What Triggers a Data Protection Impact Assessment?

Data Protection Impact Assessments, or DPIAs, are frequently required by the GDPR. They are risk-analysis exercises that balance the benefits of a specific processing operation involving personal data against the potential for harm to data subjects. DPIAs are designed to identify and mitigate risks and are a critical part of privacy by design.

Under the GDPR, DPIAs may be required:

- Prior to the first time any new business process involving personal data is completed (Rec. 90).
- Where a business process involving personal data has not undergone a DPIA in the past (Rec. 90).
- When the personal data being processed could pose a high risk to the data subjects if an incident were to occur (Rec. 84).
- When processing old data sets or personal data (Rec.90).
- When personal data, including IP addresses, are being used to make decisions regarding a data subject (Profiling) (Rec. 91).
- When public areas are being monitored on a large scale. (Rec. 91).
- When sensitive categories of data, criminal data, or national security data are being processed on a large scale (Rec. 91).*
- If a business process incorporates a new technology (Art. 35).
- If a business process involves automated decision making, "the ability to make decisions by technological means without human involvement" (Art. 35).
- When the processing of personal data involves the systematized processing of personal data. (Art. 35)
- When there is a change of the risk represented by processing operations (Art. 35).

Look for Supervisory Authorities to also provide lists of common forms of processing that explicitly will or will not trigger DPIAs.

*** The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.**

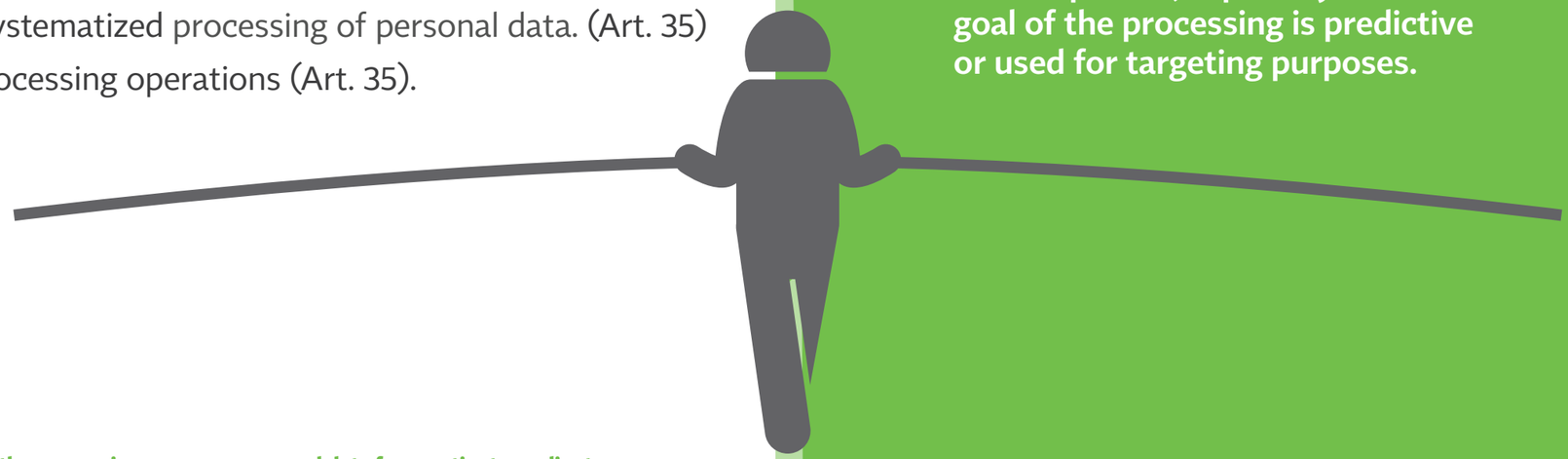
iapp

What makes data old?

When considering whether the age of the data you're processing would trigger a DPIA, consider the following questions: When was the data collected? What was the purpose of collection? Would the data subject expect their data to be processed now? Has the purpose of processing changed?

Profiling

Under the GDPR, profiling is defined as any automated evaluation of a natural person, especially when the goal of the processing is predictive or used for targeting purposes.



iapp.org