Lesson 6 | Data Protection Impact Assessments (DPIAs)

Updated 2020-09-21

Data protection impact assessments (DPIAs) are required by Article 35 of GDPR. It is up to the organization to determine when to do a DPIA as GDPR allows consideration based on the scope of processing and risk to data subjects.

A DPIA is an brief assessment of risk to data. They should be done when there are significant operational or technical changes made.

One area where GDPR calls out the potential need for a DPIA is in regard to the use of new technologies. As a best practice, erring on the side of fast, regular DPIAs in the use of new technologies is a great way to capture risks and mitigations.

GDPR does define what goes into a DPIA and it is similar to a broader risk assessment.

1. Description of the processing.
2. Justification of the processing in regards to the purpose.
3. Assessment of the risks to individuals.
4. Mitigations, typically security and technical controls, to minimize the risks from the processing.

DPIAs should be centrally stored and easily accessible for future review internally as well as by supervisory authorities.

DPIAs are a structured way to assess the risk to personal data and should be performed in a standardized way within your organization.