THE DATA PRIVACY LAWYER

Privacy Program Documentation

THE DATA PRIVACY LAWYER
info@thedataprivacylawyer.com

Building and maintaining a strong privacy program requires more than a website Privacy Policy and a consent form. Organizations are expected to have a complete set of documented policies, procedures, and records that demonstrate accountability and compliance with privacy regulations.

This guide provides an overview of the core documentation typically expected under major privacy laws and frameworks. While regulations may vary by jurisdiction, the documents below represent best practices for organizations that want to build trust, meet compliance obligations, and be prepared for audits or regulatory inquiries.

Core Documentation:

Personal Data Protection Policy
Sets the overall strategy and governance framework for protecting personal data across the organization.

Privacy Notice
Explains how personal information is collected, used, shared, and protected. Typically made available on websites or at the point of data collection.

Employee Privacy Notice
Outlines how employee and applicant data is used, including sensitive categories such as health or benefits information.

Data Retention Policy
Defines how long personal data is kept, aligned with legal, contractual, or business requirements, and how it will be securely disposed of.

Data Retention Schedule
Lists categories of data and the corresponding retention periods.

Consent Management Form or Record
Captures when and how individuals gave consent, and how that consent can be withdrawn.

Parental Consent Form
Used when processing children's data, where parental or guardian authorization is required.

Data Protection Impact Assessment (DPIA) Register
Maintains records of risk assessments conducted on higher-risk processing activities.

Vendor / Third-Party Data Processing Agreement
Defines privacy and security obligations between your organization and external vendors who process data on your behalf.

Data Breach Response and Notification Procedure
Outlines the steps to detect, investigate, and respond to data incidents, including when notifications are required.

Data Breach Register
A log documenting incidents, outcomes, and corrective actions taken.

Notification Templates
- To regulators or authorities (if required under applicable laws).
- To affected individuals, explaining the incident, risks, and protective steps.

Data Protection Officer (DPO) Role Description
Defines responsibilities if a DPO or privacy lead is designated.

Record of Processing Activities (RoPA)
Comprehensive documentation of processing activities, often required for larger organizations or those handling higher-risk data.

Data Transfer Agreements or Clauses
For organizations moving data across borders, to ensure protection when data leaves its original jurisdiction.

Privacy program documentation is not a one-time task: it is a living framework that must evolve with regulatory changes, business growth, and new technologies. By keeping records up to date, your organization demonstrates accountability and builds trust with customers, employees, and partners.