Service Description
Privacy Impact Assessment (Comprehensive)

Scope

A Privacy Impact Assessment (PIA) is a structured process used to identify, analyse, and mitigate privacy risks that may arise from new or significantly changed projects, technologies, or business processes involving personal or sensitive information. According to the OAIC's PIA Guidelines, a PIA is "a systematic assessment of how a project or initiative might affect the privacy of individuals, and a plan to manage, minimise, or eliminate those risks before implementation."

PIAs are required or strongly recommended when initiatives introduce new systems or digital services that handle personal data, alter existing data flows or vendor relationships, or involve cross border transfers and automated decision making. By addressing these factors early, organisations can ensure that privacy is built into the design of their projects rather than applied as an afterthought.

The scope of a PIA is to provide a proactive governance mechanism that ensures new or changing projects handle personal information lawfully, ethically, and transparently. It combines the OAIC's regulatory expectations with the risk-based structure of the NIST Privacy Framework, embedding privacy by design principles into IT and business initiatives. Through this process, organisations can reduce privacy risks, enhance compliance, and strengthen trust and accountability.

A comprehensive PIA typically includes defining project objectives, mapping data flows, identifying legal and regulatory obligations, assessing privacy risks, reviewing security and governance controls, evaluating third party and cross border considerations, and recommending mitigation actions or control enhancements.

Approach

Delivered over five practical phases, the PIA service balances risk tolerance with regulatory concern and organisational requirements. Further context relating to the engagement can be found below:

Initiation & Planning

- Define project scope, stakeholders, and regulatory context
- Confirm trigger conditions for conducting a PIA.

Data Flow Mapping & Information Gathering

- Document data lifecycle – consent → collection → use → storage → sharing → disposal.
- Identify personal and sensitive data touchpoints.

Risk Analysis & Impact Evaluation

- Assess likelihood and severity of privacy impacts.
- Align risks with OAIC APPs, NIST PF categories, and organisational risk appetite.

Mitigation & Control Design

- Recommend safeguards (technical, procedural, contractual).
- Integrate privacy controls into IT system architecture and workflows.

Reporting & Endorsement

- Deliver a PIA Report summarising risks, mitigations, and residual exposure.
- Obtain sign-off from project sponsors and Privacy Officer prior to implementation

Value

- Regulatory Compliance: Demonstrates proactive alignment with OAIC expectations and global standards.
- Risk Prevention: Identifies and mitigates privacy issues before they become breaches or reputational events.
- Trust & Transparency: Builds confidence with customers, regulators, and partners.
- Design Assurance: Embeds privacy and security early, reducing rework and compliance cost later.
- Governance Integration: Provides audit-ready documentation for enterprise risk, compliance, and data-governance programs.

Benefits

These are the key advantages of undertaking this service offering.

- Ensures privacy controls are addressed before launch to support regulatory compliance.
- Improves the ability to provide timely and complete privacy evidence for audits and reviews.
- Reduces the likelihood of privacy or consent breaches through stronger controls and governance.
- Minimises project rework and delays caused by privacy issues, improving delivery confidence.
- Enhances stakeholder trust and organisational privacy maturity through demonstrable assurance.

Outputs

- Privacy Impact Assessment Report – Comprehensive record of privacy risks, mitigations, and sign-off status.
- Data Flow Diagrams - Visual representation of personal-information handling, including - systems, data types, and transfer methods.
- Risk Register & Mitigation Plan - Prioritised list of privacy issues with residual risk ratings.
- Compliance Mapping Matrix - Alignment with APPs, NIST PF, ISO 27701 controls.
- Executive Summary / Board Brief - Key findings, governance obligations, and recommended actions.
- Privacy-by-Design Checklist - To embed controls into system architecture and SDLC.

Genesys DATA

Genesys Data stands with you to transform how to measure, approach and harness the power of your data, offering a portfolio of services that address the complexities of – getting data right! By integrating cutting-edge AI data-discovery techniques, advancing maturity modelling, and offering Data, Privacy and Security by Design, you'll be able to demonstrate appropriate duty-of-care, exceed privacy obligations, effectively gain control of data and understand how to become more cyber resilient and AI ready!

Learn more at www.genesysdata.com.au