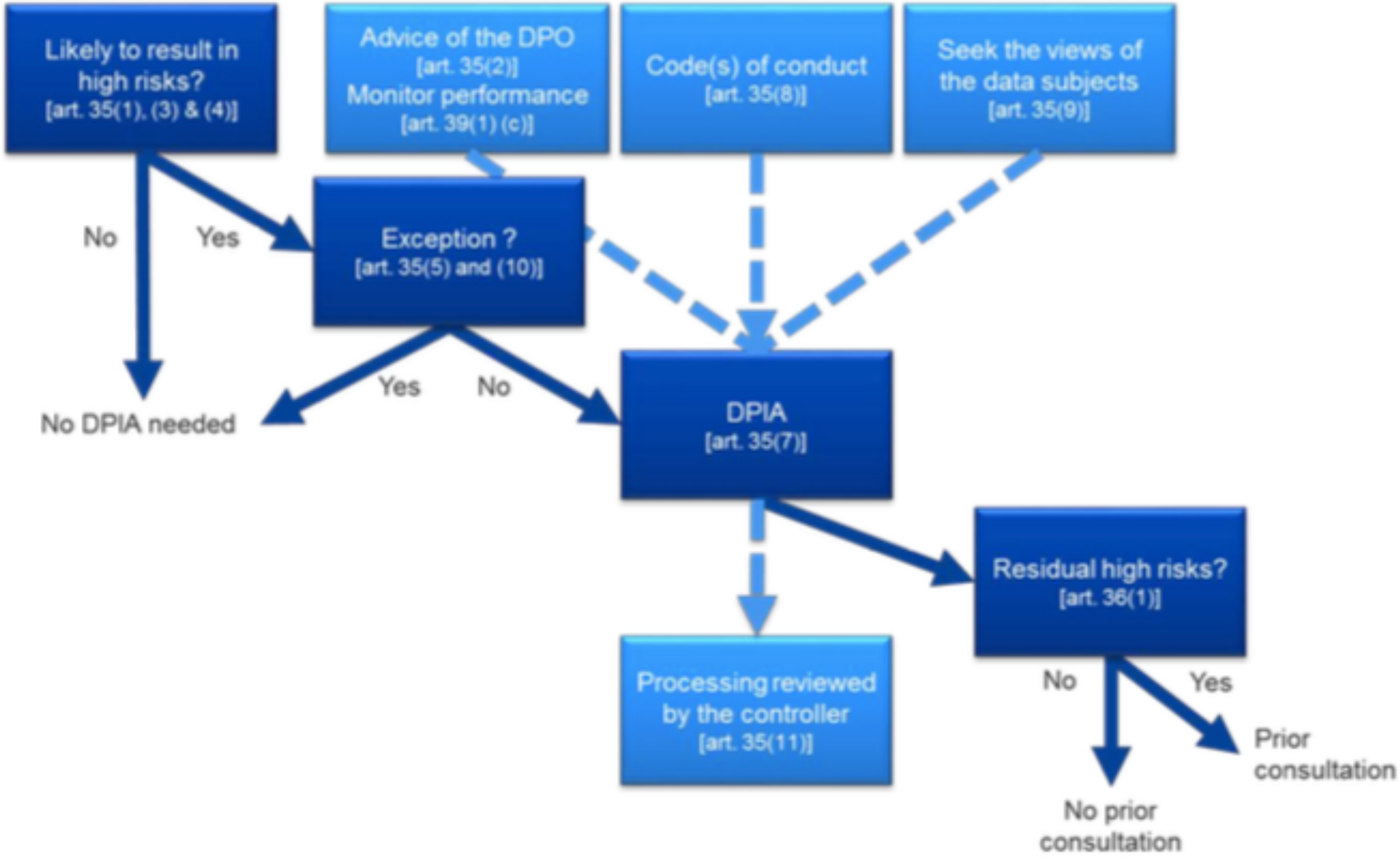
Figure 4 – Factors used to estimate the risks

PIA: an continuous process



Description of the envisaged processing
Assessment of the necessity and proportionality
Measures envisaged to demonstrate compliance
Assessment of the risks to the rights and freedoms
Measures envisaged to adress the risks
Documentation
Monitoring and review

When is a PIA necessary?


Likely to result in high risks? [art. 35(1), (3) & (4)]
Advice of the DPO [art. 35(2)] Monitor performance [art. 39(1) (c)]
Code(s) of conduct [art. 35(8)]
Seek the views of the data subjects [art. 35(9)]
No
Yes
Exception ? [art. 35(5) and (10)]
Yes
No
No DPIA needed
DPIA [art. 35(7)]
Residual high risks? [art. 36(1)]
Processing reviewed by the controller [art. 35(11)]
No
Yes
Prior consultation
No prior consultation

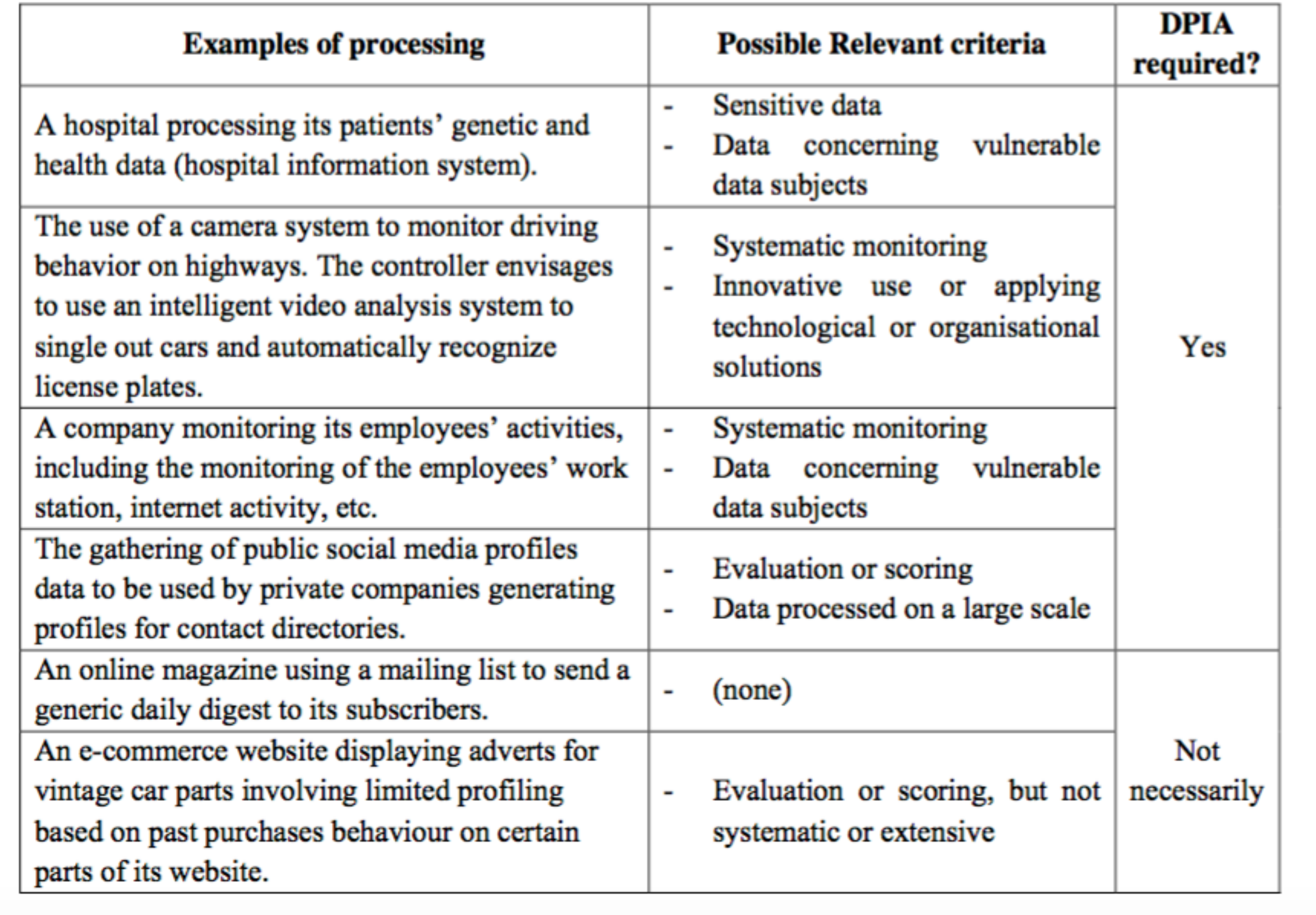
When is a PIA necessary?

the following criteria should be considered:

- Evaluation or scoring
- Automated-decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data
- Data processed on a large scale
- Datasets that have been matched or combined
- Data concerning vulnerable data subjects
- Innovative use or applying technological or organisational solutions
- Data transfer across borders outside the European Union
- When the processing in itself “prevents data subjects from exercising a right or using a service or a contract”
-

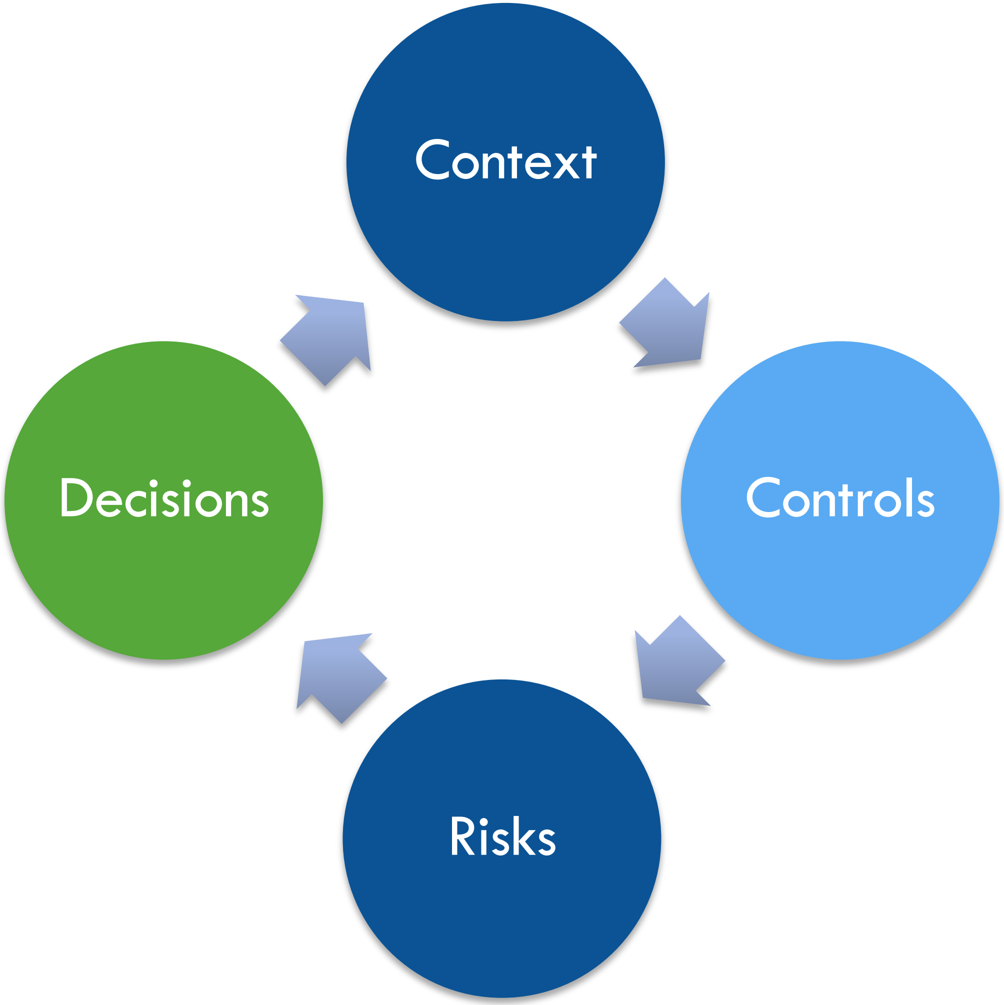
(see Article 29 guidelines- april 2017)

When is a PIA necessary?



Examples of processing	Possible Relevant criteria	DPIA required?
A hospital processing its patients' genetic and health data (hospital information system).	- Sensitive data - Data concerning vulnerable data subjects	Yes
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.	- Systematic monitoring - Innovative use or applying technological or organisational solutions	
A company monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.	- Systematic monitoring - Data concerning vulnerable data subjects	
The gathering of public social media profiles data to be used by private companies generating profiles for contact directories.	- Evaluation or scoring - Data processed on a large scale	
An online magazine using a mailing list to send a generic daily digest to its subscribers.	- (none)	Not necessarily
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on past purchases behaviour on certain parts of its website.	- Evaluation or scoring, but not systematic or extensive	

CNIL: Iterative process



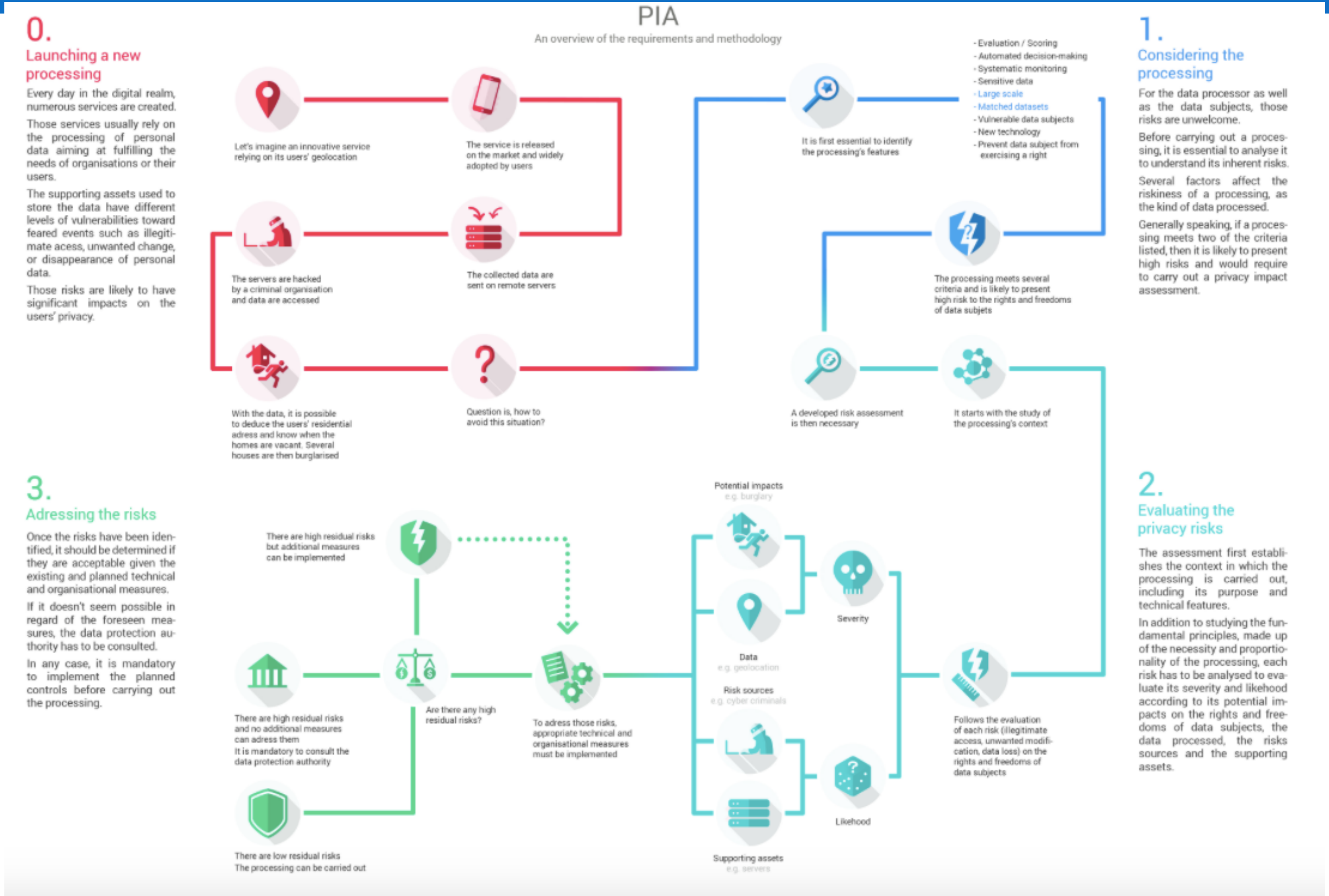
How to Perform a PIA?

1. **Considering the context (processing + control)**
   - What is application/service doing?
   - What data are you collecting/processing?
   - What are the measures that are considered?
   - How are the user rights implemented?

2. **Evaluating the Privacy Risks**
   - What are the risk sources, feared events, threats?
   - What is the severity, likehood of the feared events?

3. **Addressing the Risks**
   - How severe and probable are the risks?
   - How can they be addressed? What measures to implement?

How to Perform a PIA?



PIA

An overview of the requirements and methodology

0. Launching a new processing

Every day in the digital realm, numerous services are created.

Those services usually rely on the processing of personal data aiming at fulfilling the needs of organisations or their users.

The supporting assets used to store the data have different levels of vulnerabilities toward feared events such as illegitimate acess, unwanted change, or disappearance of personal data.

Those risks are likely to have significant impacts on the users' privacy.

Let's imagine an innovative service relying on its users' geolocation

The service is released on the market and widely adopted by users

The collected data are sent on remote servers

The servers are hacked by a criminal organisation and data are accessed

With the data, it is possible to deduce the users' residential adress and know when the homes are vacant. Several houses are then burglarised

Question is, how to avoid this situation?

1. Considering the processing

For the data processor as well as the data subjects, those risks are unwelcome.

Before carrying out a processing, it is essential to analyse it to understand its inherent risks.

Several factors affect the riskiness of a processing, as the kind of data processed.

Generally speaking, if a processing meets two of the criteria listed, then it is likely to present high risks and would require to carry out a privacy impact assessment.

It is first essential to identify the processing's features

- Evaluation / Scoring
- Automated decision-making
- Systematic monitoring
- Sensitive data
- Large scale
- Matched datasets
- Vulnerable data subjects
- New technology
- Prevent data subject from exercising a right

The processing meets several criteria and is likely to present high risk to the rights and freedoms of data subjets

A developed risk assessment is then necessary

It starts with the study of the processing's context

2. Evaluating the privacy risks

The assessment first establishes the context in which the processing is carried out, including its purpose and technical features.

In addition to studying the fundamental principles, made up of the necessity and proportionality of the processing, each risk has to be analysed to evaluate its severity and likehood according to its potential impacts on the rights and freedoms of data subjects, the data processed, the risks sources and the supporting assets.

Follows the evaluation of each risk (illegitimate access, unwanted modification, data loss) on the rights and freedoms of data subjects

3. Adressing the risks

Once the risks have been identified, it should be determined if they are acceptable given the existing and planned technical and organisational measures.

If it doesn't seem possible in regard of the foreseen measures, the data protection authority has to be consulted.

In any case, it is mandatory to implement the planned controls before carrying out the processing.

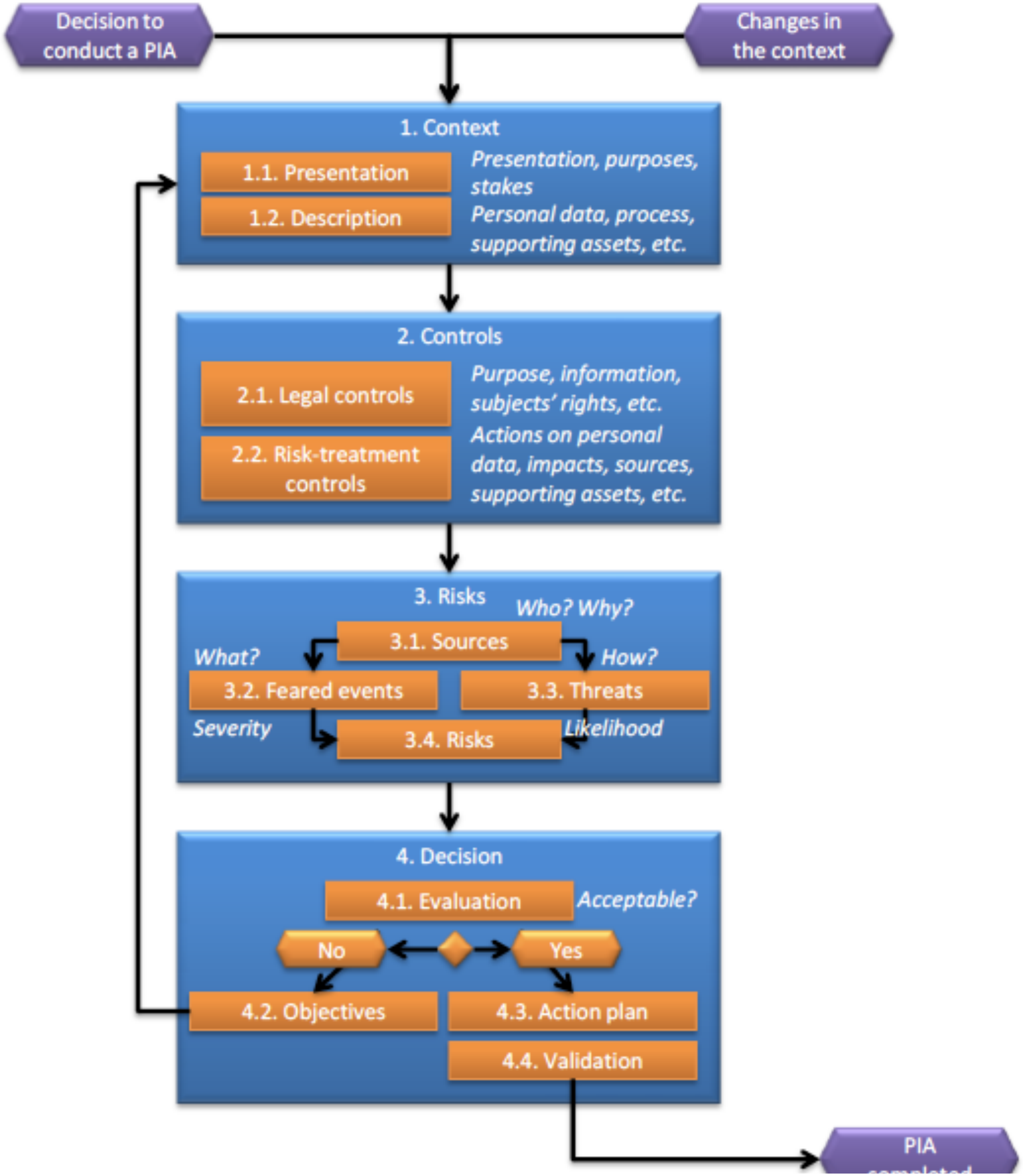
To adress those risks, appropriate technical and organisational measures must be implemented

Are there any high residual risks?

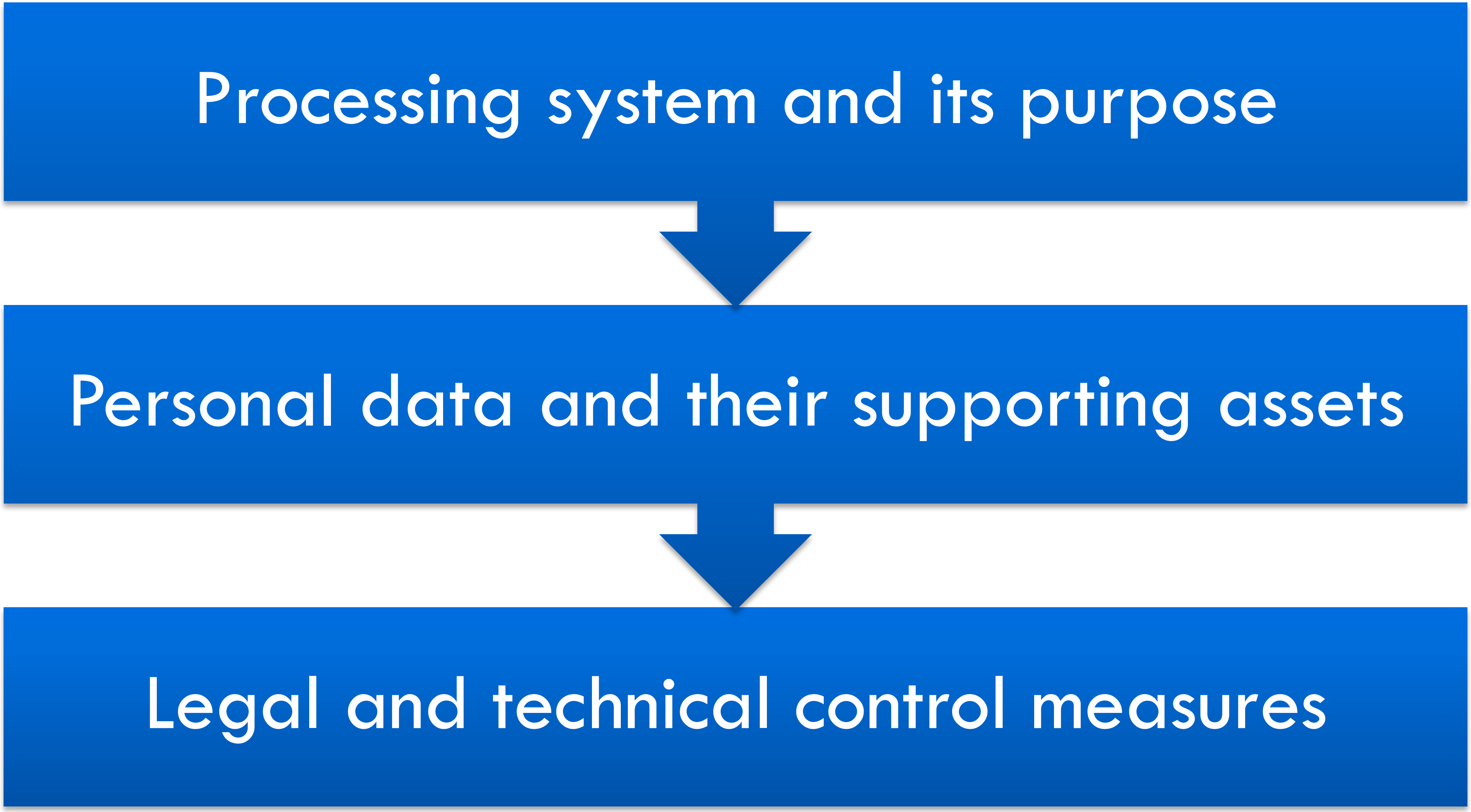
There are high residual risks but additional measures can be implemented

There are high residual risks and no additional measures can adress them
It is mandatory to consult the data protection authority

There are low residual risks
The processing can be carried out


Decision to conduct a PIA
Changes in the context
1. Context
1.1. Presentation
Presentation, purposes, stakes
1.2. Description
Personal data, process, supporting assets, etc.
2. Controls
2.1. Legal controls
Purpose, information, subjects' rights, etc.
2.2. Risk-treatment controls
Actions on personal data, impacts, sources, supporting assets, etc.
3. Risks
Who? Why?
3.1. Sources
What?
How?
3.2. Feared events
3.3. Threats
Severity
3.4. Risks
Likelihood
4. Decision
4.1. Evaluation
Acceptable?
No
Yes
4.2. Objectives
4.3. Action plan
4.4. Validation
PIA completed

1. Define Context and controls

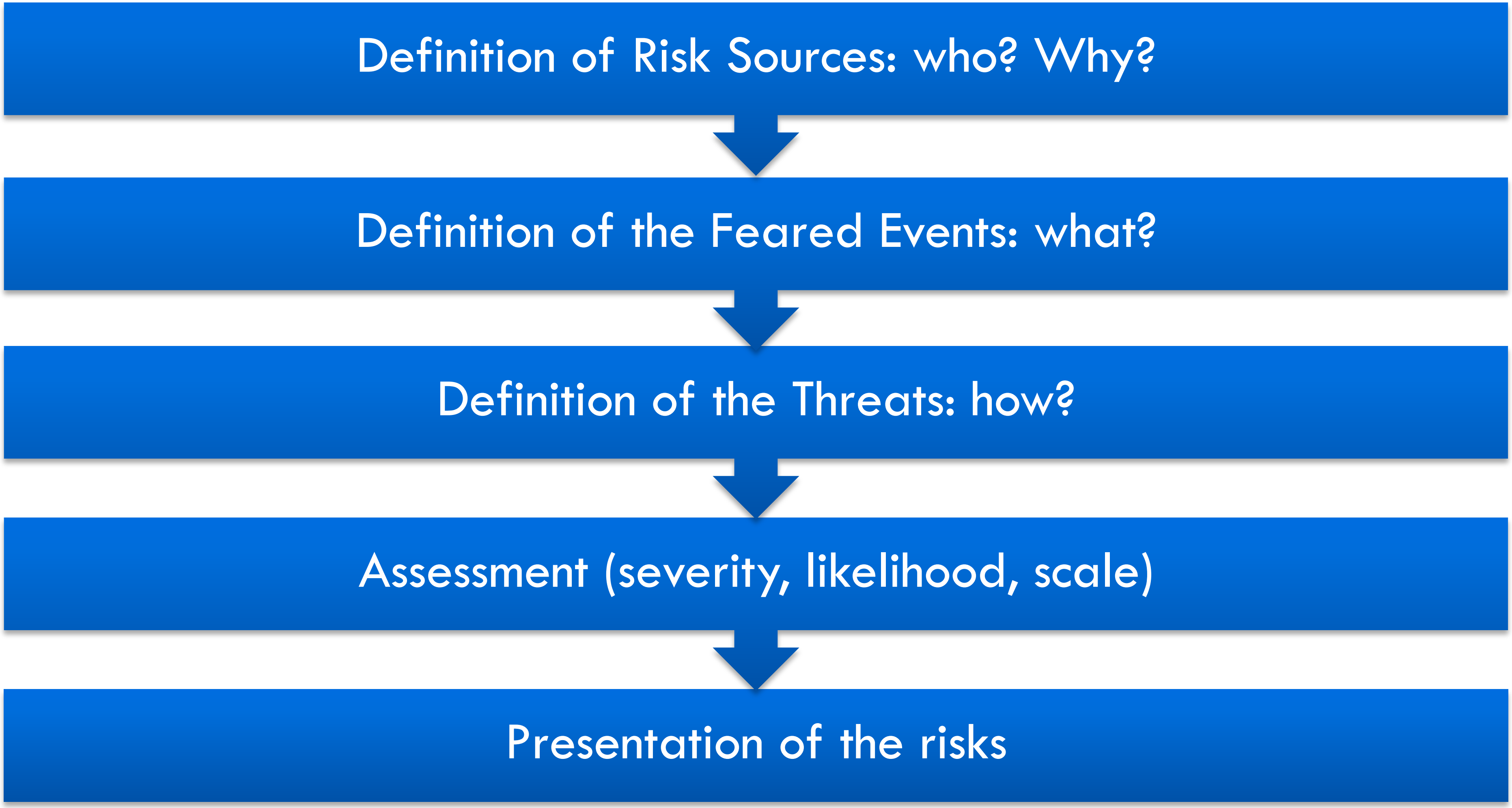


Processing system and its purpose

Personal data and their supporting assets

Legal and technical control measures

2. Perform Risk Assessment



Definition of Risk Sources: who? Why?

Definition of the Feared Events: what?

Definition of the Threats: how?

Assessment (severity, likelihood, scale)

Presentation of the risks

Risk Sources (some hints)

- □ Risk Sources related to the data controller (data controller itself, its employees, sub-contactors, etc.)
- □ Risk Sources related to the data subject (relatives, friends, neighbour, colleague, employer, bank, insurance company, etc.)
- □ Risk Sources related to the states (intelligence agencies, law enforcement agencies, administrations, etc.)
- □ Generic Risk Sources (advertisement industry, data brokers, hackers, robbers, blackmailers, etc.)

Risk Source capacities (important to evaluate risk likehood)

- Access to the supporting assets
- Resources (tools, computational power, expertise, etc.)
- Background knowledge (any auxiliary knowledge useful to breach the privacy of the subjects)

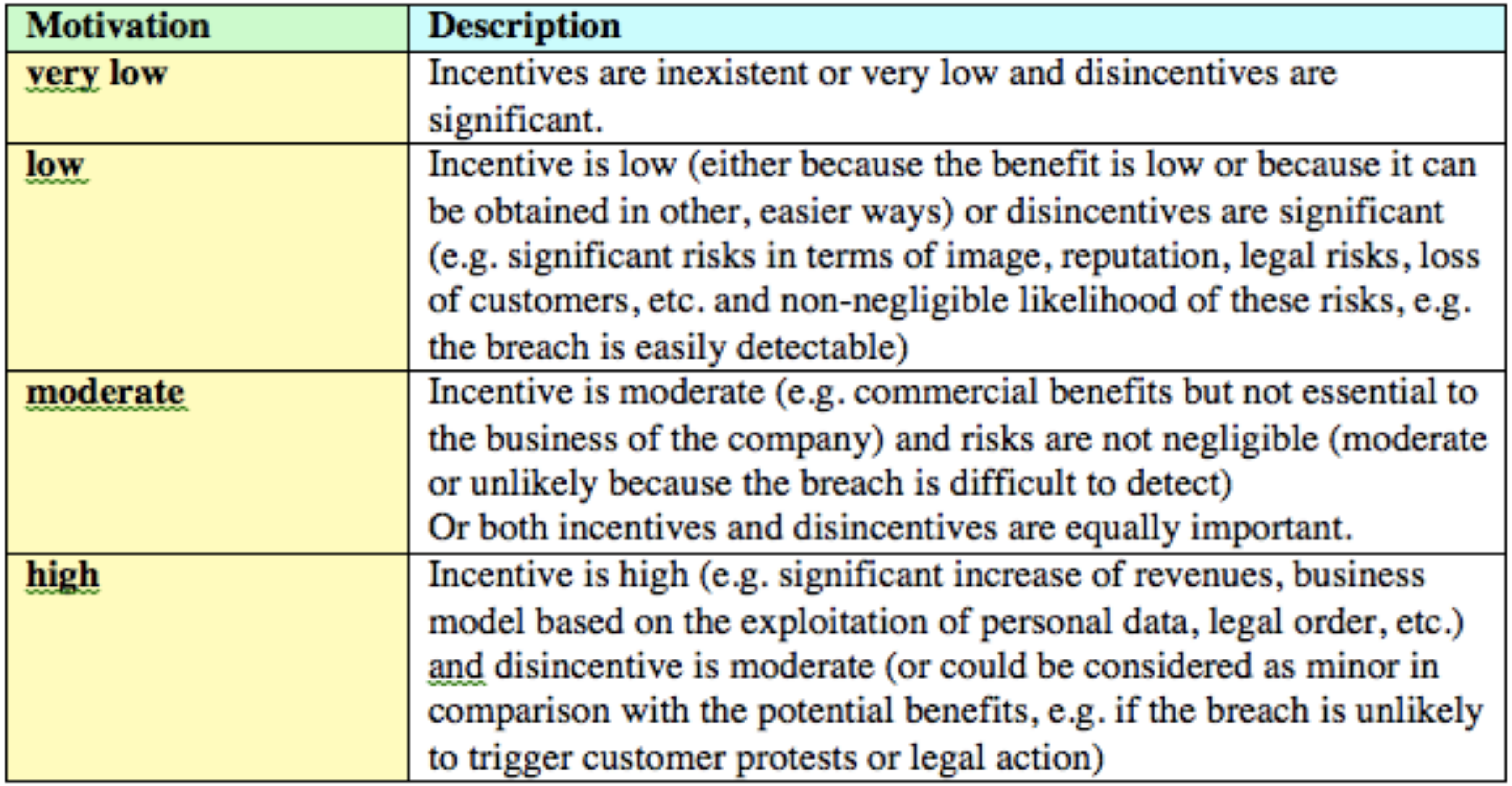
Feared Events

- Illegitimate Access to Data:
  - Anticipated collection/use of personal data: the Risk Source is “passive”, it only collects (or gets access to) the data that it is supposed to collect without trying to collect more data or perform any actions beyond the declared purpose.
  - Unanticipated use of personal data (secondary usage): the Risk Source is “active”, it might try to collect more data than expected or process collected data beyond the declared purpose.
  - Unanticipated disclosure of personal data to a third party. The Risk Source is “active” and might share the collected data with a third party.
- Unwanted Modification of personal data:
- Data disappearance:

Feared Events attributes (some hints)

- Motivation: characterizes the incentives (e.g. financial gains) of the Risk Source to perpetrate the Feared Event balanced with the potential disincentives (loss of trust, damage to reputation, etc.).
- Severity of Privacy Impacts: can be drawn from a catalogue of standard impacts (e.g. CNIL).
- List of associated Threats: different ways to bring about a Feared Event + likehood.
- Likelihood: probability that a user may be concerned by the Fear Event. The Likelihood of a Feared Event is derived from the Likelihoods and Scales of the associated Threats.

Motivation (important to evaluate likehood)

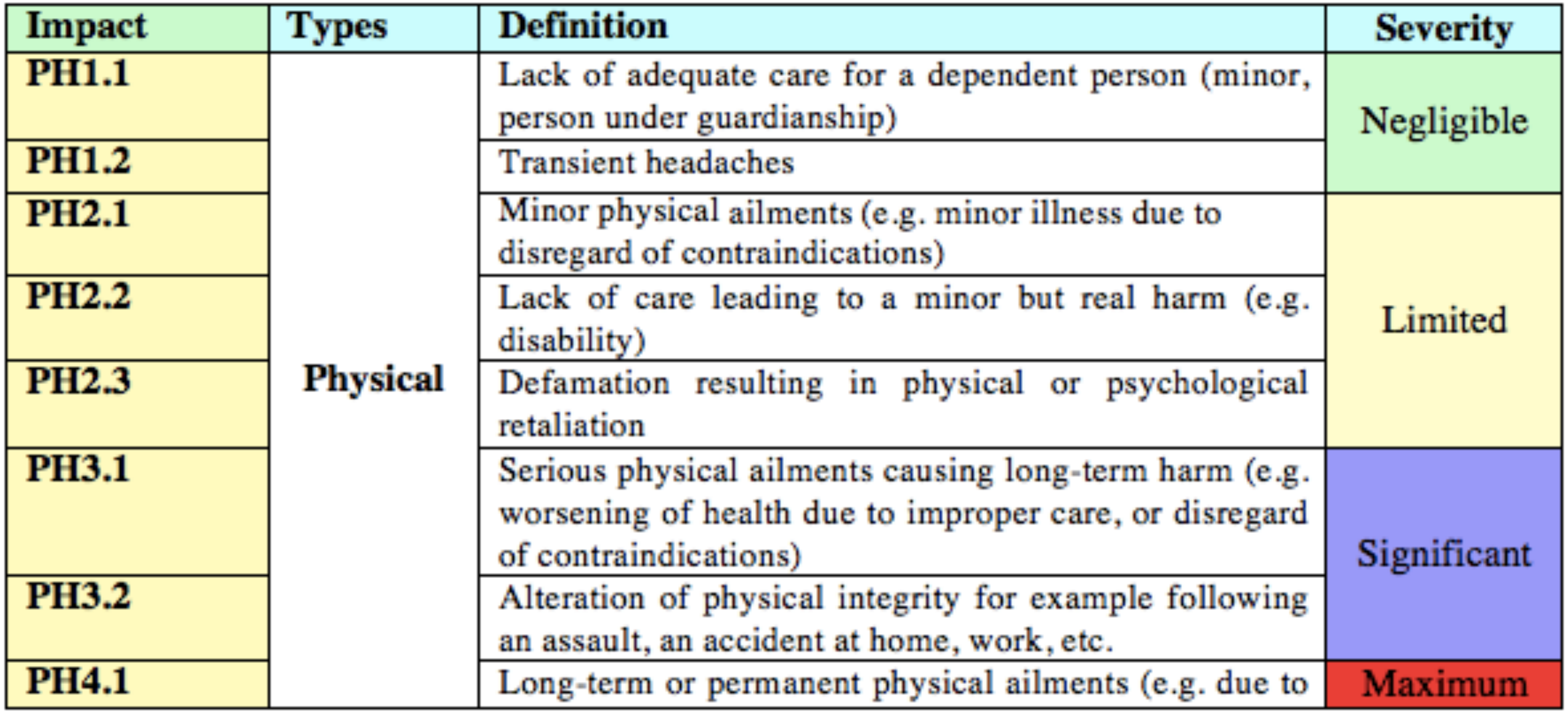


Motivation	Description
very low	Incentives are inexistent or very low and disincentives are significant.
low	Incentive is low (either because the benefit is low or because it can be obtained in other, easier ways) or disincentives are significant (e.g. significant risks in terms of image, reputation, legal risks, loss of customers, etc. and non-negligible likelihood of these risks, e.g. the breach is easily detectable)
moderate	Incentive is moderate (e.g. commercial benefits but not essential to the business of the company) and risks are not negligible (moderate or unlikely because the breach is difficult to detect) Or both incentives and disincentives are equally important.
high	Incentive is high (e.g. significant increase of revenues, business model based on the exploitation of personal data, legal order, etc.) and disincentive is moderate (or could be considered as minor in comparison with the potential benefits, e.g. if the breach is unlikely to trigger customer protests or legal action)

Privacy Impact (from CNIL)

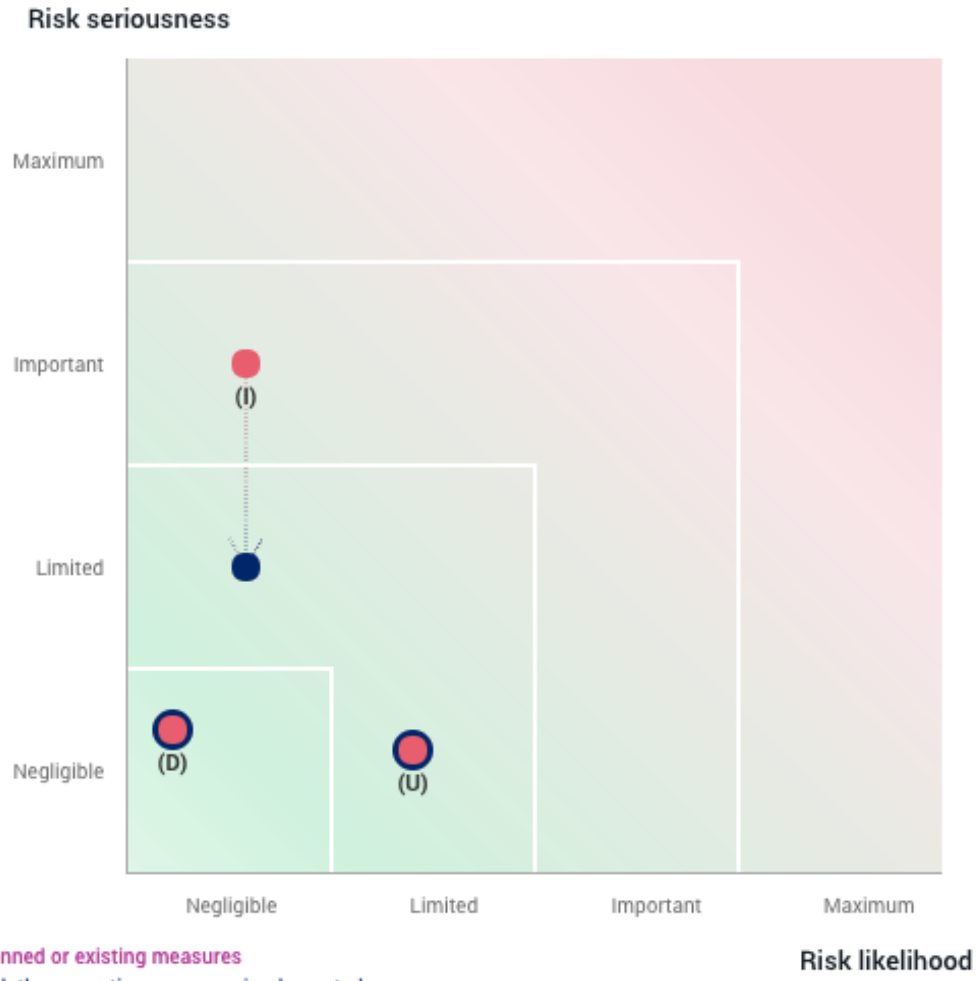
- Physical Impact
  - Ex: Permanent impairment of physical integrity
- Material
  - Ex: Blocked online services account (e.g. games, administration
- Moral
  - Ex: Feeling of invasion of privacy …

Privacy Impact: example…



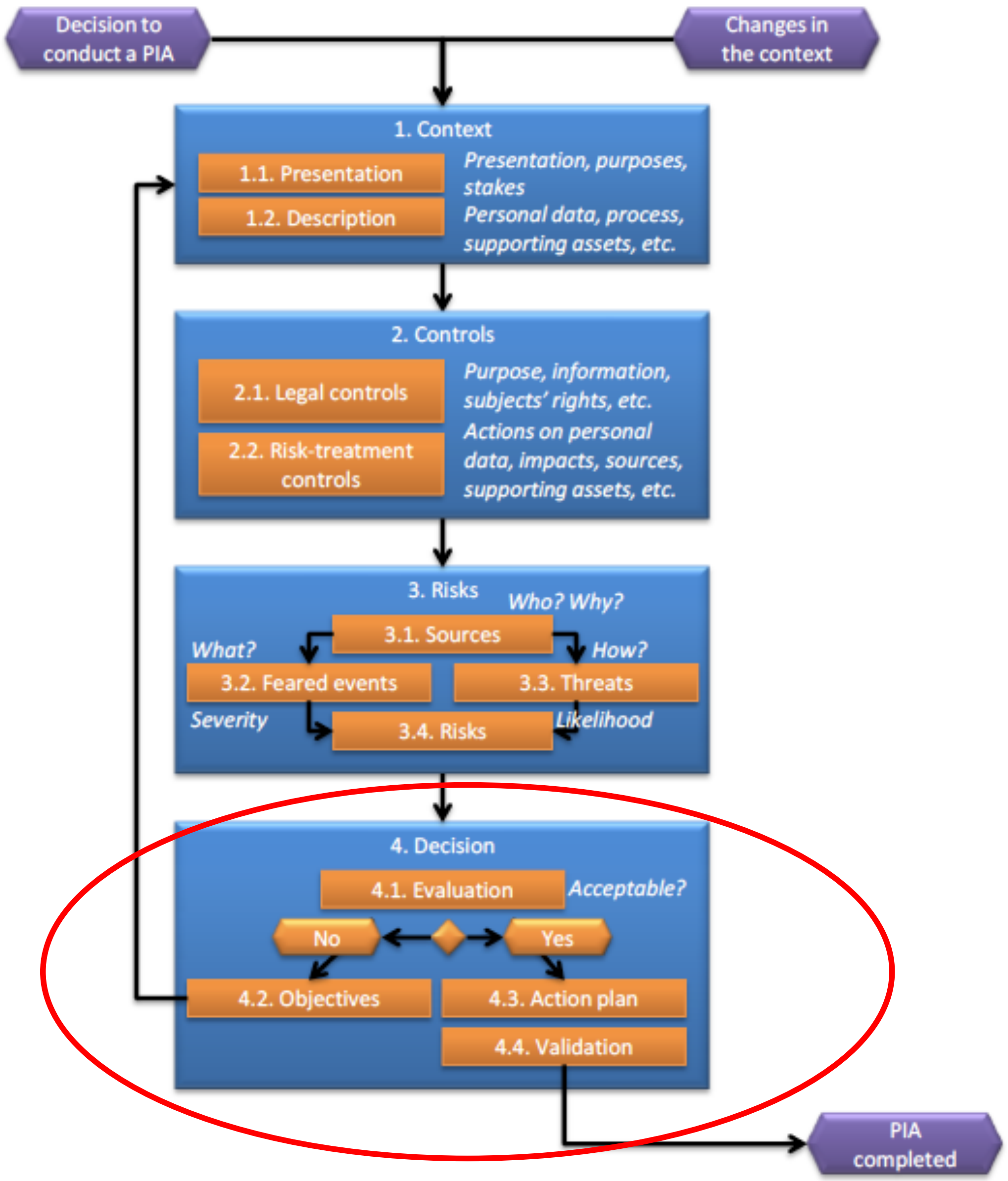
Impact	Types	Definition	Severity
PH1.1	Physical	Lack of adequate care for a dependent person (minor, person under guardianship)	Negligible
PH1.2		Transient headaches	
PH2.1		Minor physical ailments (e.g. minor illness due to disregard of contraindications)	Limited
PH2.2		Lack of care leading to a minor but real harm (e.g. disability)	
PH2.3		Defamation resulting in physical or psychological retaliation	
PH3.1		Serious physical ailments causing long-term harm (e.g. worsening of health due to improper care, or disregard of contraindications)	Significant
PH3.2		Alteration of physical integrity for example following an assault, an accident at home, work, etc.	
PH4.1		Long-term or permanent physical ailments (e.g. due to	Maximum

Presentation of the Risks



- Planned or existing measures
- With the corrective measures implemented
- (I)llegitimate access to data
- (U)nwanted modification of data
- (D)ata disappearence

3. Decision Phase

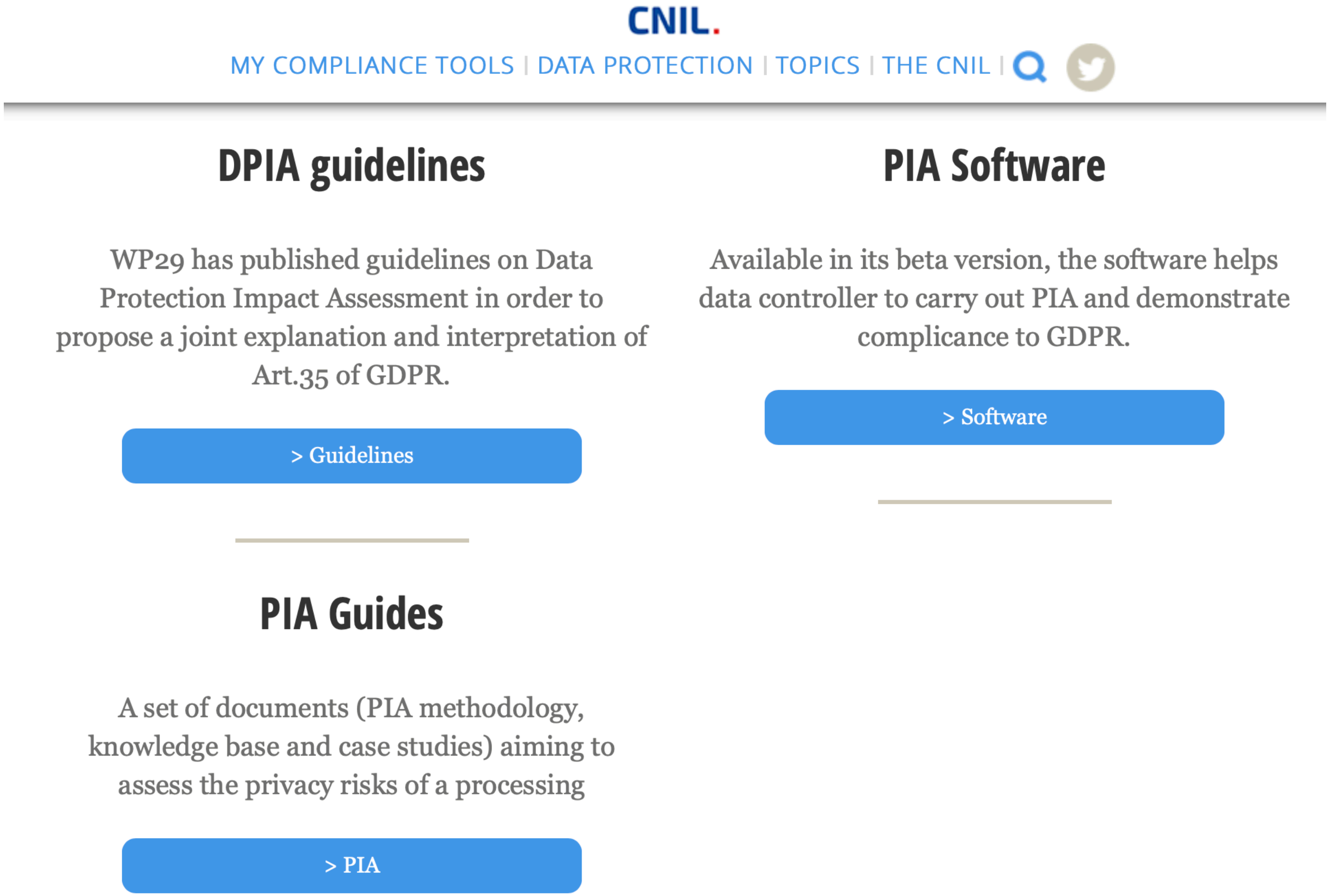


Address the Risks

- If some risks are too high, address them by providing some organizational or technical solutions.
  - Improve control
  - Use Anonymization/Encryption
  - Distribute storage
  - Drop some processing
  - Privacy-by-design
  - …
  - Go back to Step2:

More information?

https://www.cnil.fr/en/privacy-impact-assessment-pia



DPIA guidelines

WP29 has published guidelines on Data Protection Impact Assessment in order to propose a joint explanation and interpretation of Art.35 of GDPR.

> Guidelines

PIA Software

Available in its beta version, the software helps data controller to carry out PIA and demonstrate complicance to GDPR.

> Software

PIA Guides

A set of documents (PIA methodology, knowledge base and case studies) aiming to assess the privacy risks of a processing

> PIA

TP- The CNIL PIA tool

The CNIL guidelines (very useful)

- Methodology:
  - https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

- Tools:
  - https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf

The Cnil Tool:

- https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

Project

Case#1: Driving Skill Monitor

□You want to develop an app that would help users to monitor and analyze the driving quality by using the accelerometer (G-sensor) of their smartphone. This will help users determine if their driving is good or bad, helping them improving their driving skills.

- Collect name, location, speed, acceleration from gps, accelerator
- Generate a score.
- Provide advices to improve score.
- See for example: DrisSMo- Driving Skill Monotor
  - https://www.youtube.com/watch?v=vX3nVRZ8UAA

Project

Case#2: Fitness App

- An company want to deploy an App that monitor your physical activities to suggest advices on how to improve your health
  - Collect physical activities from gps + acceleration information (how long your walk, run, sleep,…)
  - Compute a fitness score and propose advices
  - Propose you to share the information on your favorate social network
  - See Google Fit app:
    - https://play.google.com/store/apps/details?id=com.google.android.apps.fitness

Project

Case#3: Sleep Monitoring App

- Sleep Time provides insight into your sleep patterns. By tracking your level of movement throughout the night, Sleep Time generates customized sleep data in easy-to-read charts.

- Azumio Sleep Time: http://www.azumio.com/s/sleeptime/index.html

Project

Case#4: Select your favorite app!

TousAntiCovid, Deliveroo, uber, Airbnb, AliceM,…

What to do:

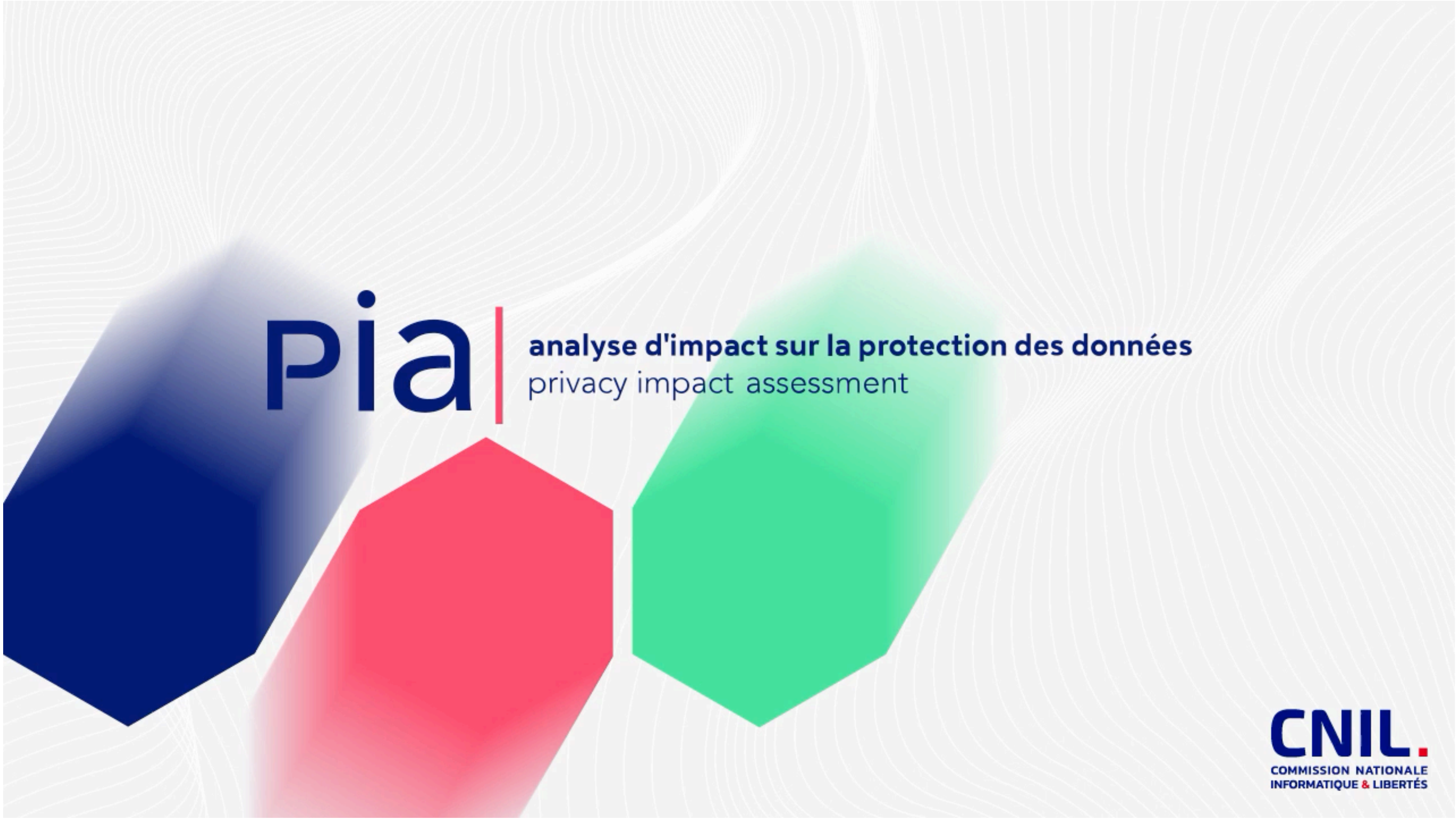
- 1. **Form a group of 4-5 students** (send me a email with list of the students today)

- 2. **Describe the App. (max 4 pages)**
  - Which data are collected, with which accuracy, when, how often?
  - Do you implement data minimization?
  - Where are they store store, how are they stored, who can get access to them? How are they processed? How are they deleted?
  - How do get users' consent?
  - How do you implement users' rights (right to access, modify, delete)?
  - How do you implement privacy-by-design?

What to do (2):

- 3. **Perform a PIA. using CNIL tool**
  - You are the editor and reviewer
  - I will be the validator.
- 4. **Make a Presentation (15-20 min.) on XX of your work**
- **5. Send me (claude.castelluccia@inria) before the presentation**
  - Your description of the app. (max 4 pages)
  - Your PIA (json file)
  - Your Class presentation (pdf).
- **6.You'll get a mark for the project**

CNIL PIA Tool Tutorial



pia

analyse d'impact sur la protection des données

privacy impact assessment

CNIL.

COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS