# GLOSSARY

KEY PRIVACY PROGRAM MANAGEMENT
TERMS, LAWS, STANDARDS …

# CONTENTS

## Accountability

The implementation of appropriate technical and organisational measures to ensure and be able to demonstrate that the handling of personal data is performed in accordance with relevant law, an idea codified in the EU General Data Protection Regulation and other frameworks, including APEC's Cross Border Privacy Rules. Traditionally, accountability has been a fair information practices principle, that due diligence and reasonable steps will be undertaken to ensure that personal information will be protected and handled consistently with relevant law and other fair use principles.

## Active Scanning Tools

DLP network, storage, scans and privacy tools can be used to identify security and privacy risks to personal information. They can also be used to monitor for compliance with internal policies and procedures, and block e-mail or file transfers based on the data category and definitions.

## American Institute of Certified Public Accountants (AICPA)

A U.S. professional organization of certified public accountants and co-creator of the WebTrust seal program (now managed by CPA Canada), through which accountants can become certified to conduct privacy evaluations

Associated term(s): Canadian Institute of Chartered Accountants, Seal Programs, WebTrust

## Anonymization

The process in which individually identifiable data is altered in such a way that it no longer can be related back to a given individual. Among many techniques, there are three primary ways that data is anonymized. Suppression is the most basic version of anonymization and it simply removes some identifying values from data to reduce its identifiability. Generalization takes specific identifying values and makes them broader, such as changing a specific age (18) to an age range (18-24). Noise addition takes identifying values from a given data set and switches them with identifying values from another individual in that data set. Note that all of these processes will not guarantee that data is no longer identifiable and have to be performed in such a way that does not harm the usability of the data.

Associated law(s):Anonymous Data, De-Identification, Mircodata Sets, Re-identification

## APEC Framework

The APEC Framework, published by the Asia-Pacific Economic Cooperation, is a framework to protect privacy within and beyond economies and to enable regional transfers of personal information benefits consumers, businesses, and governments. This framework is used as a basis for the APEC Cross-Border Privacy Rules (CBPR) System.

## APEC Privacy Principles

A set of non-binding principles adopted by the Asia-Pacific Economic Cooperative (APEC) that mirror the OECD Fair Information Privacy Practices. Though based on OECD Guidelines, they seek to

promote electronic commerce throughout the Asia-Pacific region by balancing information privacy with business needs.

## Assess

The first of four phases of the privacy operational life cycle; provides the steps, checklists and processes necessary to assess any gaps in a privacy program as compared to industry best practices, corporate privacy policies, applicable privacy laws, and objective-based privacy program frameworks.

Associated term(s): Privacy Operational Life Cycle; Protect; Sustain; Respond

## Audit Life Cycle

High-level, five-phase audit approach. The steps include: Audit Planning; Audit Preparation; Conducting the Audit; Reporting; and Follow-up.

## Australian Privacy Principles (APPs)

The Australian Privacy Principles (APPs) provide well-developed and current examples of generic privacy principles implemented through national law.

## Behavioral Advertising (OBA)

Advertising that is targeted at individuals based on the observation of their behaviour over time. Most often done via automated processing of personal data, or profiling, the General Data Protection Regulation requires that data subjects be able to opt-out of any automated processing, to be informed of the logic involved in any automatic personal data processing and, at least when based on profiling, be informed of the consequences of such processing. If cookies are used to store or access information for the purposes of behavioral advertising, the ePrivacy Directive requires that data subjects provide consent for the placement of such cookies, after having been provided with clear and comprehensive information.

Associated term(s): Online Behavioral Advertising, Behavioral Targeting, Contextual Advertising, Demographic Advertising, Premium Advertising, Psychographic Advertising, Remnant Advertising

## Binding Corporate Rules (BCR)

Binding Corporate Rules (BCRs) are an appropriate safeguard allowed by the General Data Protection Regulation to facilitate cross-border transfers of personal data between the various entities of a corporate group worldwide. They do so by ensuring that the same high level of protection of personal data is complied with by all members of the organizational group by means of a single set of binding and enforceable rules. BCRs compel organizations to be able to demonstrate their compliance with all aspects of applicable data protection legislation and are approved by a member state data protection authority. To date, relatively few organizations have had BCRs approved.

## Bureau of Competition

The United States' Federal Trade Commission's Bureau of Competition enforces the nation's antitrust laws, which form the foundation of our free market economy. The antitrust laws promote the interests of consumers; they support unfettered markets and result in lower prices and more choices.

Associated term(s): Bureau of Consumer Protection; Bureau of Economics

## Bureau of Consumer Protection

The United States' Federal Trade Commission's Bureau of Consumer Protection stops unfair, deceptive and fraudulent business practices by collecting complaints and conducting investigations, suing companies and people that break the law, developing rules to maintain a fair marketplace, and educating consumers and businesses about their rights and responsibilities.

Associated term(s): Bureau of Competition; Bureau of Economics

## Bureau of Economics

The United States' Federal Trade Commission's Bureau of Economics helps the FTC evaluate the economic impact of its actions by providing economic analysis for competition and consumer protection investigations and rulemakings, and analyzing the economic impact of government regulations on businesses and consumers.

Associated term(s): Bureau of Competition; Bureau of Consumer Protection

## Business case

The starting point for assessing the needs of the privacy organization, it defines the individual program needs and the ways to meet specific business goals, such as compliance with privacy laws or regulations, industry frameworks, customer requirements and other considerations.

## Business Continuity and Disaster Recovery Plan (BCDR)

A risk mitigation plan designed to prepare an organization for crises and to ensure critical business functions continue. The focus is to recover from a disaster when disruptions of any size are encountered.

## Business Continuity Plan (BCP)

The business continuity plan is typically drafted and maintained by key stakeholders, spelling out departmental responsibilities and actions teams must take before, during and after an event in order to help operations run smoothly. Situations covered in a BCP often include fire, flood, natural disasters (tornadoes and hurricanes), and terrorist attack.

## California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States.

## Canadian Institute of Chartered Accountants (CICA)

The Canadian Institute of Chartered Accountants (CICA), in partnership with the provincial and territorial institutes, is responsible for the functions that are critical to the success of the Canadian CA profession. CICA, pursuant to the 2006 Protocol, is entrusted with the responsibility for providing strategic leadership, co-ordination of common critical functions of strategic planning, protection of the public and ethics, education and qualification, standard setting and communications.

AICPA & CICA created WebTrust, now managed by CPA Canada, through which accountants can become certified to conduct privacy evaluations

Associated terms: AICPA, Webtrust

## The Canadian Standards Association (CSA)

The CSA's ten privacy principles are based on the OECD Guidelines and serve as the basis of Canada's PIPEDA.

Associated law(s): PIPEDA

## Centralized governance

Privacy governance model that leaves one team or person responsible for privacy-related affairs; all other persons or organizations will flow through this point.

## Children's Online Privacy Protection Act (COPPA) of 1998

A U.S. federal law that applies to the operators of commercial websites and online services that are directed to children under the age of 13. It also applies to general audience websites and online services that have actual knowledge that they are collecting personal information from children under the age of 13. COPPA requires these website operators: to post a privacy notice on the homepage of the website; provide notice about collection practices to parents; obtain verifiable parental consent before collecting personal information from children; give parents a choice as to whether their child's personal information will be disclosed to third parties; provide parents access and the opportunity to delete the child's personal information and opt out of future collection or use of the information, and maintain the confidentiality, security and integrity of personal information collected from children.

## Choice

In the context of consent, choice refers to the idea that consent must be freely given and that data subjects must have a genuine choice as to whether to provide personal data or not. If there is no true choice it is unlikely the consent will be deemed valid under the General Data Protection Regulation.

Associated term(s): Consent

See Consent

## CIA Triad

Also known as information security triad; three common information security principles from the 1960s:  Confidentiality, integrity, availability.

Associated term(s): Information Security Triad

## COBIT 2019

ISACA developed COBIT 2019 framework to guide to the governance and management of information systems for large organizations.

## Collection Limitation

A fair information practices principle, it is the principle stating there should be limits to the collection of personal data, that any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

## Consent

This privacy requirement is one of the fair information practices. Individuals must be able to prevent the collection of their personal data, unless the disclosure is required by law. If an individual has choice about the use or disclosure of his or her information, consent is the individual's way of giving permission for the use or disclosure. Consent may be affirmative; i.e., opt-in; or implied; i.e., the individual didn’t opt out.

(1) Affirmative/Explicit Consent: A requirement that an individual ""signifies"" his or her agreement with a data controller by some active communication between the parties.

(2) Implicit Consent: Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

Associated term(s): Choice

See Choice

## Consumer Reporting Agency (CRAs)

Any person or entity that complies or evaluates personal information for the purpose of furnishing consumer reports to third parties for a fee.

Associated term(s): Credit Reporting Agency

## Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM)

That act is a law that establishes the rules for commercial email and commercial messages, gives recipients the right to have a business stop emailing them, and outlines the penalties incurred for those who violate the law.

## Current baseline

“As-is” data privacy requirements; the current environment and any protections, policies, and procedures currently deployed.

## Cyber liability insurance

Relatively new form of insurance protection that fills gaps typically not covered by General Commercial Liability plans. Cyber liability insurance may cover many breach-related expenses, including forensic investigations, outside counsel fees, crisis management services, public relations experts, breach notification, and call center costs.

## Data Breach

The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a data collector. Breaches do not include good faith acquisitions of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector—provided the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

Associated term(s): Breach, Privacy Breach (Canadian)

## Data Controller

The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by EU or member state law, the controller or the specific criteria for its nomination may be provided for by EU or member state law.

Associated term(s): Data Processor

## Data Inventory

Also known as a record of authority, identifies personal data as it moves across various systems and thus how data is shared and organized, and its location. That data is then categorized by subject area, which identifies inconsistent data versions, enabling identification and mitigation of data disparities.

## Data Life Cycle Management

Also known as Information Life Cycle Management (ILM) or data governance, DLM is a policy-based approach to managing the flow of information through a life cycle from creation to final disposition. DLM provides a holistic approach to the processes, roles, controls and measures necessary to

organize and maintain data, and has 11 elements: Enterprise objectives; minimalism; simplicity of procedure and effective training; adequacy of infrastructure; information security; authenticity and accuracy of one's own records; retrievability; distribution controls; auditability; consistency of policies; and enforcement.

Acronym(s): DLM; ILM

Associated term(s): Information Life Cycle Management

## Data Minimization Principle

The idea that one should only collect and retain that personal data which is necessary.

## Data Protection Authority

Independent public authorities that supervise the application of data protection laws in the EU. DPAs provide advice on data protection issues and field complaints from individuals alleging violations of the General Data Protection Regulation. Each EU member state has its own DPA. Under GDPR, DPAs have extensive enforcement powers, including the ability to impose fines that total 4% of a company's global annual revenue.

Associated Terms: Supervisory Agency

## Data Protection Impact Assessment (DPIA)

The process by which companies can systematically assess and identify the privacy and data protection impacts of any products they offer and services they provide. It enables them to identify the impact and take the appropriate actions to prevent or, at the very least, minimise the risk of those impacts. DPIAs are required by the General Data Protection Regulation in some instances, particularly where a new product or service is likely to result in a high risk to the rights and freedoms of natural persons.

Associated term(s): Privacy Impact Assessments (PIAs)

## Data Protection Models

Sectorial laws: Enhancement of laws that specifically address a particular industry sector (example: Financial transactions, credit controls, law enforcement, medical records, communications)
Country: US

Comprehensive laws: Govern The collection, you son dissemination of personal information in public and private sectors with an official oversight enforcement agency.
Country: EU member states, Canada

Co-Regulatory model : Variant of the comprehensive model where industry develops enforcement standards that are overseen by privacy agency.
Country: Australia

Self-Regulated model: Companies use a code of practice by group of companies known as industry bodies. The Online Privacy Allliance (OPA), TrustArc.
Country: US, Japan, Singapore

## Data Quality

A fair information practices principle, it is the principle that personal data should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. The quality of data is judged by four criteria: Does it meet the business needs?; Is it accurate?; Is it complete?, and is it recent? Data is of an appropriate quality if these criteria are satisfied for a particular application.

## Decentralized Governance

Also known as “local governance,” this governance model involves the delegation of decision-making authority down to the lower levels in an organization, away from and lower than a central authority. There are fewer tiers in the organizational structure, wider span of control and bottom-to-top flow of decision-making and ideas.

Associated term(s): Local Governance

## Direct Marketing

When the seller directly contacts an individual, in contrast to marketing through mass media such as television or radio.

## Do Not Track (DNT)

A proposed regulatory policy, similar to the existing Do-Not-Call Registry in the United States, which would allow consumers to opt out of web-usage tracking.

## Electronic Communications Privacy Act (ECPA) of 1986

The collective name of the Electronic Communications Privacy and Stored Wire Electronic Communications Acts, which updated the Federal Wiretap Act of 1968. ECPA, as amended, protects wire, oral and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The act applies to e-mail, telephone conversations and data stored electronically. The USA PATRIOT Act and subsequent federal enactments have clarified and updated ECPA in light of the ongoing development of modern communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

Associated law(s): Stored Communications Act, Stored Wire Electronic Communications Act, USA Patriot Act

## The European Union Agency for Cybersecurity (ENISA)

ENISA is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Provides guidance on Network and Information Security (NIS).

## European Telecommunications Standards Institute (ETSI)

The European Telecommunications Standards Institute is an independent, not-for-profit, standardization organization in the information and communications technology industry fulfilling European and global market needs.

## EU Data Protection Directive

The EU Data Protection Directive (95/46/EC) was replaced by the General Data Protection Regulation in 2018. The Directive was adopted in 1995, became effective in 1998 and was the first EU-wide legislation that protected individuals' privacy and personal data use.

Associated term(s): Data Protection Directive

## The Fair Information Practices (FIPs)

FIPs provide basic privacy principles central to several modern frameworks, laws and regulations. (Rights of individuals, controls of information, information life cycle, and management.

## Federal Trade Commission (FTC)

The Federal Trade Commission (FTC) is an independent agency of the U.S. government that aims to protect consumers and ensure a strong competitive market by enforcing consumer protection and antitrust laws.

## Foreign Intelligence Surveillance Act (FISA)

FISA provides a statutory framework for the use of electronic surveillance in the context of foreign intelligence gathering

## Foreign Intelligence Surveillance Act (FISA)

US Cloud Service Providers are subject to FISA. In 2008, Congress passed a set of updates to the Foreign Intelligence Surveillance Act (FISA), including Section 702 which authorized warrantless surveillance of non-U.S. persons reasonably believed to be outside the country. However, documents leaked by Edward Snowden revealed that 702 was being used far more heavily than many expected, serving as the legal basis for the collection of large quantities of telephone and Internet traffic  passing through the United States (and unlike 215, including content rather than just metadata). Still, as 702 only permits overseas collection, most criticism of the provision has come from abroad. But many domestic privacy advocates also worry that large amounts of American communication are being swept up "incidentally" and then used as well.

## FISMA

The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and

assets of the agency, including those provided or managed by another agency, contractor, or other source.

## Five-Step Metric Life Cycle

See Metrics

## Gap Analysis

Performed to determine the capability of current privacy management to support each of the business and technical requirements uncovered during an audit or privacy assessment, if any exist; requires reviewing the capabilities of current systems, management tools, hardware, operating systems, administrator expertise, system locations, outsourced services and physical infrastructure.

## Generally Accepted Privacy Principles (GAPP)

A framework promulgated by the American Institute of Certified Public Accountants (AICPA) in conjunction with the Canadian Institute of Chartered Accountants (CICA). The ten principles are management, notice, choice and consent, collection, use and retention, access, disclosure to third parties, security for privacy, quality, monitoring and enforcement.

## Governance, Risk and Compliance (GRC)

The acronym GRC was invented as a shorthand reference to the critical capabilities that must work together to achieve Principle performance – the capabilities that integrate the governance, management and assurance or performance, risk and compliance activities.

Governance, risk and compliance (GRC) is an umbrella term whose scope touches the privacy office among several other internal departments, such as HR, IT, compliance and the C-suite.

## Gramm-Leach-Bliley Act

The commonly used name for The Financial Services Modernization Act of 1999. The act re-organized financial services regulation in the United States and applies broadly to any company that is "significantly engaged" in financial activities in the U.S. In its privacy provisions, GLBA addresses the handling of non-public personal information, defined broadly to include a consumer's name and address, and consumers' interactions with banks, insurers and other financial institutions. GLBA requires financial institutions to securely store personal financial information; give notice of their policies regarding the sharing of personal financial information, and give consumers the ability to opt-out of some sharing of personal financial information.

Acronym(s): GLBA

## Health Insurance Portability and Accountability Act (HIPAA)

A U.S. law passed to create national standards for electronic healthcare transactions, among other purposes. HIPAA required the U.S. Department of Health and Human Services to promulgate regulations to protect the privacy and security of personal health information. The basic rule is that patients have to opt in before their information can be shared with other organizations—although there are important exceptions such as for treatment, payment and healthcare operations.

Related terms: HITECH, The Privacy Rule, The Security Rule

## Hybrid Governance

This privacy governance model allows for a combination of centralized and local governance. Typically seen when a large organization assigns a main individual responsibility for privacy-related affairs, and the local entities then fulfil and support the policies and directives from the central governing body.

## Individual Participation

It is fair information practices principle that an individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have data relating to them communicated to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner, and in a form that is readily intelligible to them; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Associated term(s): FIPs

## Information Life Cycle

The information life cycle recognizes that data has different value, and requires approaches, as it moves through an organization from collection to deletion. The stages are generally considered to be: Collection, processing, use, disclosure, retention, and destruction.

## Information Life Cycle Management

Also known as data life cycle management (DLM) or data governance, ILM is a policy-based approach to managing the flow of information through a life cycle from creation to final disposition. ILM provides a holistic approach to the processes, roles, controls and measures necessary to organize and maintain data, and has 11 elements: Enterprise objectives; minimalism; simplicity of procedure and effective training; adequacy of infrastructure; information security; authenticity and accuracy of one's own records; retrievability; distribution controls; auditability; consistency of policies; and enforcement.

Acronym(s): DLM, ILM

Associated term(s): Data Life Cycle Management

## Information Security Practices/Planning

Information security, sometimes shortened to infosec, is the practice of protecting information by mitigating information risks. It is part of information risk management. It provides management, technical and operational controls to reduce probable damage, loss, modification or unauthorized data access.

## Information Security Triad

Also known as “the C-I-A triad”; consists of three common information security principles: Confidentiality, integrity, and availability.

Associated law(s): C-I-A Triad

## Internal Partners

Professionals and departments within an organization who have ownership of privacy activities, e.g., human resources, marketing, information technology.

## Jurisdiction

The authority of a court to hear a particular case. Courts must have jurisdiction over both the parties to the dispute (personal jurisdiction) and the type of dispute (subject matter jurisdiction). The term is also used to denote the geographical area or subject-matter to which such authority applies.

## Local Governance

Also known as “decentralized governance,” this governance model involves the delegation of decision-making authority down to the lower levels in an organization, away from and lower than a central authority. There are fewer tiers in the organizational structure, wider span of control and bottom-to-top flow of decision-making and ideas.

Associated term(s): Decentralized Governance

## Media Sanitization

Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort.

The NIST Sanitization Methods

- Clear: applies to logical techniques to sanitize data ina ll user-addressable storage locations for protection against simple non-invasive data recovery techniques. (example - software wipe)
- Purge: applies to physical or logical techniques that render Target data recovery infeasible using state of the art laboratory techniques. (example - SecureErase, Cryptographic Erase)
- Destroy: renders target data recovery infeasible using state of art laboratory techniques and results in the subsequent inability to use the media for storage of dat. (example shred, incinerate, Pulverize)

## Metric Life Cycle

The processes and methods to sustain a metric to match the ever-changing needs of an organization. Consists of a 5-step process: (1) Identification of the intended audience; (2) Definition of data sources; (3) Selection of privacy metrics; (4) Collection and refinement of systems/application

collection points; and (5) Analysis of the data/metrics to provide value to the organization and provide a feedback quality mechanism.

## Metrics

Tools that facilitate decision-making and accountability through collection, analysis, and reporting of data. They must be measurable, meaningful, clearly defined (with boundaries), indicate progress, and answer a specific question to be valuable and practical.

Associated term(s): Metric Life Cycle

## National Institute of Standards and Technology (NIST)

NIST is an agency within the Department of Commerce. NIST has the lead responsibility for the development and issuance of security standards and guidelines for the federal government, contractors, and the United States critical information infrastructure.

The NIST has published a series of publications in support of its risk management framework (RMF). The RMF is a multi-tiered and structured methodology for creating a unified information security framework for the federal government in order to meet the vast array of requirements set forth in FISMA.

Associated term(s): FISMA

Associated law(s): FISMA

## Negligence

An organization will be liable for damages if it breaches a legal duty to protect personal information and an individual is harmed by that breach.

Associated term(s): Private Right of Action

## Non-Public Personal Information

Is defined by GLBA as personally identifiable financial information (i) provided by a consumer to a financial institution, (ii) resulting from a transaction or service performed for the consumer, or (iii) otherwise obtained by the financial institution. Excluded from the definition are (i) publicly available information and (ii) any consumer list that is derived without using personally identifiable financial information.

Acronym(s): NPI

Associated law(s): GLBA

## Openness

A fair information practices principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available to establish the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. Closely linked with transparency.

## Opt-In

One of two central concepts of choice. It means an individual makes an active affirmative indication of choice; i.e., checking a box signaling a desire to share his or her information with third parties.

Associated term(s): Choice; Consent; Opt-Out

## Opt-Out

One of two central concepts of choice. It means an individual's lack of action implies that a choice has been made; i.e., unless an individual checks or unchecks a box, their information will be shared with third parties.

Associated term(s): Choice; Consent; Opt-In

## Organization for Economic Cooperation and Development (OECD)

An international organization that promotes policies designed to achieve the highest sustainable economic growth, employment and a rising standard of living in both member and non-member countries, while contributing to the world economy.

### OECD Guidelines

The (OECD) guidelines on the Protection of Privacy and Transborder Flows of Personal data The most widely accepted principles; together with the Council of Europe's Convention 108, is the basis for the data Protection Directive and the GDPR.

Acronym(s): OECD

## PCI Data Security Standard

A self-regulatory system that provides an enforceable security standard for payment card data. The rules were drafted by the Payment Card Industry Security Standards Council, which built on previous rules written by the various credit card companies. Except for small companies, compliance with the standard requires hiring a third party to conduct security assessments and detect violations. Failure to comply can lead to exclusion from Visa, MasterCard or other major payment card systems, as well as penalties.

Acronym(s): PCI-DSS

## Performance Measurement

The process of formulating or selecting metrics to evaluate implementation, efficiency or effectiveness; gathering data and producing quantifiable output that describes performance.

Associated term(s): Metrics

## Personal Data

The predominant term for Personal Information in the European Union, defined broadly in the General Data Protection Regulation as any information relating to an identified or identifiable natural person.

Associated term(s): Personal Information; Personally Identifying Information; Personally Identifiable Information

## Personal Information

A synonym for "personal data." It is a term with particular meaning under the California Consumer Privacy Act, which defines it as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer.

Associated term(s): Personal Data; Personally Identifying Information; Personally Identifiable Information

## Personal Information Protection and Electronic Documents Act (PIPEDA)

A Canadian act with two goals: (1) to instil trust in electronic commerce and private sector transactions for citizens, and (2) to establish a level playing field where the same marketplace rules apply to all businesses.

## Platform for Privacy Preferences (P3P)

A machine-readable language that helps to express a website's data management practices in an automated fashion.

## Privacy by Design (PbD)

Generally regarded as a synonym for Data Protection by Design (see Data Protection by Design). However, Privacy by Design as a specific term was first outlined in a framework in the mid-1990s by then-Information and Privacy Commissioner of Ontario, Canada, Ann Cavoukian, with seven foundational principles.

## Privacy Champion

An executive who serves as the privacy program sponsor and acts as an advocate to further foster privacy as a core organization concept.

## Privacy Impact Assessment (PIA)

"An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." PIAs should disclose what PII is being collected, why it is being collected, what the intended uses of the PII are, whom the PII will be shared with, what opportunities individuals will have to opt-out of PII collection or use, how the PII will be secured, whether a system of records is being created under the Privacy Act and an analysis of the information life cycle. Checklists or tools used to ensure that the system used to collect personal information is evaluated for privacy risks, designed with lifecycle principles in mind and made to ensure that effective and required privacy protection measures are used. A PIA should be

completed pre-implementation of the privacy project, product, or service and should be ongoing through its deployment. The PIA should identify these attributes of the data collected: what information is collected; why it is collected; the intended use of the information; with whom the information is shared, and the consent and choice rights of the data subjects. The PIA should be used to assess new systems, significant changes to existing systems, operational policies and procedures and intended use of the information. PIAs should also be used before, during, and after mergers and acquisitions. An effective PIA evaluates the sufficiency of privacy practices and policies with respect to existing legal, regulatory and industry standards, and maintains consistency between policy and operational practices.

## Privacy Maturity Model

Provides a standardized reference for companies to use in assessing the level of maturity of their privacy programs.

Ad hoc: Procedures and processes are generally informal, incomplete and inconsistently applied.
Repeatable: There are procedures in place but they are not fully documented
Defined – Procedures and processes are fully documented, implemented and cover all relevant aspects
Managed: Reviews are conducted to assess the effectiveness of the controls in place
Optimized: Regular reviews and feedback are used to ensure continual improvement toward optimization of a given process.

## Privacy Operational Life Cycle

Focused on refining and improving privacy processes, this model continuously monitors and improves the privacy program, with the added benefits of a life cycle approach to measure (assess), improve (protect), evaluate (sustain) and support (respond), and then start again.

Associated term(s): Assess; Protect; Sustain; Respond

## Privacy Program Framework

This provides implementation roadmaps that offer the structure or checklists to guide the privacy team through privacy management and prompt them for the details to determine all privacy-relevant decisions for the organization.

The privacy strategy can be thought of as the '**why'**

The privacy framework can be considered the '**what'**

A privacy framework will help reduce risks, avoid incident of data loss, sustain organization market value and reputation, provide measurements in compliance with laws, regulations and standards.

## Privacy Strategy

A privacy strategy should lay out the goals of an organizations privacy program.

Key considerations:

Business alignment; Data Governance of personal information; Inquiry/complaint handling procedures (customers, regulators etc.)

## Privacy Threshold Analysis

One tool used to determine whether a PIA should be conducted.

## Privacy-Enhancing Technologies (PETs)

Privacy technology standards developed solely to be used for the transmission, storage and use of privacy data. Examples include Platform for Privacy Preferences (P3P) and Enterprise Privacy Authorization Language (EPAL).

## Private Right of Action

Unless otherwise restricted by law, any individual that is harmed by a violation of the law can file a lawsuit against the violator.

Associated term(s): Negligence

## Protect

The second of four phases of the privacy operational life cycle. It provides the data life cycle, information security practices and Privacy by Design principles to "protect" personal information.

Associated term(s): Privacy Operational Life Cycle; Assess; Sustain; Respond

## Protected Health Information (PHI)

Under HIPAA PHI is considered to be any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a healthcare clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the provision of healthcare or payment for healthcare services.

PHI includes health records, health histories, lab test results, and medical bills. Essentially, all health information is considered PHI when it includes individual identifiers. Demographic information is also considered PHI under HIPAA Rules, as are many common identifiers such as patient names, Social Security numbers, Driver's license numbers, insurance details, and birth dates, when they are linked with health information.

Acronym(s): PHI

Associated law(s): HIPAA

## Pseudonymous Data

Data points which are not directly associated with a specific individual. The identity of the person is not known but multiple appearances of that person can be linked together. Uses an ID rather than

PII to identify data as coming from the same source. IP address, GUID and ticket numbers are forms of pseudonymous values.

Associated term(s): Identifiability, Identifiers, GUID, Authentication, De-Identification, Re-Identification.

## Purpose Specification

See "Purpose Limitation".

Associated term(s): FIPs

## Qualified Protective Order (QPO)

Requires that the parties are prohibited from using or disclosing protected health information for any purpose other than the litigation and that the PHI will be returned or destroyed at the end of the litigation.

Associated law(s): HIPAA

Associated terms: PHI

## Respond

The fourth of four phases of the privacy operational life cycle. It includes the respond principles of information requests, legal compliance, incident-response planning and incident handling. The "respond" phase aims to reduce organizational risk and bolster compliance to regulations.

Associated term(s): Privacy Operational Life Cycle; Assess; Protect; Sustain

## Retention

Within the information life cycle, the concept that organizations should retain personal information only as long as necessary to fulfil the stated purpose.

## Return on Investment (ROI)

An indicator used to measure the financial gain/loss (or "value") of a project in relation to its cost. Privacy ROI defines metrics to measure the effectiveness of investments to protect investments in assets.

## Right Not To Be Subject to Fully Automated Decisions

Under Article 15 of the Data Protection Directive, individuals are entitled to object to being subject to fully automated decisions. The right, however, does not allow an individual to object to automated processing that then leads to a human decision.

Associated law(s): EU Data Protection Directive

## Risk of Harm Analysis

The analysis of harm and risk of harm is the examination and evaluation process undertaken prior to identifying an appropriate response or intervention.

## Security Safeguards

A fair information practices principle, it is the principle that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

## Social Engineering

A general term for how attackers can try to persuade a user to provide information or create some other sort of security vulnerability.

Associated term(s): Phishing

## Stakeholders

Individual executives within an organization who lead and "own" the responsibility of privacy activities.

## Strategic Management

The first high-level task necessary to implementing proactive privacy management through three subtasks: Define your organization's privacy vision and privacy mission statements; develop privacy strategy; and structure your privacy team.

## Substitute Notice

Most legislation recognizes that data breach notifications involving thousands of impacted data subjects could place an undue financial burden on the organization and therefore allow substitute notification methods. In Connecticut, for example, "Substitute notice shall consist of the following: (A) Electronic mail notice when the person, business or agency has an electronic mail address for the affected persons; (B) conspicuous posting of the notice on the website of the person, business or agency if the person maintains one, and (C) notification to major state-wide media, including newspapers, radio and television."

Associated term(s): Data Breach

## Sustain

The third of four phases of the privacy operational life cycle. It provides privacy management through the monitoring, auditing, and communication aspects of the management framework.

Associated term(s): Privacy Operational Life Cycle; Assess; Protect; Respond

## Unfair Trade Practices

Commercial conduct that intentionally causes substantial injury, without offsetting benefits, and that consumers cannot reasonably avoid.

Associated term(s): Deceptive Trade Practices

Associated law(s): U.S. Federal Trade Commission Act

## U.S. Computer Emergency Readiness Team (US-CERT)

A partnership between the Department of Homeland Security and the public and private sectors intended to coordinate the response to security threats from the Internet. As such, it releases information about current security issues, vulnerabilities and exploits via the National Cyber Alert System and works with software vendors to create patches for security vulnerabilities.

## US-CERT IT Security Essential Body of Knowledge

Fourteen generic information security practice competency areas, including: Digital Security; Digital Forensics; Enterprise Continuity; Incident Management; IT Security and Training Awareness; IT Systems Operation and Maintenance; Network and Telecommunications Security; Personnel Security; Physical and Environmental Security; Procurement; Regulatory and Standards Compliance; Security Risk Management; Strategic Security Management; and System and Application Security.

Link to: US-CERT IT Security Essential Body of Knowledge

## Vendor Management

Assessment of a third-party vendor for the vendor's privacy and information security policies, access controls, where the personal information will be held and who has access to it. Privacy/security questionnaires, privacy impact assessments and other checklists can be used to assess this risk.

## Video Surveillance

Recordings that do not have sound.

Associated term(s): Video Surveillance Guidelines

Associated law(s): FISA