Genesys DATA

Service Description

Data Privacy Assessment

Scope

A Data Privacy Assessment (DPA) is a structured evaluation of how an organisation collects, uses, stores, shares, and protects personal information, ensuring that its practices align with privacy laws, ethical standards, and its overall risk appetite.

Conducted in line with the Office of the Australian Information Commissioner (OAIC) and the Australian Privacy Principles (APPs), a DPA focuses on transparency, security, and accountability, with particular emphasis on APP 1 (management of personal information), APP 6 (use and disclosure), APP 11 (security of personal information), and APPs 12/13 (access and correction).

This process is further strengthened by the NIST Privacy Framework, which introduces a structured, risk-based approach that integrates privacy governance with cybersecurity and business resilience. Using the core functions Identify, Govern, Control, Communicate, and Protect, the assessment helps organisations operationalise privacy as part of their broader data protection strategy.

The scope of a Data Privacy Assessment includes mapping personal data flows across systems, applications, vendors, and APIs to reveal how data moves and where risks may arise. It reviews privacy policies, notices, consent mechanisms, and governance structures, including third-party and contractual obligations. Technical and procedural controls are validated for effectiveness such as access management, encryption, logging, and data minimisation, while ensuring alignment between privacy and cybersecurity programs. The assessment also examines data lifecycle and retention practices to confirm that collection, storage, and destruction comply with legal and ethical standards. Finally, it evaluates the role of technology and automation, including AI-driven data discovery, Data Security Posture Management (DSPM) tools, and privacy-by-design integrations to ensure proactive, continuous privacy risk management across IT and business functions.

Approach

Initiation

Establishes the scope, regulatory boundaries, and stakeholders to align privacy and risk objectives with business strategy and compliance requirements, and factors:

- Regulatory boundaries, target systems, and key stakeholders.
- Aligns objectives with business strategy, risk appetite, and compliance requirements.

Data Discovery & Mapping

This phase includes the:

- Inventory of personal and sensitive information across systems
- Documents processing activities, data owners, and data flows.

Assessment & Gap Analysis

This phase includes the:

- Evaluation of policies, controls, and processes against OAIC APPs and NIST Privacy Framework categories.
- Identification of gaps, risks, and control deficiencies; rated them by likelihood and impact.

Validation & Stakeholder Review

This phase includes the:

- Review of findings with Privacy Officers, CISOs, and Data Governance teams / Stakeholders.
- Validation, ownership and the prioritisation of remediation activities.

Reporting & Roadmap

This phase produces:

- A Privacy Risk Register, Maturity Scorecard, and detailed improvement roadmap.
- Recommended automation or platform solutions (e.g. DPSM tooling and Archiving strategies)

Value

This engagement intends to provide and or address:

- Regulatory Assurance: Demonstrates compliance with OAIC and global privacy standards.
- Operational Clarity: Provides a clear, data-driven view of where personal data lives and how it's managed.
- Trust & Reputation: Reinforces brand integrity through demonstrable privacy accountability.
- Risk Reduction: Reduces likelihood and impact of privacy breaches and regulatory penalties.
- Business Enablement: Enables confident data sharing, analytics, and AI adoption under a privacy-by-design model.

Benefits

These are the key advantages of undertaking this service offering:

- Reduces the time and effort required to produce privacy evidence, enabling faster and more efficient responses.

- Strengthens data-protection posture by improving the design and operation of privacy controls.
- Delivers clear visibility of personal-data flows across systems, supporting accurate reporting and informed decision-making.
- Lowers the occurrence of privacy-related alerts and breaches through stronger controls and governance alignment.
- Enhances organisational privacy maturity, embedding accountability and fostering continuous improvement.

Outputs

The following tangible outputs are produced as part of this engagement:

- Privacy Risk Assessment Report – detailed findings, risk ratings, and control recommendations.
- Data Flow & Processing Map – visual diagram of data lifecycle, storage, and transfer paths.
- Regulatory Compliance Matrix – mapping against OAIC APPs, NIST PF, and relevant sectoral frameworks.
- Privacy Maturity Scorecard – baseline and target maturity levels.
- Improvement Roadmap – prioritised actions, responsible owners, and timeframes.
- Executive Summary – board-ready overview of privacy posture, key exposures, and benefits achieved.