

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

There are high residual risks but additional measures can be implemented

* 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

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 likelihood according to its potential impacts on the rights and freedoms of data subjects, the data processed, the risks sources and the supporting assets..

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.

3.

Addressing 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.

lf 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.

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 access, unwanted change, or disappearance of personal data.

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

There are low residual risks   
The processing can be carried out

Are there any high residual risks?

Likelihood

Severity

It is first essential to identify the processing's features

PIA

An overview of the requirements and methodology

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

Potential impacts  
e.g. burglary

Data  
 e.g. geolocation

Risk sources  
 e.g. cyber criminals

Supporting assets  
 e.g. servers

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

It starts with the study of the processing's context

A developed risk assessment is then necessary

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

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

Question is, how to avoid this situation?

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

The collected data are sent on remote servers

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

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