# Data Protection Impact Assessment Guide

Version 2.0 - January 2025

Classification: INTERNAL

## 1. Introduction to DPIA

A Data Protection Impact Assessment (DPIA) is a process designed to identify and minimise data protection risks arising from a project, system, or process that involves personal data.

Under the UK GDPR, a DPIA is mandatory when processing is likely to result in a high risk to the rights and freedoms of individuals. This includes: systematic monitoring of publicly accessible areas, large-scale processing of special category data, and automated decision-making with legal effects.

Even when a DPIA is not legally required, the company policy is to conduct one for any new system or significant change that processes personal data, to demonstrate accountability and compliance with data protection principles.

## 2. When is a DPIA Required?

A DPIA must be conducted before the processing begins. It should be initiated at the planning stage of any project to allow findings to influence the design.

Mandatory DPIA triggers include: introduction of new technology for processing personal data, processing special categories of data on a large scale, systematic monitoring of employees, data sharing with new third parties, and cross-border data transfers.

The Data Protection Officer (DPO) must be consulted on all DPIAs. The DPO reviews the assessment for completeness, adequacy of risk mitigation measures, and compliance with the data protection policy.

If a DPIA identifies residual high risks that cannot be mitigated, the processing must not proceed without consultation with the Information Commissioner's Office (ICO) under Article 36 of the UK GDPR.

## 3. DPIA Process

Step 1 -- Describe the Processing: Document what personal data is collected, from whom, for what purpose, how it is stored, who has access, and how long it is retained. Include data flow diagrams where helpful.

Step 2 -- Assess Necessity and Proportionality: Evaluate whether the processing is necessary for the stated purpose and whether less intrusive alternatives exist. Document the lawful basis for processing.

Step 3 -- Identify and Assess Risks: Consider risks to individuals including: unauthorised access, data loss, inaccuracy, unfair processing, loss of control, and discrimination. Rate each risk by likelihood and severity.

Step 4 -- Identify Measures to Mitigate Risk: For each identified risk, document specific technical and organisational measures to reduce the risk to an acceptable level. Examples include encryption, access controls, pseudonymisation, and training.

Step 5 -- Record Outcomes: Complete the DPIA template (DP-001), recording all findings, decisions, and mitigations. The completed DPIA must be reviewed and signed by the project owner, the DPO, and the Information Asset Owner.

Step 6 -- Review and Update: DPIAs are living documents and must be reviewed when the processing changes, when new risks emerge, or at least annually. Material changes require a DPIA addendum rather than a completely new assessment.

## 4. DPIA Template Fields

The DPIA template (DP-001) contains the following sections: Project Overview, Data Items and Categories, Lawful Basis, Data Subjects, Data Flows, Retention Periods, Third-Party Sharing, International Transfers, Security Measures, Risk Assessment Matrix, Mitigation Measures, DPO Consultation Notes, and Sign-off.

Each section must be completed in full. Incomplete DPIAs will be returned by the DPO for revision. Average completion time for a standard DPIA is 4-6 hours; complex DPIAs may require 2-3 weeks.

The Risk Assessment Matrix uses a 5x5 grid (Likelihood x Impact), with risk levels colour-coded: Green (acceptable), Amber (requires mitigation), Red (requires senior management approval), and Black (must not proceed without ICO consultation).

## 5. Roles and Responsibilities

Project Owner: responsible for initiating the DPIA, providing accurate information about the processing, implementing approved mitigations, and maintaining the DPIA record throughout the project lifecycle.

Data Protection Officer: provides independent advice on the DPIA process, reviews completed assessments, escalates high-risk processing to the ICO where required, and maintains the central DPIA register.

Information Asset Owner: confirms the accuracy of data asset descriptions, approves the security measures proposed, and ensures ongoing compliance with DPIA conditions.

IT Security: advises on technical security measures, reviews proposed architectures for security adequacy, and validates that security controls are implemented as specified in the DPIA.

All completed DPIAs are stored in the central DPIA Register maintained by the DPO's office. The register is audited annually by Internal Audit.