Data Protection Impact Assessment (DPIA) Template

trio

This template is designed to guide you through the Data Protection Impact Assessment (DPIA) process. It outlines the key steps involved and provides prompts to help you document your assessment.

Remember:

- Read this template alongside relevant DPIA guidance from the Information Commissioner's Office (ICO) (https://ico.org.uk/).
- The criteria for an acceptable DPIA are set out in European guidelines on DPIAs.
- Initiate a DPIA at the start of any major project involving personal data or significant changes to existing processes.
- Integrate the final outcomes of your DPIA back into your project plan.

Step-by-Step Guide

Step 1: Identify the Need for a DPIA
Briefly explain your project's goals and the type of data processing involved. Reference relevant documents like project proposals. Summarize why a DPIA is necessary based on your risk assessment.

Step 2: Describe the Processing

Detail the nature of data processing: collection, storage, usage, and deletion methods. Identify the data source(s). Specify if data will be shared and with whom. Consider using a flowchart to illustrate data flows.

Describe the scope of processing, including:

- Data types (including special categories or criminal offense data, if applicable)
- Amount and frequency of data collection
- Data retention period
- Number of individuals affected
- Geographical scope

Explain your relationship with the individuals whose data is processed. Assess the level of control individuals have over their data. Consider if individuals would expect their data to be used in this way. Identify if the data pertains to children or other vulnerable groups. Address any prior concerns regarding this type of processing or security flaws. Analyze the processing's novelty and the current technological landscape.
Account for any public concerns related to data processing. Mention relevant approved codes of conduct or certification schemes.

Step 3: Assess Necessity and Proportionality

Describe compliance and proportionality measures, including:

- Lawful basis for processing
- Alignment of processing with stated purposes
- Consideration of alternative methods to achieve the same outcome
- Measures to prevent function creep (mission drift)
- Data quality and minimization practices
- Information provided to individuals regarding their data rights
- Measures to support individuals' rights
- Procedures for ensuring processors comply
- Safeguards for international data transfers

Step 4: Identify and Assess Risks

Analyze potential risks to individuals' rights and freedoms arising from data processing. Include relevant compliance and corporate risks. Consider the following risk factors:

- Source of the risk
- Nature of potential impact on individuals (including associated compliance and corporate risks)
- Likelihood of harm (remote, possible, or probable)
- Severity of harm (minimal, significant, or severe)
- Overall risk level (low, medium, or high)

Step 5: Identify Measures to Reduce Risk

- Address risks identified as medium or high in Step 5.
- Propose additional measures to reduce or eliminate these risks.
- Evaluate the impact of each measure on the overall risk level.
- Document the residual risk level after implementing the proposed measures.
- Obtain approval for the proposed measures.

Step 6: Sign Off and Record Outcomes

Record the following:

- Measures approved by (with date)
- Integration of actions into the project plan (including deadlines and responsible parties)
- Residual risks approved by (with justification for accepting high residual risks, if applicable)
- DPO (Data Protection Officer) advice provided (including date)
- Summary of DPO advice
- Party accepting or overruling DPO advice (with justification for overruling)
- Any additional comments