

# Data Protection Impact Assessment

## in a nutshell

### What is it?

A Data Protection Impact Assessment (DPIA) is a prior written assessment of the impact of the planned processing operations on the protection of personal data. DPIAs provide a structured way of thinking about the risks posed to the people whose data you process. DPIAs also help you to comply with the requirement of data protection by design.

### Why is a DPIA needed?

- To understand and mitigate risks to people's rights
- To comply with a legal obligation (Art. 39 Regulation (EU) 2018/1725)

### When to do a DPIA?

Start preparing it when designing a new processing operation. Then review and update it regularly.



### Who gets involved?

- Top management (accountable)
- Business owner
- DPO
- IT department
- Processors

### When is it mandatory?

A DPIA is mandatory for data processing operations presenting **high risks to data subjects** such as when two of the following criteria apply:

1. Systematic evaluation/profiling
2. Automated decision making
3. Systematic monitoring
4. Sensitive data processing
5. Large scale processing
6. Match/combine datasets with different purposes
7. Vulnerable data subjects
8. New technologies
9. Preventing people from exercising their rights or entering into a service/contract

### What should a DPIA include?

- Description of the planned processing and its purposes
- Necessity and proportionality assessment
- Risk assessment to data subjects
- Measures to address the risks

### If in doubt, do a DPIA!

For more information:

- [EDPS video on DPIA](#)
- [EDPS Guidance Accountability on the ground part II](#)
- [EDPS decision on DPIA lists](#)

