CIPT - GLOSSARY

ALLNET LAW

Contents

Abstract

Limit the amount of detail in which personal information is processed.

Access Control Entry

An element in an access control list (ACL). Each ACE controls, monitors, or records access to an object by a specified user.

Acronym(s): ACE

Associated term(s): Access Control List (ACL)

Access Control List

A list of access control entries (ACE) that apply to an object. Each ACE controls or monitors access to an object by a specified user. In a discretionary access control list (DACL), the ACL controls access; in a system access control list (SACL) the ACL monitors access in a security event log which can comprise part of an audit trail.

Acronym(s): ACL

Associated term(s): Access Control Entry (ACE)

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.

Accuracy

Organizations must take every reasonable step to ensure the data processed is accurate and, where necessary, kept up to date. Reasonable measures should be understood as implementing processes to prevent inaccuracies during the data collection process as well as during the ongoing data processing in relation to the specific use for which the data is processed. The organization must consider the type of data and the specific purposes to maintain the accuracy of personal data in relation to the purpose. Accuracy also embodies the responsibility to respond to data subject requests to correct records that contain incomplete information or misinformation.

Act Respecting the Protection of Personal Information in the Private Sector

A Québéquois privacy law that, other than different terminology, is similar to PIPEDA, though at a province level. It came into force in 1994 and espouses three principles: (1) Every person who establishes a file on another person must have a serious and legitimate reason for doing so; (2) The person establishing the file may not deny the individual concerned access to the information contained in the file; (3) The person must also

respect certain rules that are applicable to the collection, storage, use and communication of this information.

Link to text of law: Act Respecting the Protection of Personal Information in the Private Sector

Active Data Collection

When an end user deliberately provides information, typically through the use of web forms, text boxes, check boxes or radio buttons.

Associated term(s): Passive Data Collection, First-party Collection, Surveillance Collection, Repurposing, Third-party Collection

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.

Ad Exchange

An ad trafficking system through which advertisers, publishers, and networks meet and do business via a unified platform. An ad exchange allows advertisers and publishers to use the same technological platform, services, and methods, and "speak the same language" in order to exchange data, set prices, and ultimately serve an ad.

Ad Network

A company that serves as a broker between a group of publishers and a group of advertisers. Networks traditionally aggregate unsold inventory from publishers in order to offer advertisers a consolidated and generally less expensive pool of impressions, but they can have a wide variety of business models and clients.

AdChoices

A program run by the Digital Advertising Alliance to promote awareness and choice in advertising for internet users. Websites with ads from participating DAA members will have an AdChoices icon near advertisements or at the bottom of their pages. By clicking on the Adchoices icon, users may set preferences for behavioral advertising on that website or with DAA members generally across the web.

Associated term(s): Digital Advertising Alliance

Adequate Level of Protection

A transfer of personal data from the European Union to a third country or an international organisation may take place where the European Commission has decided

that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question, ensures an adequate level of protection by taking into account the following elements: (a) the rule of law, respect for human rights and fundamental freedoms, both general and sectoral legislation, data protection rules, professional rules and security measures, effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data is being transferred; (b) the existence and effective functioning of independent supervisory authorities with responsibility for ensuring and enforcing compliance with the data protection rules; (c) the international commitments the third country or international organisation concerned has entered into in relation to the protection of personal data.

Associated term(s): Adequacy

Administrative Purpose

The use of personal information about an individual in Canada in a decision-making process that directly affects that individual.

Advanced Encryption Standard

An encryption algorithm for security sensitive non-classified material by the U.S. Government. This algorithm was selected in 2001 to replace the previous algorithm, the Data Encryption Standard (DES), by the National Institute of Standards and Technology (NIST), a unit of the U.S. Commerce Department, through an open competition. The winning algorithm (RijnDael, pronounced rain-dahl), was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen.

Acronym(s): AES

Associated term(s): Authentication, Encryption

Adverse Action

Under the Fair Credit Reporting Act, the term “adverse action” is defined very broadly to include all business, credit and employment actions affecting consumers that can be considered to have a negative impact, such as denying or canceling credit or insurance, or denying employment or promotion. No adverse action occurs in a credit transaction where the creditor makes a counteroffer that is accepted by the consumer. Such an action requires that the decision maker furnish the recipient of the adverse action with a copy of the credit report leading to the adverse action.

Associated law(s): FCRA

Agile Development Model

A process of software system and product design that incorporates new system requirements during the actual creation of the system, as opposed to the Plan-Driven Development Model. Agile development takes a given project and focuses on specific portions to develop one at a time. An example of Agile development is the Scrum Model.

Associated term(s): Plan-Driven Development Model, User Stories, SRS

Alberta PIPA

A privacy law in the Canadian province of Alberta, similar to PIPEDA, that came into force in 2004. Unlike PIPEDA, these acts clearly apply to employee information.

Link to text of law: Alberta PIPA

Associated law(s): PIPEDA

Algorithms

Mathematical applications applied to a block of data.

American Institute of Certified Public Accountants

A U.S. professional organization of certified public accountants and co-creator of the WebTrust seal program.

Acronym(s): AICPA

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

Americans with Disabilities Act

A U.S. law that bars discrimination against qualified individuals with disabilities.

Link to text of law: Americans with Disabilities Act

Acronym(s): ADA

Annual Independent Evaluations

Under FISMA, U.S. agencies' information security programs must be independently evaluated yearly. The independent auditor is selected by the agency's inspector general or the head of the agency. The audit is submitted to the Office of Management and Budget.

Associated law(s): FISMA

Annual Reports

The requirement under the General Data Protection Regulation that the European Data Protection Board and each supervisory authority periodically report on their activities. The supervisory authority report should include infringements and the activities that the authority conducted under their Article 58(2) powers. The EDPB report should include guidelines, recommendations, best practices and binding decisions. Additionally, the report should include the protection of natural persons with regard to processing in the EU and, where relevant, in third countries and international organisations. The report

shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

Associated law(s): EU Data Protection Directive

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

Anonymous Information

In contrast to personal data, anonymous information or data is not related to an identified or an identifiable natural person and cannot be combined with other information to re-identify individuals. It has been rendered unidentifiable and, as such, is not protected by the GDPR.

Associated term(s): Pseudonymous Data, De-Identification, Re-Identification

Anthropomorphism

Attributing human characteristics or behaviors to non-human objects.

Anti-discrimination Laws

Anti-discrimination laws are indications of special classes of personal data. If there exists law protecting against discrimination based on a class or status, it is likely personal information relating to that class or status is subject to more stringent data protection regulation, under the GDPR or otherwise.

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.

Application or field encryption
Ability to encrypt specific fields of data; specifically sensitive data such as credit cards numbers or health-related information.

Application-Layer Attacks
Attacks that exploit flaws in the network applications installed on network servers. Such weaknesses exist in web browsers, e-mail server software, network routing software and other standard enterprise applications. Regularly applying patches and updates to applications may help prevent such attacks.

Appropriate Safeguards
The General Data Protection Regulation refers to appropriate safeguards in a number of contexts, including the transfer of personal data to third countries outside the European Union, the processing of special categories of data, and the processing of personal data in a law enforcement context. This generally refers to the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules. This may also refer to the use of encryption or pseudonymization, standard data protection clauses adopted by the Commission, contractual clauses authorized by a supervisory authority, or certification schemes or codes of conduct authorized by the Commission or a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the European Union.

Appropriate Technical and Organizational Measures
The General Data Protection Regulation requires a risk-based approach to data protection, whereby organizations take into account the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, and institute policies, controls and certain technologies to mitigate those risks. These "appropriate technical and organisational measures" might help meet the obligation to keep personal data secure, including technical safeguards against accidents and negligence or deliberate and malevolent actions, or involve the implementation of data protection policies. These measures should be demonstrable on demand to data protection authorities and reviewed regularly.

Appropriation
Using someone's identity for another person's purposes.

Article 29 Working Party

The Article 29 Working Party (WP29) was a European Union organization that functioned as an independent advisory body on data protection and privacy and consisted of the collected data protection authorities of the member states. It was replaced by the similarly constituted European Data Protection Board (EDPB) on May 25, 2018, when the General Data Protection Regulation (GDPR) went into effect.

Acronym(s): WP29

Artificial Intelligence

Artificial intelligence is a broad term used to describe a process where machines learn from experience, adjusting to new inputs, and potentially performing tasks previously done by humans. More specifically, it is a field of computer science dedicated to simulating intelligent behavior in computers. It may include automated decision-making (see also Machine Learning).

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

Asymmetric Encryption

A form of data encryption that uses two separate but related keys to encrypt data. The system uses a public key, made available to other parties, and a private key, which is kept by the first party. Decryption of data encrypted by the public key requires the use of the private key; decryption of the data encrypted by the private key requires the public key.

Associated term(s): Symmetric Encryption, Encryption

Attribute-Based Access Control

An authorization model that provides dynamic access control by assigning attributes to the users, the data, and the context in which the user requests access (also referred to as environmental factors) and analyzes these attributes together to determine access.

Acronym(s): ABAC

Associated term(s): User-based Access Control

Audit Life Cycle

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

Audit Trail

A chain of electronic activity or sequence of paperwork used to monitor, track, record, or validate an activity. The term originates in accounting as a reference to the chain of paperwork used to validate or invalidate accounting entries. It has since been adapted for more general use in e-commerce, to track customer's activity, or cyber-security, to investigate cybercrimes.

Authentication

The process by which an entity (such as a person or computer system) determines whether another entity is who it claims to be.

Associated term(s): Authorization

Authorization

In the context of information security, it is process of determining if the end user is permitted to have access to the desired resource such as the information asset or the information system containing the asset. Authorization criteria may be based upon a variety of factors such as organizational role, level of security clearance, applicable law or a combination of factors. When effective, authentication validates that the entity requesting access is who or what it claims to be.

Associated term(s): Authentication

Automated decision making

The process of making a decision without human involvement.

Automated Processing

A processing operation that is performed without any human intervention. "Profiling" is defined in the General Data Protection Regulation, for example, as the automated processing of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Data subjects, under the GDPR, have a right to object to such processing.

Availability

Data is "available" if it is accessible when needed by the organization or data subject. The General Data Protection Regulation requires that a business be able to ensure the availability of personal data and have the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

Background Screening/Checks

Organizations may want to verify an applicant's ability to function in the working environment as well as assuring the safety and security of existing workers. Background checks range from checking a person's educational background to checking on past criminal activity. Employee consent requirements for such check vary by member state and may be negotiated with local works councils.

Bank Secrecy Act, The

A U.S. federal law that requires U.S. financial institutions and money services businesses (MSBs), which are entities that sell money orders or provide cash transfer services, to record, retain and report certain financial transactions to the federal government. This requirement is meant to assist the government in the investigation of money laundering, tax evasion, terrorist financing and various other domestic and international criminal activities.

Link to text of law: The Bank Secrecy Act (BSA)

Acronym(s): BSA

Associated term(s): Financial Record Keeping and Reporting Currency and Foreign Transactions Act of 1970

Basel III

A comprehensive set of reform measures, developed by the Basel Committee on Banking Supervision, to strengthen the regulation, supervision and risk management of the banking sector.

BC PIPA

A privacy law in the Canadian province of British Columbia, similar to PIPEDA, that came into force in 2004. Unlike PIPEDA, these acts clearly apply to employee information.

Link to text of law: BC PIPA

Associated law(s): PIPEDA

Behavioral Advertising

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.

Acronym(s): OBA

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

Big Data

A term used to describe the large data sets which exponential growth in the amount and availability of data have allowed organizations to collect. Big data has been articulated as "the three V's: volume (the amount of data), velocity (the speed at which data may now be collected and analyzed), and variety (the format, structured or unstructured, and type of data, e.g. transactional or behavioral).

Associated term(s): Metadata

Binding Corporate Rules

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.

Acronym(s): BCR

Binding Safe Processor Rules

Previously, the EU distinguished between Binding Corporate Rules for controllers and Binding Safe Processor Rules for processors. With the General Data Protection Regulation, there is now no distinction made between the two in this context and Binding Corporate Rules are appropriate for both.

Acronym(s): BSPR

Associated term(s): Binding Corporate Rules

Biometrics

Data concerning the intrinsic physical or behavioral characteristics of an individual. Examples include DNA, fingerprints, retina and iris patterns, voice, face, handwriting, keystroke technique and gait. The General Data Protection Regulation, in Article 9, lists biometric data for the purpose of uniquely identifying a natural person as a special category of data for which processing is not allowed other than in specific circumstances.

Associated term(s): Personal Information

Blackmail
The threat to disclose an individual's information against his or her will.

Bodily Privacy
One of the four classes of privacy, along with information privacy, territorial privacy and communications privacy. It focuses on a person's physical being and any invasion thereof. Such an invasion can take the form of genetic testing, drug testing or body cavity searches.

Breach Disclosure
The requirement that an organization notify regulators and/or victims of incidents affecting the confidentiality and security of personal data. The requirements in this arena vary wildly by jurisdiction. It is a transparency mechanism that highlights operational failures, which helps mitigate damage and aids in the understanding of causes of failure.

Associated law(s): FCRA, GLBA, HIPAA, various U.S. state laws

Associated term(s): Breach notification

Breach Disclosure (EU specific)
The requirement that a data controller notify regulators, potentially within 72 hours of discovery, and/or victims, of incidents affecting the confidentiality and security of personal data, depending on the assessed risks to the rights and freedoms of affected data subjects (see Data Breach).

Breach of confidentiality
Revealing an individual's personal information, despite a promise not to do so.

Bring Your Own Device
Use of employees' own personal computing devices for work purposes.

Acronym(s): BYOD

Associated term(s): Consumerization of information technology (COIT)

Browser Fingerprinting
As technology has advanced, it has become easier to differentiate between users just based on the given instance of the browser they are using. Each browser keeps some information about the elements it encounters on a given webpage. For instance, a browser will keep information on a text font so that the next time that font is encountered on a webpage, the information can be reproduced more easily. Because each of these saved elements have been accessed at different times and in different

orders, each instance of a browser is to some extent unique. Tracking users using this kind of technology continues to become more prevalent.

Bundesdatenschutzgesetz-neu

Germany's federal data protection act, implementing the General Data Protection Regulation. With the passage of the GDPR, it replaced a previous law with the same name (hence "neu" in common parlance) and enhanced a series of other acts mainly in areas of law enforcement and intelligence services. Furthermore, the new version suggests a procedure for national data protection authorities to challenge adequacy decisions of the EU Commission.

Link to text of law: Bundesdatenschutzgesetz

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

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.

Acronym(s): BCDR

Business Continuity Plan

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.

Acronym(s): BCP

Caching

The saving of local copies of downloaded content, reducing the need to repeatedly download content. To protect privacy, pages that display personal information should be set to prohibit caching.

California Consumer Privacy Act

The first state-level comprehensive privacy law in the U.S. The CCPA, which comes into force in 2020, will apply broadly to businesses that collect personal information from California consumers, imposing extensive transparency and disclosure obligations. It also creates consumers' rights to access their personal data and to request its deletion; to opt-out of the sale of their personal data; and to nondiscrimination on the basis of their exercising any of their CCPA rights.

California Investigative Consumer Reporting Agencies Act

A California state law that requires employers to notify applicants and employees of their intention to obtain and use a consumer report.

Link to text of law: California Investigative Consumer Reporting Agencies Act

Acronym(s): CICRAA

California Online Privacy Protection Act

Requires that all websites catering to California citizens provide a privacy statement to visitors and a easy-to-find link to it on their web pages. Websites that carry personal data on children less than 18 years of age must permit those children to delete data collected about them. Websites also must inform visitors of the type of Do Not Track mechanisms they support or if they do not support any at all.

Link to text of law: California Online Privacy Protection Act

Acronym(s): CalOPPA

Associated term(s): Do Not Track

Canada's Anti-Spam Legislation

Canadian anti-SPAM legislation applying to all forms of electronic messaging. It requires that when a commercial electronic message (CEM) is sent, consent, identification and unsubscribing requirements must be complied with. Typically, consent from the recipient must be obtained before a CEM is sent. There are, however, a number of exceptions to the need for consent.

Link to text of law: Canada's Anti-Spam Legislation

Acronym(s): CASL

Canadian Institute of Chartered Accountants

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

Acronym(s): CICA

Canadian Organization for the Advancement of Computers in Health

A Canadian health informatics association whose mission is to promote health technology systems and the effective use of health information.

Acronym(s): COACH

Canadian Standards Association

A non-profit standards organization that developed its own set of privacy principles and broke the OECD's code into ten principles: (1) Accountability; (2) Identifying purposes; (3) Consent; (4) Limiting Collection; (5) Limiting Use, Disclosure, and Retention; (6) Accuracy; (7) Safeguards; (8) Openness; (9) Individual Access; (10) Challenging Compliance. These ten principles would go on to be listed in PIPEDA.

Acronym(s): CSA

Associated term(s): CSA Privacy Principles

Case Law

Principles of law that have been established by judges in past decisions. When similar issues arise again, judges look to the past decisions as precedents and decide the new case in a manner that is consistent with past decisions.

CCTV

Originally an acronym for "closed circuit television," CCTV has come to be shorthand for any video surveillance system. Originally, such systems relied on coaxial cable and was truly only accessible on premise. Today, most surveillance systems are hosted via TCP/IP networks and can be accessed remotely, and the footage much more easily shared, eliciting new and different privacy concerns.

Associated term(s): Video Surveillance

Census Bureau

The Census Bureau collects data to meet the nation's statistical needs. Because the data that the Census Bureau collects is often highly personal in nature, and the Census Bureau depends on the trust of the individuals and businesses that supply the data, privacy protection is a high priority.

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.

Certification Mechanisms

Introduced by the General Data Protection Regulation, certification mechanisms are a new valid adequacy mechanism for the transfer of personal data outside of the European Union in the absence of an adequacy decision and instead of other mechanisms such as binding corporate rules or contractual clauses. Certification mechanisms must be developed by certifying bodies, approved by data protection authorities or the European Data Protection Board, and have a methodology for auditing compliance. Similar to binding corporate rules, they compel organizations to be able to demonstrate their compliance with all aspects of applicable data protection legislation.

Charter of Fundamental Rights

A treaty that consolidates human rights within the EU. The treaty states that everyone has a right to protect their personal data, that data must be processed for legitimate and specified purposes and that compliance is subject to control by an authority.

Link to text of law: Charter of Fundamental Rights of the European Union

Charter Rights

Rights created by the Canadian Charter of Rights and Freedoms. They are constitutional rights and thus are considered to be the most valued rights in Canada. The Charter of Rights and Freedoms was made part of the Canadian Constitution in 1982.

Link to text of law: Canadian Charter of Rights and Freedoms

Chat bots

Computerized intelligence that simulates human interactions and may be used to handle basic customer requests and interactions.

Chief FOIA Officer

Executive Order 13392 supplemented FOIA by reiterating the requirement for agencies to process requests in a courteous and expeditious manner. In addition, it required agencies to appoint a chief FOIA officer. The Open Government Act of 2007 codified this requirement and expanded on the responsibilities of the chief FOIA officer to include the following: have agency-wide responsibility for efficient and appropriate compliance with FOIA; monitor FOIA implementation throughout the agency; recommend to the head of the agency any necessary adjustments in practices, personnel, policies or funding.

Associated term(s): Freedom of Information Act

Associated law(s): Freedom of Information Act

Chief Privacy Officer (Agency level)

A position within an organization that is responsible for managing risks of privacy laws and policies. Within the U.S. government, this position was created under section 522(a) of the Consolidated Appropriations Act of 2005.

Acronym(s): CPO

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.

Acronym(s): COPPA

Link to text of law: 15 U.S.C. §§ 6501-6508

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

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

CIO Council

The CIO Council is the principal interagency forum on Federal agency practices for IT management. Originally established by Executive Order 13011 (Federal Information Technology) and later codified by the E-Government Act of 2002, the CIO Council's mission is to improve practices related to the design, acquisition, development, modernization, use, sharing and performance of Federal Government information resources.

Ciphertext

Encrypted (enciphered) data.

Associated term(s): NIST SP 800-21

Cloud Computing

The provision of information technology services over the Internet. These services may be provided by a company for its internal users in a "private cloud" or by third-party suppliers. The services can include software, infrastructure (i.e., servers), hosting and platforms (i.e., operating systems). Cloud computing has numerous applications, from personal webmail to corporate data storage, and can be subdivided into different types of service models.

Co-regulatory Model

Emphasizes industry development of enforceable codes or standards for privacy and data protection against the backdrop of legal requirements by the government. Co-regulation can exist under both comprehensive and sectoral models.

Associated term(s): Comprehensive Laws, Sectoral Laws, Self-regulatory Model, Technology Based Model

Code audits

Provide analysis of source code that detect defects, security breaches or violations within a technology ecosystem.

Code reviews

Generally in-person meeting organized by developers who authored the code. The review may consist of a reader, moderator and privacy specialist.

Codes of Conduct

Introduced by the General Data Protection Regulation, codes of conduct are a new valid adequacy mechanism for the transfer of personal data outside of the European Union in the absence of an adequacy decision and instead of other mechanisms such as binding corporate rules or contractual clauses. Codes of conduct must be developed by industry trade groups, associations or other bodies representing categories of controllers or processors. They must be approved by supervisory authorities or the European Data Protection Board, and have a methodology for auditing compliance. Similar to binding corporate rules, they compel organizations to be able to demonstrate their compliance with all aspects of applicable data protection legislation.

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.

Commercial Activity

Under Canada's PIPEDA, “commercial activity” means any particular transaction, act or conduct, or any regular course of conduct, that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists. Non-profit associations, unions and private schools are likely to be found to exist outside of this definition.

Commercial Electronic Message

Any form of electronic messaging, including e-mail, SMS text messages and messages sent via social networking about which it would be reasonable to conclude its purpose is to encourage participation in a commercial activity. Examples include electronic messages that offer to purchase, sell, barter or lease products, goods, services, land or an interest or right in land; offers to provide a business, investment or gaming opportunity; advertises or promotes anything previously mentioned.

Acronym(s): CEM

Common Law
Unwritten legal principles that have developed over time based on social customs and expectations.

Communications Privacy
One of the four classes of privacy, along with information privacy, bodily privacy and territorial privacy. It encompasses protection of the means of correspondence, including postal mail, telephone conversations, electronic e-mail and other forms of communicative behavior and apparatus.

Completeness Arguments
Used as a means of assuring compliance with privacy rules and policies in the design of new software systems. Completeness arguments take privacy rules and compare them to the system requirements that have been used to design a new software system. By pairing privacy rules with specific system requirements, necessary technical safeguards can be accounted for, preventing the software from being designed in such a way that would violate privacy policies and regulations.

Associated term(s): SRS, User Stories, Plan-driven Development Model, Agile Development Model

Comprehensive Laws
Laws that govern the collection, use and dissemination of personal information in the public and private sectors.

Associated term(s): Omnibus Laws

Computer Forensics
The discipline of assessing and examining an information system for relevant clues even after it has been compromised by an exploit.

Computer Matching and Privacy Protection Act

Requires agencies that match data among agency systems granting financial benefits to publicly disclose that matching and explain its scope.

Concept of Operations
Used in Plan-driven Development Models, a Concept of Operations is a detailed outline of how a software product or system will work once it is fully operational. This is used to shape how a product or system will be designed and implemented.

Acronym: CONOPS

Associated term(s): Plan-driven Development Model, SRS

Confidentiality

Data is "confidential" if it is protected against unauthorised or unlawful processing. The General Data Protection Regulation requires that an organization be able to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services as part of its requirements for appropriate security. In addition, the GDPR requires that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

Confirmed Opt-In

An email approach where email marketers send a confirmation email requiring a response from the subscriber before the subscriber receives the actual marketing e-mail.

Associated term(s): Double Opt-In

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

Consent (EU specific)

This privacy requirement is one of the fair information practices. In the General Data Protection Regulation, however, consent is specifically one of the legal bases for processing personal data. According to the GDPR, for consent to be valid, it must be: clearly distinguishable from other matters, intelligible, and in clear and plain language; freely given; as easy to withdraw as it was to provide; specific; informed; and unambiguous. Further, it must be a positive, affirmative action (e.g., checking opt-in or choosing technical settings for web applications), with pre-ticked boxes expressly not allowed. For certain special categories of data, as outlined in Article 9, explicit consent is required for processing, a higher standard than unambiguous consent.

Consent Decree

A judgment entered by consent of the parties. Typically, the defendant agrees to stop alleged illegal activity and pay a fine, without admitting guilt or wrongdoing. This legal document is approved by a judge and formalizes an agreement reached between a U.S. federal or state agency and an adverse party.

Associated term(s): FTC

Consistency Mechanism

In order to ensure the consistent application of the General Data Protection Regulation throughout the European Union, the GDPR establishes a "consistency mechanism" that allows member state supervisory authorities to cooperate with one another. The mechanism applies particularly where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several member states. When a member state supervisory authority intends to take action, such as approving a code of conduct or certification mechanism, it shall provide a draft to the European Data Protection Board, and the EDPB's members shall render an opinion on that draft, which the supervisory authority shall take into account and then either amend or decide to go forward with the draft in its original form. Should there be significant difference in opinion, the dispute resolution mechanism will be triggered.

Consumer Financial Protection Bureau

Created by the Dodd-Frank Act, the consumer financial protection bureau is intended to consolidate the oversight of the financial industry. It is an independent bureau within the Federal Reserve and when it was created CFPB took rule-making authority over FCRA and GLBA regulations from the FTC and Financial Industry Regulators. Its enforcement powers include authority to take action against “abusive acts and practices” as specified by the Dodd-Frank Act.

Acronym: CFPB

Associated law(s):Dodd-Frank Act, Gramm-Leach-Bliley Act, Fair Credit Reporting Act, Federal Trade Commission

Consumer Report

As defined in the U.S. Fair Credit Reporting Act: Any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (1) credit or insurance to be used primarily for personal, family, or household purposes, or (2) employment purposes, or (3) other purposes authorized under section 604. The term does not include any (A) any report containing information solely as to transactions or experiences between the consumer and the person making the report; (B) authorization or approval of a specific extension of credit

directly or indirectly by the issuer of a credit card or similar device; or (C) report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer conveys his decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made and such person makes the disclosures to the consumer required under section 615.

Associated term(s): Credit Reporting Agency

Associated law(s): Fair Credit Reporting Act

Consumer Reporting Agency

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

Acronym(s): CRAs

Associated term(s): Credit Reporting Agency

Consumerization of Information Technology (COIT)

A trend in the adoption of information technology where the technology emerges first in the consumer market before spreading to business and government organizations. The adoption of technology within organizations is driven by employees using consumer devices at home and then introducing them into the workplace.

Content Data

The text, images, etc., contained within any communication message, such as an email, text, or instant message on any given communications platform. Specifically used often to distinguish from metadata (see Metadata). The ePrivacy Directive and draft ePrivacy Regulation protect the confidentiality of content data.

Content Delivery Network

The servers that contain most or all of the visible elements of a web page and that are contacted to provide those elements. In the realm of advertising, a general ad server is contacted after a webpage is requested, that ad server looks up any known information on the user requesting to access the webpage.

Context aware computing

When a technological device adapts itself to the environment. This includes characteristics as location, video, audio, brightness.

Context of authority

Control over the access to resources on a network is based on the context in which the employee is connected to the network.

Contextual Advertising

The most used form of targeted advertising on the internet. The content of the ad relies on the content of the webpage or the query entered by a user.

Associated term(s): Behavioral Advertising, Demographic Advertising, Premium Advertising, Psychographic Advertising, Remnant Advertising.

Contextual Integrity

A concept developed by Helen Nissenbaum, contextual integrity is a way to think about and quantify potential privacy risks in software systems and products. Contextual Integrity focuses on what consumer expectations are in a given situation and how the product or system differs from that expectation. The more a product or system deviates from those expectations, the more likely a consumer will perceive a privacy harm.

Associated term(s): Privacy Risk

Contractual Clauses

Adopted either directly by the European Commission or by a supervisory authority in accordance with the consistency mechanism (see Consistency Mechanism) and then adopted by the Commission, contractual clauses are mechanisms by which organisations can commit to protect personal data to facilitate ongoing and systematic cross-border personal data transfers.

Controlled Unclassified Information

A system that standardizes and simplifies the way the executive branch handles unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies. The program emphasizes the openness and uniformity of government-wide practices. Its purpose is to address the current inefficient and confusing patchwork that leads to inconsistent marking and safeguarding as well as restrictive dissemination policies, which are often hidden from public view.

Acronym(s): CUI

Convention 108

Convention 108 is a legally binding international instrument that requires signatory countries to take the necessary steps in their domestic legislation to apply the principles

it lays down ensuring fundamental human rights with regard to the processing of personal information.

Link to text of law: The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

Cookie

A small text file stored on a client machine that may later be retrieved by a web server from the machine. Cookies allow web servers to keep track of the end user's browser activities, and connect individual web requests into a session. Cookies can also be used to prevent users from having to be authorized for every password protected page they access during a session by recording that they have successfully supplied their username and password already. Cookies may be referred to as "first-party" (if they are placed by the website that is visited) or "third-party" (if they are placed by a party other than the visited website). Additionally, they may be referred to as "session cookies" if they are deleted when a session ends, or "persistent cookies" if they remain longer. Notably, the General Data Protection Regulation lists this latter category, so-called "cookie identifiers," as an example of personal information. The use of cookies is regulated both by the GDPR and the ePrivacy Directive (see Cookie Directive).

Associated term(s): First-Party Cookie, Persistent Cookie, Third-Party Cookie, Tracking Cookie, Web Cookie

Cookie Directive

The so-called "Cookie Directive" is an amendment made to the European Union's Directive 2002/58, also known as the ePrivacy Directive, that requires organizations to get consent before placing cookies (see Cookies) and other tracking technologies on digital devices. With the passage of the General Data Protection Regulation, this definition of consent has changed and opt-out consent is no longer viable in this area.

Associated term(s): Directive 2009/136/EC, ePrivacy Directive

Cooperation

Part of the consistency mechanism (see Consistency Mechanism) of the General Data Protection Regulation, cooperation is required between supervisory authorities when working with controllers or processors handling the personal data of data subjects in multiple member states. This is often referred to as the "one-stop shop," whereby a lead supervisory authority works with the supervisory authorities of other member states with affected data subjects.

Copland v. United Kingdom

A case in which the European Court of Human Rights held that monitoring an applicant's email at work was contrary to Article 8 of the Convention on Human Rights.

Link to case: Copland v. United Kingdom

Corporate Owned, Personally Enabled (COPE)

COPE is the IT business strategy of providing employees with company-owned devices. COPE may, nonetheless, implicate BYOD concerns when employees use COPE devices equally for personal use.

Costeja

Shorthand for the case of Google Spain v AEPD and Mario Costeja González, where Costeja successfully sued Google Spain, Google Inc. and La Vanguardia newspaper. When the Court of Justice of the EU ruled that Google Spain must remove the links to the article, the "right to be forgotten" (see Right To Be Forgotten) was effectively established in the European Union. The General Data Protection Regulation subsequently more formally granted data subjects the right to deletion in certain circumstances.

Council of Europe

The Council of Europe, launched in 1949, is a human rights organization with 47 member countries, including the 28 member states of the European Union. The members have all signed the European Convention on Human rights and are subject to the European Court of Human Rights. The Council's Convention 108 (see Convention 108) was the first legally binding international agreement to protect the human right of privacy and data protection.

Council of the European Union

A council of ministers from the 28 member states of the European Union, this is the main decision-making body of the EU, with a central role in both political and legislative decisions. The council was established by the treaties of the 1950s, which laid the foundations for the EU, and works with the European Parliament to create EU law.

Link to: Council of the European Union

Associated term(s): Council of Ministers

Coupling

The interdependence between objects within a technology ecosystem and controls the flow of information within a design. Tightening the coupling, allows objects to depend on the inner working of other objects. Loosening the coupling reduces object's dependency on other objects. Loosening isolates information processing to a select group of approved classes and reduces the chance of unintentionally re-purposing data.

Court of Justice of the European Union

The Court of Justice is the judicial body of the EU that makes decisions on issues of EU law and enforces European decisions either in respect to actions taken by the European Commission against a member state or actions taken by individuals to enforce their rights under EU law. Based in Luxembourg, the Court was set up in 1951, and was originally named the Court of Justice of the European Communities. The court is frequently confused with the European Court of Human Rights (ECHR), which oversees human rights laws across Europe, including in many non-EU countries, and is not linked to the EU institutions.

Acronym(s): CJEU

Link to: Court of Justice of the European Union

Credit Freeze

A consumer-initiated security measure which locks an individual's data at consumer reporting agencies. Is used to prevent identity theft, as it disallows both reporting of data and issuance of new credit.

Credit Reporting Agency

Under the Fair Credit Reporting Act, any organization that regularly engages in assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties for a fee.

Acronym(s): CRA

Associated term(s): Consumer reporting agency

Associated law(s): FCRA

Cross-border Data Transfers

The transmission of personal information from one jurisdiction to another. Many jurisdictions, most notably the European Union, place significant restrictions on such transfers. The EU requires that the receiving jurisdiction be judged to have "adequate" data protection practices.

Cross-border Data Transfers (EU specific)

Transfers of personal data to any country outside the European Economic Area (EEA) may only take place subject to the condition that the third country ensures an adequate level of protection for the personal data as determined by the European Commission. It also applies to onward transfers — from one third country or international organisation to another (outside the EEA). In the absence of an adequacy finding, organizations must use other mechanisms, such as binding corporate rules, contractual clauses, or certification, for lawful transfer.

Cross-site Scripting
Code injected by malicious web users into web pages viewed by other users.

Acronym(s): XSS

Cryptography
The science or practice of hiding information, usually through its transformation. Common cryptographic functions include: encryption, decryption, digital signature and non-repudiation.

Associated term(s): Digital signature, encryption, non-repudiation, PKI

Cryptosystem
The materials necessary to encrypt and decrypt a given message, usually consisting of the encryption algorithm and the security key.

Associated term(s): Encryption

CSA Privacy Principles
The Canadian Standards Association (CSA) ten privacy principles are based on the OECD Guidelines and serve as the basis of Canada's PIPEDA.

Associated term(s): Canadian Standards Association

Associated law(s): PIPEDA

Current baseline
"As-is" data privacy requirements; the current environment and any protections, policies, and procedures currently deployed.

Customer Access
A customer's ability to access the personal information collected on them as well as review, correct or delete any incorrect information.

Customer Data Integration
The consolidation and managing of customer information in all forms and from all sources allowable. CDI is a vital component of customer relationship management.

Acronyms: CDI

Associated term(s): Customer Relationship Management

Customer Information

In contrast to employee information, customer information includes data relating to the clients of private-sector organizations, patients within the healthcare sector and the general public within the context of public-sector agencies that provide services.

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.

Cyberbullying

Exposing a person's private details or re-characterizing the person beyond the person's control via technology.

Dark patterns

Recurring solutions that are used to manipulate individuals into giving up personal information.

Data Aggregation

Taking Individual data sets and combining them to statistically analyze data trends while protecting individual privacy by using groups of individuals with similar characteristics rather than isolating one individual at a time. To effectively aggregate data so that it cannot be re-identified (or at least make it difficult to do so) the data set should: (1) have a large population of individuals, (2) Categorized to create broad sets of individuals, and; (3) not include data that would be unique to a single individual in a data set.

Associated term(s): De-identification, Re-identification, Pseudonymous Data, Anonymous Information, Identifiability, Identifiers.

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 Breach (EU specific)

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. The General Data Protection Regulation instituted new rules for notification of supervisory authorities and data subjects following the discovery of a data breach, depending on the risk the breach presents to the rights and freedoms of data subjects.

Data Breach Notification (EU specific)

The requirement that a data controller notify regulators, potentially within 72 hours of discovery, and/or victims, of incidents affecting the confidentiality and security of personal data, depending on the assessed risks to the rights and freedoms of affected data subjects (see Data Breach).

Data Brokers

Entities that collect, aggregate and sell individuals' personal data, derivatives and inferences from disparate public or private sources.

Data Centers

Facilities that store, manage and disseminate data and house a network's most critical systems. Data centers can serve either as a centralized facility for a single organization's data management functions or as a third-party provider for organization's data management needs.

Data Classification

A scheme that provides the basis for managing access to, and protection of, data assets.

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 Elements

A unit of data that cannot be broken down further or has a distinct meaning. This may be a date of birth, a numerical identifier, or location coordinates. In the context of data protection, it is important to understand that data elements in isolation may not be personal data but, when combined, become personally identifiable and therefore personal data.

Data Flow Diagrams

A graphical representation of the flow of data in an information system thus allowing the visualization of how the system operates to accomplish its purpose. DFDs are used both by systems analysts to design information systems and by management to model the flow of data within organizations.

Acronym(s): DFD

Data Integrity Board

Under the Privacy Act, federal agencies using computerized means to match data between electronic federal privacy record systems, or to match data from any federal system with non federal records, are required to create a DIB composed of senior officials and the agency's inspector general. The DIB shall, among other things: review, approve and maintain all matching programs; review all existing matching programs annually to determine compliance with laws, regulations, guidelines and agreements, and; assess the cost and benefits of the agreements.

Link to law: Privacy Act

Acronym(s): DIB

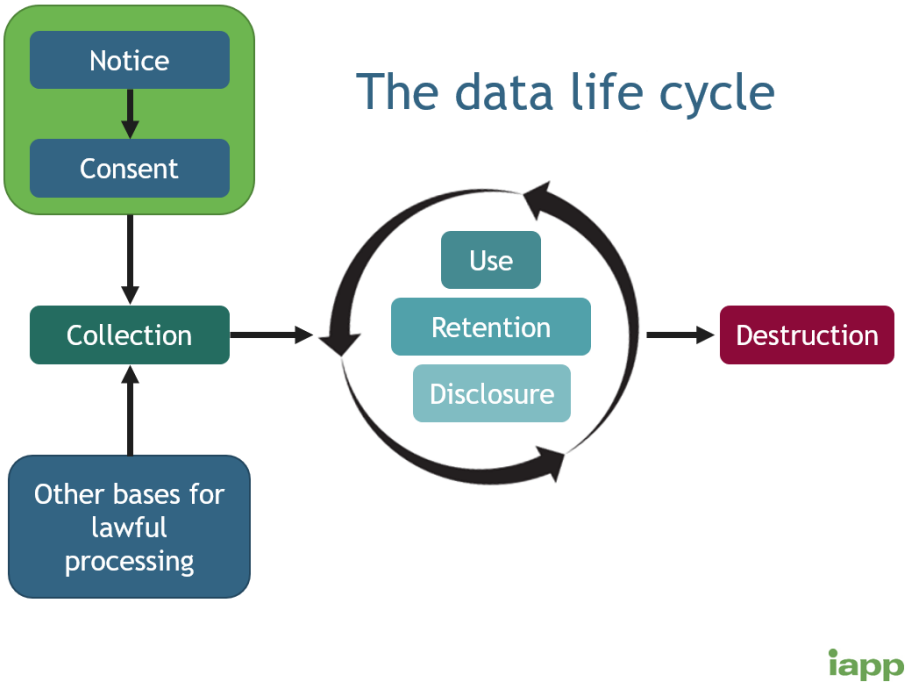
Associated term(s): Data Matching

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

This refers to how data is processed through an organization.



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 Loss Prevention

Term used to describe both the strategy for ensuring end users do not disseminate sensitive information, whether intentionally or unintentionally, to outside ineligible sources and the software products that aid network administrators in controlling what data end users can transfer.

Acronym: DLP

Data Masking

The process of de-identifying, anonymizing, or otherwise obscuring data so that the structure remains the same but the content is no longer sensitive in order to generate a data set that is useful for training or software testing purposes.

Associated term(s): Obfuscation

Data Matching
An activity that involves comparing personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the data pertains.

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

Link to text of law: Directive 95/46/EC

Link to text of law: Regulation EC (No) 45/2001

Data Minimization Principle (EU specific)
Data controllers must only collect and process personal data that is relevant, necessary and adequate to accomplish the purposes for which it is processed.

Data Portability
In certain circumstances, generally where data processing is done on the basis of consent or a contract, data subjects have the right to receive their personal data, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller without hindrance from the controller to which the personal data has been provided.

Data Processing
Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Associated term(s): Data Processor, Processing, Processor

Data Processor
A natural or legal person (other than an employee of the controller), public authority, agency or other body which processes personal data on behalf of the controller. An organization can be both a controller and a processor at the same time, depending on the function the organization is performing.

Associated term(s): Data Controller, Processor

Data Protection

The rules and safeguards applying under various laws and regulations to personal data about individuals that organizations collect, store, use and disclose. “Data protection” is the professional term used in the EU, whereas in the U.S. the concept is generally referred to as “information privacy.” Importantly, data protection is different from data security, since it extends beyond securing information to devising and implementing policies for its fair use.

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.

Acronym(s): DPA

Data Protection Authority (EU specific)

A term often used to refer to a supervisory authority (see Supervisory Authority), which is an independent public authority responsible for monitoring the application of the General Data Protection Regulation in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the European Union. DPAs also oversee other data protection-related laws, such as the ePrivacy Directive and other local member state laws.

Data Protection by Default

The implementation of appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. Such organizational measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, and enabling the data subject to monitor the data processing.

Data Protection by Design

When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.

Data Protection Commissioner

The title given in some member states to the supervisory authority (see Supervisory Authority).

Link to text of law: SI 535/2003

Associated term(s): Data Protection Authority

Data Protection Directive

See EU Data Protection Directive

Data Protection Impact Assessment

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.

Acronym (s): DPIA

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

Data Protection Officer

While the title of data protection officer has long been in use, particularly in Germany and France, the General Data Protection Regulation introduced a new legal defintion of a DPO with specific tasks. Certain organizations, particularly those that process personal data as part of their business model or those who process special categories of data as outlined in Article 9, are obligated to designate a DPO on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices. The DPO has a variety of mandated tasks, including communication with the supervisory authority, conducting DPIAs, and advising the organization on the mandates of the GDPR and how to comply with it.

Data Protection Policy

Data protection policies outline the basic contours of the measures an organization takes in the processing and handling of personal data. Key matters the policy should address include: Scope, which explains both to whom the internal policy applies and the type of processing activities it covers; Policy statement; Employee responsibilities; Management responsibilities; Reporting incidents; Policy compliance.

Data Protection Principles

Article 5 of the General Data Protection Regulation lists the principles as such: Lawfulness, fairness and transparency; Purpose limitation; Data minimisation; Accuracy; Storage limitation; Integrity and confidentiality.

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.

Data Quality (EU specific)

One of the General Data Protection Regulation's explicitly stated data protection principles, 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.

Data Quality Act of 2000

Passed in response to the increased use of the Internet by U.S. federal agencies, the act was designed to ensure the quality of information released by agencies by establishing four major requirements: (1) Office of Management and Budget was to issue guidelines "ensuring and maximizing the quality, objectivity, utility and integrity" of disseminated information; (2) agencies must issue their own sets of information quality guidelines; (3) agencies must establish administrative mechanisms for persons to correct erroneous information about themselves; (4) agencies must annually report to OMB regarding the number, nature and handling of complaints.

Link to text of law: Data Quality Act of 2000

Acronym(s): DQA

Associated term(s): Information Quality

Data Recipient

A natural or legal person, public authority, agency or another body, to which personal data is disclosed, whether a third party or not. Public authorities that receive personal data in the framework of a particular inquiry in accordance with EU or member state law shall not be regarded as recipients, however. The processing of that data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Data Retention Directive

The now-defunct Data Retention Directive was designed to align the rules on data retention across the EU member states in order to ensure the availability of traffic and location data for serious crime and antiterrorism purposes. The Data Retention Directive is no longer part of EU law, although member states retain competence to adopt their own national data retention laws under Article 15(1) of the ePrivacy Directive (2002/58/EC) provided that those laws comply with the fundamental rights principles that form part of EU law and the CJEU ruling that struck down the Data Retention Directive. Accordingly, EU member states have introduced draft legislative amendments or implemented national data retention laws at an individual country level.

Link to text of law: Directive 2006/24/EC

Data Sanitization

Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. Information disposition and sanitization decisions occur throughout the information system life cycle.

- Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques.
- Purge applies physical or logical techniques that render target data recovery infeasible using state-of-the art laboratory techniques.
- Destroy renders target data recovery (using state-of-the-art laboratory techniques) infeasible and results in the subsequent inability to use the media for storage of data.

Data schema

Used to separate customer information. Data schema formulates all the constraints to be applied on the data, defines its entities and relationships among them.

Data Subject

An identified or identifiable natural person.

De Novo

A Latin expression meaning “from the beginning,” “anew” or “beginning again.” In a legal context, a de novo hearing is one in which a higher authority can make a new decision, entirely ignoring the findings and conclusions of a lower authority.

De-identification

An action that one takes to remove identifying characteristics from data.

Acronym(s): De-ID

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

Deceptive Trade Practices

In the context of U.S. federal law, a term associated with corporate entities who mislead or misrepresent products or services to consumers and customers. These practices are regulated in the U.S. by the Federal Trade Commission at the federal level and typically by an attorney general or office of consumer protection at the state level. Law typically provides for both enforcement by the government to stop the practice and individual actions for damages brought by consumers who are hurt by the practices.

Associated term(s): Unfair Trade Practices

Link to text of law: U.S. Federal Trade Commission Act

Declared Data

Personal information that is directly given to a social network or other website by a user.

Associated term(s): Consent

Deep learning

A subset of artificial intelligence and machine learning. It learns by performing a tasks repeatedly and adding layers of data to improve the outcome.

Defamation

Common law tort focuses on a false or defamatory statement, defined as a communication tending “so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him.”

Associated term(s): Common Law

Demand Side Platform (DSP)

A company that allows advertising clients to buy digital media on several different selling systems, or exchanges, through one interface.

Demographic Advertising

Web advertising based on information about an individual such as age, height, weight, geographic location or gender.

Associated term(s): Behavioral Advertising, Contextual Advertising, Premium Advertising, Psychographic Advertising, Remnant Advertising.

Derogation

In the context of European Union legislation interacting with member state law, a derogation is a place in an EU-wide regulation where individual member states are left to make their own law or have the option to deviate. A derogation can also simply refer to an exception to a certain basic rule or principle.

Design patterns

Describes shared solutions to recurring problems. Design patterns serve to improve program code maintenance by providing developers with a common mental module when approaching a recurring problem.

Design Thinking Process

Used in combination with value-sensitive design. The design thinking process has five phases: empathize, define, ideate, prototype and test.

Differential identifiability

Setting parameters that limits the confidence that any particular individual has contributed to an aggregated value.

Digital Advertising Alliance

A non-profit organization that sets standards for consumer privacy, transparency and control in online advertising. Over 100 advertising companies participate in and comply with their standards. The DAA has an agreement with both the Council on Better Business Bureaus and the Direct Marketing Association to enforce the self-regulatory standards set down by the Digital Advertising Alliance including AdChoices, a programming offering user control over behavioral advertising.

Acronym: DAA

Associated term(s): AdChoices

Digital Fingerprinting

The use of log files to identify a website visitor. It is often used for security and system maintenance purposes. Log files generally include: the IP address of the visitor; a time stamp; the URL of the requested page or file; a referrer URL, and the visitor's web browser, operating system and font preferences. In some cases, combining this information can be used to "fingerprint" a device. This more detailed information varies enough among computing devices that two devices are unlikely to be the same. It is used as a security technique by financial institutions and others initiating additional security assurances before allowing users to log on from a new device. Some privacy enforcement agencies; however, have questioned what would constitute sufficient notice and consent for digital fingerprinting techniques to be used for targeted advertising.

Associated term(s): Biometric Data, Authentication, Authorization

Digital Rights Management

The management of access to and use of digital content and devices after sale. DRM is often associated with the set of access control (denial) technologies. These technologies are utilized under the premise of defending copyrights and intellectual property but are considered controversial because they may often restrict users from utilizing digital content or devices in a manner allowable by law.

Acronym(s): DRM

Digital Signature

A means for ensuring the authenticity of an electronic document, such as an e-mail, text file, spreadsheet or image file. If anything is changed in the electronic document after the digital signature is attached, the signature is rendered invalid.

Associated term(s): Authentication, Encryption

Direct Marketing

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

Direct Marketing (EU specific)

In the context of data protection law, direct marketing can be defined as personal data processed to communicate a marketing or advertising message. This definition includes messages from commercial organisations, as well as from charities and political organisations. While direct marketing is offered in the General Data Protection Regulation as an example of processing for the legitimate interest of an organization, it also says the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Directive on Privacy and Electronic Communications Act 2002/58EC

A continuation of policy directives for the European Union Member States as set forth in the Data Protection Directive. It has been amended by the Cookie Directive 2009/136EC, which added a requirement that all websites using tracking cookies obtain user consent unless the cookie is "strictly necessary for the delivery of a service requested by the use." This policy recognizes the importance of cookies for the functioning of modern websites while still making users aware of any tracking the user may not want to participate in.

Link to text of law: Directive on Privacy and Electronic Communications Act 2002/58EC

Acronyms: ePrivacy Directive, Cookie Directive

Associated term(s): Data Protection Directive

Disassociability

Minimization of connections between data and individuals to the extent compatible with system operational requirements.

Disclosure

The provision of access to personal data.

Discretionary Access Control

A type of access control that allows an owner of an object, within a given computer-based information system, to grant or deny access.

Acronym(s): DAC

Associated term(s): Mandatory Access Control

Dispute Resolution

In the context of the consistency mechanism (see Consistency Mechanism), the European Data Protection Board can issue binding decisions on objections to lead authority decisions, on disputes about which supervisory authority should be the lead authority, and where there has been a failure to request the EDPB's opinion under Article 64 or the opinion is not followed.

Distortion

Spreading false and inaccurate information about an individual.

DMZ (Demilitarized Zone) Network

A firewall configuration for securing local area networks (LANs). In a DMZ configuration, there are a set of computers that act as a broker for traffic between the LAN and an outside network allowing the majority of computers to run safely behind a

firewall. Thus these computers act as a broker similar to a joint security area in a political demilitarized zone.

Do Not Track

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.

Acronym(s): DNT

Do Not Track

A catch-all term for various technologies and browser settings designed to allow data subjects to indicate their objection to tracking by websites. Years of effort, by the W3C and other organizations, to create an official Do Not Track standard for HTTP headers has of yet led to naught.

Acronym(s): DNT

Do-Not-Call Implementation Act of 2003

Grants the authority to the Federal Trade Commission to create the National Do-Not-Call Registry in the United States. The registry is open to all consumers, allowing them to place their phone numbers on a national list which makes it illegal for telemarketers to make unsolicited calls to those numbers, the only exceptions being for political activities and non-profit organizations. Originally consumers would have to re-register their numbers with the FTC every five years for continued prevention, but the Do-Not-Call Improvement Act of 2007 extended registration indefinitely. Violations can be enforced by the FTC, Federal Communications Commission, and state attorneys general with up to a $16,000 fine per violation.

Associated term(s): Federal Trade Commission, Federal Communication Commission, Do-Not-Call Improvement Act, National Do-Not-Call Registry

Do-Not-Call Improvement Act of 2007

Amending the U.S. Do-Not-Call Implementation Act to remove the re-registration requirement. Originally registration with the National Do-Not-Call Registry ended after five years, but with this act the registrations became permanent.

Associated term(s): Federal Trade Commission, Federal Communications Commission, Do-Not-Call Implementation Act, National Do-Not-Call Registry

Dodd-Frank Wall Street Reform and Consumer Protection Act

In 2010 the U.S. Congress passed the Dodd-Frank Act to reorganize and improve financial regulation. Among other reforms it put in place, the Dodd-Frank Act created the Consumer Financial Protection Bureau and granted it rule-making authority over FCRA and GLBA as well as a few other regulations.

Link to text of law: Dodd-Frank Wall Street Reform and Consumer Protection Act

Associated law(s): Gramm-Leach-Bliley Act, Fair Credit Reporting Act, Consumer Financial Protection Bureau

Durant v. Financial Services Authority

A court case in which the Court of Appeal of the United Kingdom narrowed the definition of personal data under the Data Protection Act of 1998. It established a two-stage test; the information must be biographical in a significant sense and the individual must be the focus of the information.

Link to text of case: Durant v. Financial Services Authority

E-Authentication

To address the rise in citizen use of the Internet to access government information and services, some type of identity verification or authentication is needed. As such, agencies are required to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance.

Associated term(s): Authorization

E-Commerce Websites

Websites with online ordering capabilities have special privacy advantages and risks. Unlike other web advertisers, E-Commerce websites have direct access to information regarding user purchases and payment information. While creating a great opportunity for targeted advertising, it also puts extra onus on these websites to protect user information.

E-Government Act

A U.S. federal law that, among other things, requires federal agencies to conduct Privacy Impact Assessments on new or substantially revised information technology.

Link to text of law: E-Government Act

Associated law(s): FISMA

Electronic Communications Data

Consists of three main categories of personal data, as defined in the European Union under the ePrivacy Directive: the content of a communication, traffic data, and location data.

Electronic Communications Network

Transmission systems, and, where applicable, switching or routing equipment and other resources that permit the conveyance of signals by wire, radio, optical or other

electromagnetic means, including satellite networks; fixed and mobile terrestrial networks; electricity cable systems, to the extent that they are used for the purpose of transmitting signals; networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. In the discussions surrounding the update of the ePrivacy Directive to the ePrivacy Regulation, so-called "over the top" providers, like app-based messaging services, are beginning to be considered as part of the electronic communications network.

Acronym(s): ECN

Electronic Communications Privacy Act 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.

Link to text of law: Electronic Communications Privacy Act of 1986

Acronym(s): ECPA

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

Electronic Communications Service

Any service which provides to users thereof the ability to send or receive wire or electronic communications.

Acronym(s): ECS

Electronic Discovery

Prior to trial, information is typically exchanged between parties and their attorneys. E-discovery requires civil litigants to turn over large volumes of a company’s electronic records in litigation.

Associated term(s): Electronically stored information (ESI), Sedona Conference

Associated law(s): Federal Rules of Civil Procedure

Electronic Health Record

A computer record of an individual's medical file that may be shared across multiple healthcare settings. In some cases this sharing can occur by way of network-connected enterprise-wide information systems and other information networks or exchanges.

EHRs may include a range of data including demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal stats such as age and weight and billing information. Their accessibility and standardization can facilitate large-scale data collection for researchers.

Acronym(s): EHR

Associated law(s): HIPAA, HITECH

Electronic Surveillance

Monitoring through electronic means; i.e., video surveillance, intercepting communications, stored communications or location based services.

Associated law(s): Electronic Communications Privacy Act, Stored Communications Act, Wiretap Act

Employee Information

Personal information reasonably required by an organization that is collected, used or disclosed solely for the purposes of establishing, managing or terminating; (1) an employment relationship, or (2) a volunteer work relationship between the organization and the individual but does not include personal information about the individual that is unrelated to that relationship.

Employee Personal Data

Article 88 of the General Data Protection Regulation recognises that member states may provide for more specific rules around processing employees' personal data. These rules must include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the workplace. Because of the power imbalance between employer and employee, consent is generally not considered a legal basis for processing employee data.

Employment at Will

An employment contract can be terminated by either the employer or the employee at any time for any reason.

Encryption

The process of obscuring information, often through the use of a cryptographic scheme in order to make the information unreadable without special knowledge; i.e., the use of code keys. Encryption is mentioned in the General Data Protection Regulation as a potential way to mitigate risk, and certain breach notification requirements may be mitigated by the use of encryption as it reduces the risks to the rights and freedoms of data subjects should data be improperly disclosed.

Encryption Key

A cryptographic algorithm applied to unencrypted text to disguise its value or to decrypt encrypted text.

End-User License Agreement

A contract between the owner of the software application and the user. The user agrees to pay for the use of the software and promises to comply with certain restrictions on that use.

Acronym(s): EULA

Associated term(s): Terms of Service

Enterprise Architecture

A conceptual outline, blueprint, or diagram that defines the structure and the operation of an organization, normally in the context of developing a strategy for the realization of current and future goals or objectives.

Acronym(s): EA

Associated term(s): IT Architecture

Enterprise Mobility Management (EMM)

EMM refers to a comprehensive organizational strategy for securing and enabling employee use of mobile devices such as smartphones and tablets. EMMs are used to prevent unauthorized access to applications containing corporate data on mobile devices, usually through the use of password protection, encryption and remote wiping technology.

ePrivacy Directive

A sectoral privacy directive for European Union Member States, which applies to the digital industry. Among other provisions, the ePrivacy Directive requires websites to obtain consumer consent before placing cookies for marketing purposes. The EU is currently considering reform of the ePrivacy Directive.

Equal Employment Opportunity Commission, The

An independent U.S. federal agency that enforces laws against workplace discrimination. The EEOC investigates discrimination complaints based on an individual's race, color, national origin, religion, sex, age, perceived intelligence, disability and retaliation for reporting and/or opposing a discriminatory practice. It is empowered to file discrimination suits against employers on behalf of alleged victims and to adjudicate claims of discrimination brought against federal agencies.

Link to: Equal Employment Opportunity Commission

Acronym(s): EEOC

Erasure

Article 17(1) of the GDPR establishes that data subjects have the right to erasure of their personal data if: the data is no longer needed for its original purpose and no new lawful purpose exists; the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; the data has been processed unlawfully; or erasure is necessary for compliance with EU law or the national law of the relevant member state.

Established Business Relationship

An exemption to the Do Not Call (DNC) registry, a marketer may call an individual on the DNC registry if a prior or existing relationship formed by a voluntary two-way communication between a person or entity and a residential subscriber with or without an exchange of consideration, on the basis of an inquiry, application, purchase or transaction by the residential subscriber regarding products or services offered by such person or entity, which relationship has not been previously terminated by either party.

Associated term(s): Established customer relationship

Established Service Provider

The GDPR establishes direct legal obligations applicable to service providers acting as "processors" (see Processor), whilst giving an increased emphasis to the contractual obligations in place between customers and data processing service providers.

Establishment

Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect (see Main Establishment).

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

EU Data Retention Directive

See Data Retention Directive

EU-U.S. Safe Harbor Agreement

An agreement between the European and United States, invalidated by the Court of Justice of the European Union in 2015, that allowed for the legal transfer of personal data between the EU and U.S. in the absence of a comprehensive adequacy decision for the United States (see Adequacy). It was replaced by the EU-U.S. Privacy Shield in 2016 (see Privacy Shield).

EU-US Privacy Shield

Created in 2016 to replace the invalidated U.S.-EU Safe Harbor agreement, the Privacy Shield is a data transfer mechanism negotiated by U.S. and EU authorities that received an adequacy determination from the European Commission that allowed for the transfer of personal data from the EU to the United States for companies participating in the program. Only those companies that fell under the jurisdiction of the U.S. Federal Trade Commission could certify to the Shield principles and participate, which notably excludes health care, financial services, and non-profit institutions. On July 16, 2020, the Court of Justice of the European Union invalidated the European Commission's adequacy determination for Privacy Shield.

European Commission

The executive body of the European Union. Its main function is to implement the EU's decisions and policies, along with other functions. It initiates legislation in the EU, proposing initial drafts that are then undertaken by the Parliament and Council of the European Union. It is also responsible for making adequacy determinations with regard to data transfers to third-party countries.

European Convention on Human Rights

A European convention that sought to secure the recognition and observance of the rights enunciated by the United Nations. The Convention provides that "(e)veryone has the right to respect for his private and family life, his home and his correspondence." Article 8 of the Convention limits a public authority's interference with an individual's right to privacy, but acknowledges an exception for actions in accordance with the law and necessary to preserve a democratic society. This created the Council of Europe (see Council of Europe) and the European Court of Human Rights (see European Court of Human Rights).

Link to text of law: European Convention on Human Rights

European Council

The European Council is the collection of heads of states of European Union member states. It provides general political direction for the EU and does not exercise legislative functions.

Link to: European Council

European Court of Human Rights

The European Court of Human Rights (ECHR) in Strasbourg, France, upholds privacy and data protection laws through its enforcement of the European Convention on Human Rights and Convention 108. The ECHR applies the Convention and ensures that signatory states respect the rights and guarantees set out in the Convention.

Acronym(s): ECHR

Link to: European Court of Human Rights

European Data Protection Board

The successor to the Article 29 Working Party, it consists of the heads of the supervisory authorities of the member states and the European Data Protection Supervisor (see European Data Protection Supervisor), and the Commission is entitled to send a delegate to its meetings. The EDPB's role is to ensure the consistent application of the Regulation and, in addition to supporting cooperation between the regulators and applying the consistency mechanism (see Consistency Mechanism), it shall publish advice, guidance, recommendations and best practices. The supervisory authorities elect a chairperson, with certain powers, from amongst their membership.

Acronym(s): EDPB

European Data Protection Supervisor

The data protection regulator for the European Union as an entity, ensuring the EU institutions, such as the Parliament, Commission, and Council of the European Union, protect the rights and freedoms of data subjects. The EDPS acts as secretariat to the European Data Protection Board (see European Data Protection Board).

Link to: European Data Protection Supervisor

Acronym(s): EDPS

Associated law(s): Regulation (EC) No 45/2001

European Economic Area

An economic region that includes the European Union (EU) and Iceland, Norway and Liechtenstein—which are not official members of the EU but are closely linked by economic relationship. Non-EU countries in the EEA are required to adopt EU legislation regarding the single market.

Link to: European Economic Area

Acronym(s): EEA

European Economic Community

Created by the Treaty of Rome, the EEC was a predecessor to the European Union that promoted a single economic market across Europe.

Link to text of treaty: European Economic Community

Associated term(s): The Common Market

European Parliament

The only EU institution whose members are directly elected by citizens of individual member states, Parliament has four responsibilities—legislative development, supervisory oversight of other institutions, democratic representation and budget development.

Link to: European Parliament

Acronym(s): MEP (MEP stands for Member of European Parliament) - not an acronym for Parliament itself.

European Union

The European Union replaced the EEC, which was created by the Treaty of Rome and first promoted a single economic market across Europe. The EU currently comprises 28 member states: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. The U.K. is currently slated to leave the European Union in March 2019.

Acronym(s): EU

Exclusion

Denies an individual knowledge of and/or participation in what is being done with their information.

Executive Order 12333

The order that provides information about the goals, direction, duties and responsibilities with respect to the national intelligence effort and provides basic information on how intelligence activities should be conducted. The executive order states that agencies within the intelligence community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with

procedures established by the head of the agency concerned, and must be approved by the attorney general.

Link to text of law: Executive Order 12333

Exposure

The revelation of information that we normally conceal from most others, including private physical details about our bodies.

Extensible Markup Language

A markup language that facilitates the transport, creation, retrieval and storage of documents. Similar to HTML, XML uses tags to describe the contents of a web page or file. XML describes content of a web page in terms of the data that is being produced, potentially creating automatic processing of data in ways that may require attention for privacy issues, unlike HTML, which describes the content of a web page in terms of how it should be displayed.

Acronym(s): XML

Extranet

A network system formed through the connection of two or more corporate intranets. These external networks create inherent security risks, while often also meeting important organizational goals. An extranet opens a backdoor into the internal network and provides a third party with a level of trust. While these risks cannot be eliminated, they can be assessed, managed and mitigated. The foundation of this management is a thorough and detailed e-business contract that specifies who may access data, what data will be accessed and what security controls the partner has in place. It should also detail how shared devices will be managed, procedures for cooperating with technical staff in the event of problems and escalation procedures for resolving difficult technical problems.

Factors Analysis in Information Risk (FAIR) model

FAIR constructs a framework that breaks risk into the frequency of action and magnitude of the violations.

Factortame

A 1989 case brought before the European Court of Justice which established the precedence of EU law over national laws of member states in areas where the EU has competence.

Link to decision: The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and others

Fair and Accurate Credit Transactions Act of 2003

An expansion of the Fair Credit Reporting Act which focuses on consumer access and identity theft prevention. The act mandates that credit reporting agencies allow consumers to obtain a free credit report once every twelve months. Additionally, it allows consumers to request alerts when a creditor suspects identity theft and gave the Federal Trade Commission (FTC) authority to promulgate rules to prevent identity theft. The FTC used the authority to create the Red Flags Rule.

Link to text of law: Fair and Accurate Credit Transactions Act of 2003

Acronym(s): FACTA, FACT Act

Associated term(s): Red Flags Rule

Associated law(s): Fair Credit Reporting Act

Fair Credit Reporting Act, The

One of the oldest U.S. federal privacy laws still in force today. It was enacted in 1970 to mandate accurate and relevant data collection, give consumers the ability access and correct their information, and limit the use of consumer reports to permissible purposes, such as employment and extension of credit or insurance.

Link to text of law: The Fair Credit Reporting Act

Acronym(s): FCRA

Associated law(s): Fair and Accurate Credit Transactions Act of 2003 (FACTA)

Fair Information Practice Principles

(1) The Collection Limitation Principle. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

(2) The Data Quality Principle. Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

(3) The Purpose Specification Principle. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

(4) The Use Limitation Principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except a) with the consent of the data subject, or b) by the authority of law.

(5) The Security Safeguards Principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

(6) The Openness Principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing 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.

(7) The Individual Participation Principle. 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 him;

b) to have data relating to him communicated to him, 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 him;

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 him and, if the challenge is successful, to have the data erased, rectified, completed or amended;

(8) The Accountability Principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Acronym(s): FIPPs

Fairness

One of three requirements established by the General Data Protection Regulation for the processing of personal data: The first principle of processing personal data is "lawfulness, fairness, and transparency," which states that personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject. Linked most often with transparency, fairness means data subjects must be aware of the fact that their personal data will be processed, including how the data will be collected, kept and used, to allow them to make an informed decision about whether they agree with such processing and to enable them to exercise their data protection rights. Consent notices should not contain unfair terms and supervisory authority powers should similarly be exercised fairly.

Associated term(s): Data Controller, Lawfulness

Associated law(s): EU Data Protection Directive

Family Educational Rights and Privacy Act

FERPA establishes requirements regarding the privacy protection of student educational records. It applies to all academic institutions that receive funds under applicable U.S. Department of Education programs. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are referred to as "eligible students."

Link to text of law: Family Educational Rights and Privacy Act

Acronym(s): FERPA

Federal Advisory Committee Act, The

A federal law governing the behavior of federal advisory committees, restricting the formation of such committees to those deemed essential, limiting their powers and their length of operation, requiring open meetings and open records and mandating a publicly-accessible government-wide database.

Link to text of law: Federal Advisory Committee Act

Acronym(s): FACA

Federal Agency Data Mining Reporting Act

A federal law requiring agencies found of data mining to submit a yearly report to Congress. The privacy office of that agency must be involved in producing the report. The report will be made public and describe all of the agency's data-mining activity, goals and an assessment of the effectiveness of the data mining activity.

Link to text of law: Federal Agency Data Mining Reporting Act

Federal Communications Commission

The United States agency that regulates interstate communications through radio, wire, telecommunications, satellite and cable. The Federal Communications Commission has authority that overlaps with the Federal Trade Commission in some areas of privacy law including enforcement and further regulation under the Telephone Consumer Protection Act.

Acronym: FCC

Associated term(s): Federal Trade Commission, Do-Not-Call Implementation Act, Do-Not-Call Improvement Act, Telephone Consumer Protection Act, Junk Fax Prevention Act

Federal Enterprise Architecture Security and Privacy Profile

The FEA-SPP serves two functions in the integration of privacy and security risk-management practices. First, it clearly articulates that while there is a symbiotic relationship between security and privacy, these practices are not identical; they are distinct practices, but intertwined. Second, the FEA-SPP lays the groundwork for driving agency integration of privacy risk management into the fundamental design of technical systems and technologies.

Link to text of law: Federal Enterprise Architecture Security and Privacy Profile

Acronym(s): FEA-SPP

Federal Information Security Incident Center

FISMA codified a federal information security center, which is implemented in the U.S. Computer Emergency Readiness Team (US-CERT). U.S.-CERT is called upon to provide timely technical assistance regarding security incidents; compile and analyze security incident information; inform federal agency information system operators about current and potential threats, and consult with NIST and others regarding information security incidents.

Acronym(s): FISIC

Associated term(s): U.S. Computer Emergency Readiness Team (US-CERT), National Institute of Standards and Technology (NIST)

Associated law(s): FISMA

Federal Information Security Management Act of 2002, The

A U.S. federal law enacted as part of the E-Government Act of 2002. The act requires each federal agency to develop, document and implement an agency-wide program to provide information security for the data and data systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor or other source. FISMA requires agency program officials, chief information officers and inspectors general to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget. OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. In FY 2008, federal agencies spent $6.2 billion securing the government's total information technology investment of approximately $68 billion or about 9.2 percent of the total information technology portfolio.

Link to text of law: Federal Information Security Management Act of 2002

Acronym(s): FISMA

Federal Records Act

The Federal Records Act requires the establishment of standards and procedures to ensure efficient and effective records management. The objectives of the Federal Records Act interact with federal privacy to: Ensure appropriate maintenance of a record that allows access rights to subject of the record; Minimize the collection of PII; Ensure the destruction of PII when there is no longer a business, legal, or historical need for the record.

Link to text of law: Federal Records Act

Associated term(s): PII

Associated law(s): Privacy Act

Federal Trade Commission

The United States' primary consumer protection agency, the FTC collects complaints about companies, business practices and identity theft under the FTC Act and other laws that they enforce or administer. Importantly, the FTC brings actions under Section 5 of the FTC Act, which prohibits unfair and deceptive trade practices.

Acronym(s): FTC

Associated law(s): FTC Act

Federal Trade Commission Act, Section 5 of

Section 5(a) of the FTC Act empowers the agency to enforce against "unfair or deceptive acts or practices in or affecting commerce." Over the past two decades, the FTC has used this authority extensively to hold businesses to fair and transparent privacy and security standards.

Federated identity

A model in which a person's identity is authenticated in a trusted centralized service.

Final Health Breach Notification Rule

A rule, promulgated under HITECH, requiring vendors of personal health records and related entities to notify consumers when the security of their individually identifiable health information has been breached.

Associated law(s): HITECH

Financial Industry Regulatory Authority

A corporation that acts as a regulator for brokerage firms and exchange markets. Its primary charge is to make sure that security exchange markets, such as the New York Stock Exchange, operate fairly and honestly and to protect investors. Although it is a non-governmental regulator, ultimately it is subject to the regulations of the Securities and Exchange Commission along with the rest of the security exchange industry.

Link to: FINRA

Acronym: FINRA

Associated law(s): Dodd-Frank Act, Gramm-Leach-Bliley Act

Financial Institutions Reform, Recovery, and Enforcement Act of 1989

After the savings and loans crisis of the 1980s, the U.S Congress passed FIRREA to enable financial regulators to levy penalties up to $5,000,000 for failure to comply with regulations. These penalties can be levied if a Financial institution fails to comply with the information privacy requirements contained in GLBA.

Link to text of law: Financial Institutions Reform, Recovery, and Enforcement Act of 1989

Acronym: FIRREA

Associated law(s): Gramm-Leach-Bliley Act

Financial Instruments and Exchange Law of Japan

Japanese legislation aimed at the financial services sector that established cross-sectional legislative framework for investor protections, enhanced disclosure requirements, provided guidelines for the management of self-regulatory operations by financial exchanges, and implemented strict countermeasures against unfair trading.

Link to text of law: Financial Instruments and Exchange Law of Japan

First-Party Collection

A data subject provides personal data to the collector directly, through a form or survey that is sent to the collector upon the data subject submitting the information

Associated term(s): Active Collection, Passive Collection, Surveillance Collection, Repurposing, Third-party Collection

Five-Step Metric Life Cycle

See Metrics

Flash

Software that is used to add animation and other visual effects to web-based content.

Foreign Intelligence Surveillance Act of 1978, The

A U.S. federal law regulating the way that U.S. intelligence agencies conduct foreign intelligence surveillance activities, including wiretaps and the interception of communications. The act sets forth a judicial approval process required when the government targets U.S. persons located within the United States. FISA allows warrantless surveillance to be conducted without a court order for up to one year, provided the surveillance is for foreign intelligence information, is targeting foreign powers and will not capture the contents of any communication to which a U.S. person is a party. Generally speaking, FISA does not apply to activities directed at persons overseas.

Link to text of law: Foreign Intelligence Surveillance Act of 1978

Acronym(s): FISA

Freedom of Information Act, The

A U.S. federal law that ensures citizen access to federal government agency records. FOIA only applies to federal executive branch documents. It does not apply to legislative or judicial records. FOIA requests will be fulfilled unless they are subject to nine specific exemptions. Most states have some state level equivalent of FOIA. The federal and most state FOIA statutes include a specific exemption for personal information so that sensitive data (such as Social Security numbers) are not disclosed.

Link to text of law: The Freedom of Information Act

Acronym(s): FOIA

Freely Given

The General Data Protection Regulation requires that consent be a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject must have a genuine choice, must be able to refuse or withdraw consent without fear of consequence. Where there is a power imbalance, as in an employer-employee relationship, for example, it's likely that consent cannot be freely given.

Frequency data

The number of times a data value occurs.

Functional System Requirements

Specific details about how a system should work, what inputs create what outputs, and design elements to be implemented. For example, "A system shall do processing of personal information to create user profiles."

Associated term(s): Plan-driven Development Model, Agile Development Model, SRS, User Stories, Non-functional System Requirements

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.

Gaskin v. United Kingdom

A judgment delivered by the European Court of Human Rights in 1989,in Gaskin v. United Kingdom, held that the restriction of the applicant's access to his personal file was contrary to Article 8 of the Convention, citing a breach of Gaskin's right to respect for his family and private life.

Link to text of case: Gaskin v. United Kingdom

General Data Protection Regulation

The General Data Protection Regulation (GDPR) replaced the Data Protection Directive in 2018. The aim of the GDPR is to provide one set of data protection rules for all EU member states and the European Economic Area (EEA). The document comprises 173 recitals and 99 articles.

Acronym: GDPR

Generally Accepted Privacy Principles

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.

Acronym(s): GAPP

Geo-social patterns

Data from smartphones and other devices that provide information regarding mobility and social patterns and behaviors. Individuals share information such as emotions, opinions, experiences and locations; generating a data about human activity via artificial intelligence and machine learning which allows for meaningful patterns and trends to be surmised.

Geocoding

The process of assigning geographic coordinates to non-locational data so that they can be placed as points on a map. For example, geocoding could be used to translate a street address (which describes a location) into precise coordinates that identify the location on a map.

Geofencing

Geofencing is the creation of virtual perimeters linked to the geographic position of a mobile device. In the BYOD context, geofencing may be used to restrict access to applications or sensitive information inside of or outside of specific locations. For example, a company may be able to restrict access to potentially risky applications on a personal device when the device is connected to the company's network or, conversely,

restrict access to company resources when the device is outside of the company's network.

Geotagging

The process of adding geographical information to various media in the form of metadata, such as latitude and longitude coordinates or city and state details for the location of a photo or social media post.

Geotargeting

The practice of customizing an advertisement for a product or service to a specific market based on the geographic location of potential customers.

GET Method

The GET and POST HTML method attributes specify how form data is sent to a web page. The GET method appends the form data to the URL in name/value pairs allowing passwords and other sensitive information collected in a form to be visible in the browser's address bar, and is thus less secure than the POST method.

Associated term(s): POST Method

Global Privacy Enforcement Network

Organized following an OECD recommendation for cooperation among member countries on enforcement of privacy laws, GPEN is collection of data protection authorities dedicated to discussing aspects of privacy law enforcement cooperation, the sharing of best practices, development of shared enforcement priorities, and the support of joint enforcement initiatives and awareness campaigns. As of 2018, GPEN counted 50 member countries.

Acronym(s): GPEN

Globally Unique Identifier

An identifier that is one of a kind to a specific user. For example, biometric data or a loginID for a social network.

Acronym(s): GUID

Associated term(s): Authentication, Authorization, Identifiability, Identifiers.

Government in the Sunshine Act

The Government in the Sunshine Act, 5 U.S.C. § 552b, generally requires multi-member federal agencies; i.e., the FCC and SEC, to hold their meetings in public and to give advance public notice of their meetings. The goal of the Sunshine Act is to promote

public access to information about the decision-making processes of the federal government and to improve those processes by exposing them to public view.

Link to text of law: 5 U.S.C. § 552b

Acronym(s): GSA

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.

Link to text of law: Gramm-Leach-Bliley Act

Acronym(s): GLBA

Haralambie v. Romania

The European Court of Human Rights decided in 2009 that Haralambie's Article 8 right to respect for private life and family life had been violated when the applicant sought access to the secret service file on him drawn up in the days of Communist rule in Romania and was made to wait six years. The court awarded 6,000 euros.

Link to case summary: Haralambie v. Romania

Harm Dimensions

University of Washington associate professor of law, Ryan Calo, identified two dimensions of privacy harms: objective and subjective. The perception of harm is just as likely to have a significantly negative impact on individual privacy as experienced harms.

Hashing Functions

Or "hashing" is taking user identifications and converting them into an ordered system to track the user's activities without directly using personally identifiable information (PII). Hashing can be used to encrypt or map data; in the context of privacy, hashing is used in cryptographic hash functions and have many information security applications.

Associated term(s): Anonymous Information, Pseudonymous Data, De-Identification, Re-Identification

Health Breach Notification Rule

A rule in the United States, promulgated under HITECH, requiring vendors of personal health records and related entities to notify consumers when the security of their individually identifiable health information has been breached.

Link to text of rule: Health Breach Notification Rule

Associated law(s): HITECH

Health Information Technology for Economic and Clinical Health Act, The

Enacted as part of the American Recovery and Reinvestment Act of 2009, the HITECH Act, among other objectives, further addresses privacy and security issues involving PHI as defined by HIPAA. The HITECH privacy provisions include the introduction of categories of violations based on culpability that, in turn, are tied to tiered ranges of civil monetary penalties. Its most noteworthy elements elaborate upon breach notifications resulting from the use or disclosure of information that compromises its security or privacy.

Link to text of law: HITECH Act

Associated term(s): EHR

Associated law(s): HIPAA

Health Insurance Portability and Accountability Act, The

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.

Link to text of law: The Health Insurance Portability and Accountability Act

Acronym(s): HIPAA

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

Hide

Personal information is made un-connectable or un-observable to others.

High level design

How the system's part, both front end and back end work together to implement the behaviors that a system should exhibit.

High-level design

How the system's part, both front end and back end work together to implement the behaviors that a system should exhibit.

Honeypot

Honeypot is an Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system.

A firewall in a honeypot works in the opposite way that a normal firewall works: instead of restricting what comes into a system from the Internet, the honeypot firewall allows all traffic to come in from the Internet and restricts what the system sends back out.

By luring a hacker into a system, a honeypot serves several purposes:

- The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned.
- The hacker can be caught and stopped while trying to obtain root access to the system.
- By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

A network of honeypots is often called a honeynet.

Homomorphic

Allows encrypted information to be manipulated without first being decrypted.

House of Commons

One of two chambers of the Canadian Parliament, along with the Senate. Members of the House of Commons are elected at least every five years.

HTML

See Hypertext Markup Language

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 fulfill and support the policies and directives from the central governing body.

Hyperlink

Linked graphic or text that is used to connect an end user to other websites, parts of websites or web-enabled services. The URL of a web location is embedded in the HTML

code, so that when certain words or images are selected through the web browser, the end user is transported to the destination website or page.

Hypertext Markup Language (HTML)

A content authoring language used to create web pages. Web browsers use HTML to interpret and render visible and audible content from the web pages. Document "tags" can be used to format and lay out web page content and to "hyperlink"—connect dynamically—to other web content. Forms, links, pictures and text may all be added with minimal commands. Headings are also embedded into the text and are used by web servers to process commands and return data with each request.

Acronym(s): HTML

Associated term(s): HTTP, HTTPS

Hypertext Transfer Protocol

A networking language that manages data packets over the Internet. It defines how messages are formatted and transmitted over a TCP/IP network for websites. Further, it defines what actions Web servers and web browsers take in response to various commands.

Acronym(s): HTTP

Associated term(s): HTML, HTTPS

Hypertext Transfer Protocol Secure

A secure network communication method, technically not a protocol in itself, HTTPS is the result of layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

Acronym(s): HTTPS

Associated term(s): HTTP, SSL/TLS

Identifiability

The degree to which a user is identified by an authentication system. The more unique (identifiable), the easier that user is tracked or targeted. The less identifiable, the easier it is to falsely authorize a non-user.

Associated term(s): Authentication, Authorization

Identifiers

Codes or strings used to represent an individual, device or browser.

Associated term(s): Authentication, Authorization, Identifiability, GUID

Identifying Purposes

Integral to privacy protection is the obligation on organizations to identify and document the purposes for the collection of any personal information at or before the time of collection.

Individual Access

One of 10 privacy principles of PIPEDA. Organizations must be able to respond to requests from individuals for access to their personal information.

Associated law(s): PIPEDA

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 Banks

Repositories of personal information that are kept by the Canadian government to comply with the Privacy Act.

Associated law(s): The Canadian Privacy Act

Information governance

Choreography of all stakeholders involved in the processing of personal data: technical solutions, privacy compliance, security measures.

Information hiding

Identifies data that has been assigned to specific levels of classification and restrict access tot hat data via limited class functions.

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 Privacy

One of the four classes of privacy, along with territorial privacy, bodily privacy, and communications privacy. The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.

Information Security

The protection of information for the purposes of preventing loss, unauthorized access and/or misuse. It is also the process of assessing threats and risks to information and the procedures and controls to preserve confidentiality, integrity and availability of information.

Acronym(s): IS

Information Security Practices

Provide 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

Information Sharing Environment

The ISE is a conceptual framework for facilitating the sharing of terrorism-related information among federal, state, local and tribal agencies, the private sector, and foreign partners. The ISE was mandated by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). ISE guidance includes steps that ensure the information privacy and other legal rights of Americans are protected in the development and use of the information-sharing environment. The ISE privacy guidelines provide high-level direction on protecting privacy. The guidelines apply to information about U.S. citizens and lawful permanent residents.

Acronym(s): ISE

Associated law(s): Intelligence Reform and Terrorism Prevention Act

Information Utility

The culture and desire of a business that seeks to use information collected by a company in every way possible to improve services and products. This needs to be balanced with privacy considerations.

Insecurity

Results from failure to properly protect individuals' information.

Integrity

The General Data Protection Regulation requires that controllers and processors implement measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. Integrity refers to the consistency, accuracy and trustworthiness of the data (see Accuracy).

Interactive Advertising Bureau

A trade association representing advertising businesses. The IAB develops industry standards, conducts research, and provides legal support for the online advertising industry.

Link to: Interactive Advertising Bureau

Acronym(s): IAB

Internal Partners

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

Internet of Things

A term used to describe the many devices that are connected to the internet. Any device that is built with a network interface can be assigned an IP address to allow for automation and remote access.

Internet Protocol Address

A unique string of numbers that identifies a computer on the Internet or other TCP/IP network. The IP address is expressed in four groups of up to three numbers, separated by periods. For example: 123.123.23.2. An address may be "dynamic," meaning that it is assigned temporarily whenever a device logs on to a network or an Internet service provider and consequently may be different each time a device connects. Alternatively, an address may be "static," meaning that it is assigned to a particular device and does not change, but remains assigned to one computer or device.

Acronym(s): IP Address

Internet Protocol Address (EU specific)

Listed within the General Data Protection Regulation as a form of personal information, a unique string of numbers that identifies a computer on the Internet or other TCP/IP network. The IP address is expressed in four groups of up to three numbers, separated by periods. For example: 123.123.23.2. An address may be "dynamic," meaning that it is assigned temporarily whenever a device logs on to a network or an Internet service provider and consequently may be different each time a device connects. Alternatively, an address may be "static," meaning that it is assigned to a particular device and does not change, but remains assigned to one computer or device.

Acronyms: IP Address

Internet Service Provider

A company that provides Internet access to homes and businesses through modem dial-up, DSL, cable modem broadband, dedicated T1/T3 lines or wireless connections.

Acronym(s): ISP

Interrogation

When the line of questioning or probing individuals for personal information is not aligned with the context of the situation and a person feels compelled to answer, social norms are breached and individual privacy is at risk.

Intrusion Detection System

A system that inspects network activity and identifies suspicious patterns that may someone is attempting to penetrate or compromise a system or network. An IDS: may be network-based or host-based; signature-base or anomaly-based, and requires human intervention in order to respond to the attack.

Acronym(s): IDS

Associated term(s): Intrusion Prevention System (IPS)

Intrusion Prevention System

A form of access control. An IPS is much like an application firewall. Its intent is not only to detect a network attack but to prevent it. It neither requires nor involves human intervention in order to respond to a system attack.

Acronym(s): IPS

Associated term(s): Intrusion Detection System (IDS)

Intrusion reports

Monitoring a system for threats to security of a network.

Investigative Consumer Report

As defined in the U.S. Fair Credit Reporting Act: A consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information. However, such information shall not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer.

Associated term(s): Credit Reporting Agency

Associated law(s):Fair Credit Reporting Act

ISO 27001

The ISO (International Organization for Standardization) 27001 standard is a code of practice for implementing an information security management system, against which organizations can be certified.

ISO 27002

The ISO (International Organization for Standardization) 27002 standard is a code of practice for information security with hundreds of potential controls and control mechanisms. The standard is intended to provide a guide for the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities". It can be considered a guide to implementing ISO 27001 (see ISO 27001).

Link to text of: ISO 27002

IT Architecture

Also known as Enterprise Architecture (EA) is the set of policies (standards and guidelines), principles, services, and products used by IT providers.

Associated term(s): Enterprise Architecture (EA)

IT Department

The division or component of an organization responsible for all forms of technology used to create, store, exchange and use information in its various forms.

Javascript

A computer scripting language used to produce interactive and dynamic web content.

Joint Operations

A reference to joint investigations and joint enforcement measures in which members or staff from the supervisory authorities of multiple member states are involved. The General Data Protection Regulation requires supervisory authorities to work with one another when processing operations affect data subjects in multiple member states (see Consistency Mechanism).

Junk Fax Prevention Act of 2005

Creates the Existing Business Relationship exception to the U.S. Telephone Consumer Protection Act's ban of fax-based marketing without consent but contains a requirement that all marketing faxes be accompanied by instructions on how to opt out of further unsolicited communications.

Link to text of law: Junk Fax Prevention Act of 2005

Acronym: JFPA

Associated term(s): Federal Trade Commission, Federal Communication Commission, Telephone Consumer Protection Act

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.

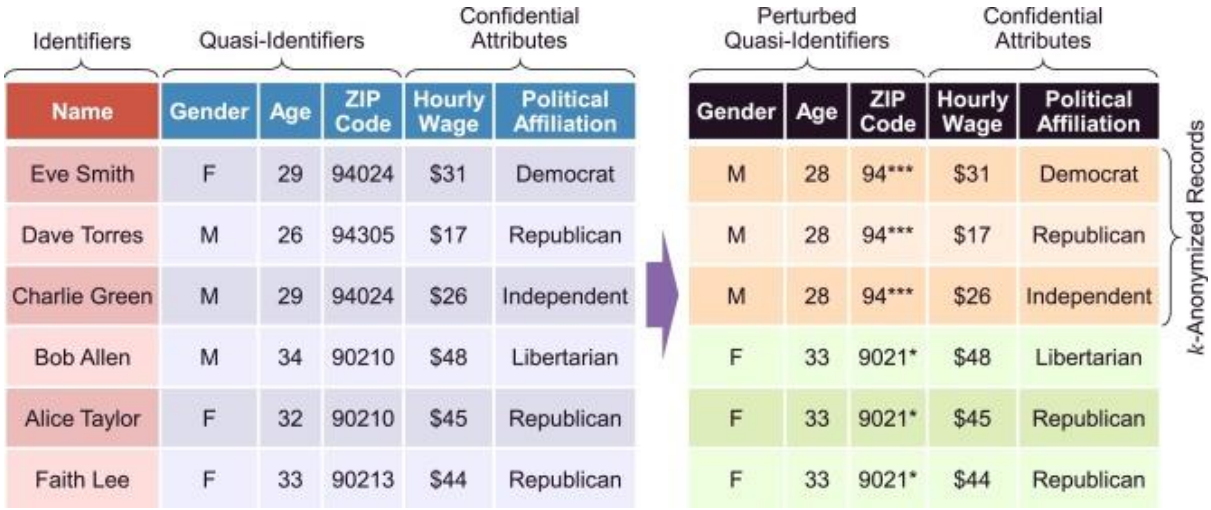
Just-in-Time Notification

Disclosure of specific information practices posted, usually accompanied by a consent request, at the point of information collection.

Acronym(s): JIT Notice

k-anonymity

Relies on the creation of generalized, truncated or redacted quasi-identifiers as replacements for direct identifiers such that a given minimum number ("k") of individuals in a data set have the same identifier.



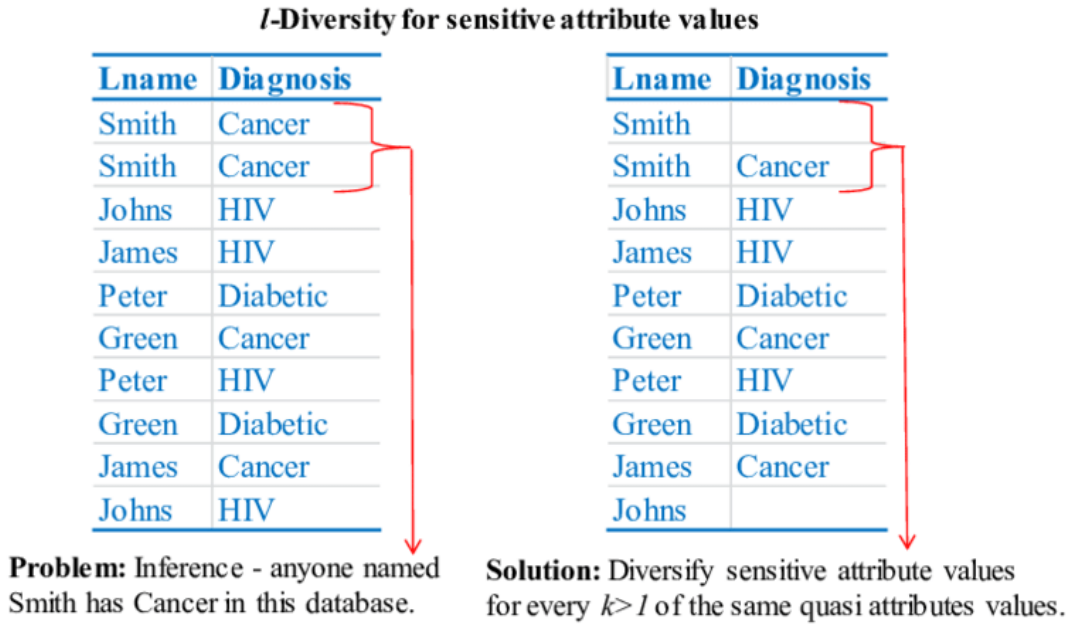
Name	Gender	Age	ZIP Code	Hourly Wage	Political Affiliation
Eve Smith	F	29	94024	$31	Democrat
Dave Torres	M	26	94305	$17	Republican
Charlie Green	M	29	94024	$26	Independent
Bob Allen	M	34	90210	$48	Libertarian
Alice Taylor	F	32	90210	$45	Republican
Faith Lee	F	33	90213	$44	Republican

Gender	Age	ZIP Code	Hourly Wage	Political Affiliation
M	28	94***	$31	Democrat
M	28	94***	$17	Republican
M	28	94***	$26	Independent
F	33	9021*	$48	Libertarian
F	33	9021*	$45	Republican
F	33	9021*	$44	Republican

Credit - ScienceDirect.com

l-diversity

Builds on k-anonymity by requiring at least "l" distinct values in each group of k records for sensitive attributes.



Credit: ReserachGate.net

Law Enforcement Authority

A body sanctioned by local, regional or national governments to enforce laws and apprehend those who break them.

Associated term(s): Public Law Enforcement Authorities

Acronym(s): LEA

Law Enforcement Authority (EU specific)

A body sanctioned by local, regional or national governments to enforce laws and apprehend those who break them. In Europe, public law enforcement authorities are governed by strict rules of criminal procedure designed to protect the fundamental human right to privacy enshrined in Article 8 of the European Convention on Human Rights (ECHR). In the arena of data protection, law enforcement is governed by the Directive on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purpose of Law Enforcement (Directive 2016/680), which came into force in April 2016 (see Law Enforcement Directive).

Acronym(s): LEA

Law Enforcement Directive

Technically Directive 2016/680, or the Directive on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Law Enforcement, this is the EU law governing the handling of personal data by competent law enforcement authorities. Each member state has a law that translates this directive into national law. The directive covers the cross-border and national processing of data by member states' competent authorities for the purpose of law enforcement. This includes the prevention, investigation, detection and prosecution of criminal offences, as well as the safeguarding and prevention of threats to public security. It does not cover activities by EU institutions, bodies, offices and agencies, nor activities falling outside the scope of EU law.

Lawfulness

One of three requirements established by the General Data Protection Regulation for the processing of personal data. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Data subjects must be aware of the fact that their personal data will be processed, including how the data will be collected, kept and used, to allow them to make an informed decision about whether they agree with such processing and to enable them to exercise their data protection rights. The GDPR outlines six bases for the lawful processing of personal data.

Associated term(s): Fairness

Associated law(s): EU Data Protection Directive

Layered Notice

A privacy notice designed to respond to problems with a excessively long notices. A short notice — the top layer — provides a user with the key elements of the privacy notice. The full notice — the bottom layer — covers all the intricacies in full. In its guidance on complying with the General Data Protection Regulation, the Article 29 Working Party, which has now been replaced by the European Data Protection Board, recommended a layered notice in order to meet requirements of the GDPR that privacy notices be easily accessible and easy to understand, and that clear and plain language be used.

Layered Security Policy

A layered approach defines three levels of security policies. The top layer is a high-level document containing the controller's policy statement. The next layer is a more detailed document that sets out the controls that will be implemented to achieve the policy statements. The third layer is the most detailed and contains the operating procedures, which explain how the policy statements will be achieved in practice.

Lead Supervisory Authority

The supervisory authority (see Supervisory Authority) of the main establishment (see Main Establishment) or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Least Privilege

A security control where access is granted at the lowest possible level required to perform the function.

Legal Basis for Processing

The General Data Protection Regulation requires data controllers to demonstrate one of these six legal bases for processing: consent, necessity, contract requirement, legal obligation, protection of data subject, public interest, or legitimate interest of the controller. The controller is required to provide a privacy notice, specify in the privacy notice the legal basis for the processing personal data in each instance of processing, and when relying on the legitimate interest ground must describe the legitimate interests pursued.

Legitimate Interests of Controller

One of the six legal bases for processing personal data in the General Data Protection Regulation, the legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the

data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

Associated term(s): EU Data Protection Directive, Legitimate Processing Criteria

Legitimate Processing Criteria

See Legal Basis for Processing.

Associated term(s): Consent, Legitimate Interests of Controller

Associated law(s): EU Data Protection Directive

Limiting Use

The concept that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law.

Lindqvist Judgement

A case in which the European Court of Justice ruled that a woman who identified and included information about fellow church volunteers on her website was in breach of the Data Protection Directive 95/46/EC. The ECJ held that the creation of a personal website was not a personal activity allowing the woman to be exempted from the data protection rules. Some observers wonder whether Recital 18 of the General Data Protection Regulation, which says the law does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity, might affect this precedential ruling. Recital 18 says personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities.

Link to text of: Lindqvist Judgement

Associated law(s): Directive 95/46/EC

Linkability

The degree to which identifiers used to track an individual user can be paired with outside information to identify that individual. For example, public record can be paired with date of birth, gender and zip code to identify an individual.

Associated term(s): Anonymous Information, Pseudonymous Data, De-Identification, Identifiability, Re-Identification, Identifiers, GUID

Local Area Network

Networks that exist within an operational facility. They are considered within local operational control and are relatively easy to manage.

Acronym(s): LAN

Associated term(s): WAN

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

Local Shared Objects

Data files created on a computer’s hard drive by a domain to track user preferences and used by all versions of Adobe Flash Player. They are often called flash cookies. LSOs differ from HTTP cookies in that they are saved to a computer’s hard drive rather than the web browser.

Acronym(s): LSOs

Associated term(s): Cookies

Location Data

Data indicating the geographical position of a device, including data relating to the latitude, longitude, or altitude of the device, the direction of travel of the user, or the time the location information was recorded.

Location-Based Service

Services that utilize information about location to deliver, in various contexts, a wide array of applications and services, including social networking, gaming and entertainment. Such services typically rely upon GPS, RFID, Wi-Fi, or similar technologies in which geolocation is used to identify the real-world geographic location of an object, such as a mobile device or an internet-connected computer terminal.-

Acronym(s): LBS

Associated term(s): Geolocation; GPS; Global Positioning System; RFID

Logs

A record of both normal and suspect events by a computer system (typically an operating system). The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. The program developer decides which events to record. The system log contains events logged by the operating system components; for example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types

logged by system components are predetermined for the operating system. The security log can record security events, such as valid and invalid log-in attempts as well as events related to resource use, such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log. For example, if you have enabled log-in auditing, attempts to log in to the system are recorded in the security log.

Low level design

The details of a high-level design system.

Machine Learning

A subfield of, or building block for, artificial intelligence (see Artificial Intelligence), machine learning is a problem-solving technique that trains a computer to identify new patterns. It implements various algorithms in a problem-solving process that includes data cleansing, feature selection, training, testing, and validation. Companies and government agencies increasingly deploy machine learning algorithms for tasks such as fraud detection, speech recognition, image classification and other pattern-recognition applications.

Machine-readable Formats

"[W]ritten in a standard computer language (not English text) that can be read automatically by a web browser." (Source: OMG PIA Guidance)

Madrid Resolution

A resolution adopted in 2009 by the International Conference of Data Protection and Privacy Commissioners, consisting of 80 data protection authorities from 42 countries around the world. The resolutions proposes international standards on the protection of privacy with regard to the processing of personal data, to include: lawfulness and fairness; purpose specification; proportionality; data quality; openness; and accountability.

Link to text of resolution: The Madrid Resolution

Magnitude data

Refers to the size of the data. A table showing average income by age is magnitude data.

Main Establishment

The main establishment of a controller in the Union should be the place of its central administration in the European Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the EU in which case that other establishment should be considered to be the main establishment. The main establishment of the processor should be the place of its central administration in the EU or, if it has no central administration in the EU the place where

the main processing activities take place in the EU. The member state location of the main establishment determines the controller or processor's lead supervisory authority (see Lead Supervisory Authority).

Manageability

The ability to granularly administer personal information, including modification, disclosure and deletion.

Mandatory Access Control

An access control system by which access to data, by the owner or user, is constrained by the operating system itself.

Acronym(s): MAC

Associated term(s): Discretionary Access Control

Matching Program (from The Privacy Act of 1974)

Any computerized comparison of two or more automated systems of records or a system of records with non-Federal records for the purpose of establishing or verifying the eligibility of, or continuing compliance by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or (any computerized comparison of) two or more automated Federal personnel or payroll systems of records or (any such system) with non-Federal records.

Associated term(s): The Privacy Act of 1974

Material Scope

The actions covered by a particular law or regulation.

Material Scope (EU specific)

The actions covered by a particular law or regulation. The material scope of the General Data Protection Regulation, for example, is the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system, other than that processing that falls outside of the scope of EU law, is done for personal or household use, or is done for law enforcement purposes.

Max Schrems

Chairman and founder of noyb, a "privacy enforcement platform" that brings data protection cases to the courts under the EU General Data Protection Regulation. Schrems first came to notoriety as an Austrian law student, who filed a complaint to the

Irish Data Commissioner that Facebook Ireland was illegally sharing his personal data with the U.S. government, following the revelations of Edward Snowden. The case, known as "The Schrems case" or "Schrems I," eventually led to the invalidation of the Safe Harbor data-transfer agreement between the EU and U.S. (see "Safe Harbor" and "Privacy Shield"). Schrems later amended his complaint against Facebook Ireland with the Irish Data Protection Commission after Facebook switched its transfer mechanism from Safe Harbor to standard contractual clauses, leading to a new referral to the CJEU implicating both standard contractual clauses and the EU-U.S. Privacy Shield Framework. On July 16, 2020, the Court of Justice of the European Union invalidated Privacy Shield, and placed additional requirements for companies using standard contractual clauses to third countries outside the EU.

Media Access Control Address

A hardware identification number that uniquely identifies each device connected to a network. The MAC address is manufactured into every network card in each device and therefore it cannot be changed and remains constant no matter what network the device is connected to.

Acronym: MAC address

Medical Information

Information or records obtained, with the consent of the individual to whom it relates, from licensed physicians or medical practitioners, hospitals, clinics or other medical or medically related facilities.

Associated term(s): HIPAA

Member State

A member state of the European Union, formally created by the Maastricht Treaty in 1992. As of the last addition of member states in 2013, the EU consists of: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom. The U.K. submitted a notice of withdrawal under Article 50 of the Treaty of Lisbon in 2016 and will leave the European on March 29, 2019, unless the European Council decides to extend the two-year negotiating period by unanimous vote.

Members of the European Parliament

The only directly elected body of the European Union, the Parliament represents one half of the legislative arm of the EU, alongside the Council of the European Union. Members of Parliament are elected by citizens of the member states, in proportion to the size of each country, every five years. Those MEPs then elect the president of the European Commission. Its three primary responsibilities are legislative development, supervisory oversight of the other institutions, and development of the budget. As of 2018, the Parliament had 751 members.

Link to list of: Members of the European Parliament

Acronym(s): MEPs

Memorandum of Understanding/Agreement

"A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide [NIST SP 800-47], an MOU/A defines the responsibilities of two or more organizations in establishing, operating and securing a system interconnection." For the proposed transmission of PII among federal agencies, a memorandum will govern the purpose, methods of transmission, relevant authorities, specific responsibilities of the organizations transmitting and receiving the PII, and risks associated with its transmission.

Link to text of: NIST SP 800-47

Acronym(s): MOU

Metadata

Data that describes other data. "Meta" is a prefix meaning "an underlying description" in information technology usage.

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

Microdata Sets

Groups of information on individuals that have been altered or suppressed in some way to anonymize the data, protecting individuals from being identified.

Associated term(s):Anonymous Information, De-Identification

Minimum Necessary Requirement

Under HIPAA, the standard that the level of information that may be disclosed by healthcare providers to third parties is the minimum amount necessary to accomplish the intended purpose.

Associated term(s): Minimum Necessary Standard

Associated law(s): HIPAA

Mobile Device Management (MDM)

MDM refers to software solutions that allow administrators to oversee the use of mobile devices for productivity and security reasons. MDM solutions usually allow an organization to control mobile apps, networks and data used by the mobile device from a single centralized software product, thereby assuring better control of company information on personal devices. MDM solutions also present challenges in the BYOD context because they allow for greater monitoring of employees' personal use of their devices. Some MDM solutions enable organizations to remotely wipe a mobile device if it is suspected of being lost or compromised, which raises additional concerns if personal employee information is deleted.

Mobility

The extent to which a system moves from one location to another, as in laptop and mobile phone capabilities.

Model Clauses

See: Standard Model Clauses

Model Code for the Protection of Personal Information

A set of privacy principles developed by the Canadian Standards Association, that parallel the OECD's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data and espouse 10 principles: Accountability, Identifying Purpose, Consent, Limiting Collection, Limiting Use, Disclosure, & Retention, Accuracy, Safeguards, Openness, Individual Access and Challenging Compliance.

Link to text of: OECD's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data

Monetary Instrument Log

Under the Bank Secrecy Act, the log of transactions a financial institution must retain a record for cash purchases of monetary instruments (e.g., money orders, cashier's checks, travelers checks) ranging from $3,000 to $10,000.

Acronym(s): MIL

Associated law(s): Bank Secrecy Act

Multi-Factor Authentication

An authentication process that requires more than one verification method (see Authentication), such as a password and biometric identifier, or log-in credentials and a code sent to an email address or phone number supplied by a data subject.

Associated term(s): Two-Factor Authentication; Two-Step Authentication

Mutual Assistance

The General Data Protection Regulation requires that supervisory authorities assist each other in performing their tasks and provide mutual assistance to one another so as to ensure the consistent application and enforcement (see Consistency Mechanism). In certain cases, supervisory authorities can go forward without mutual assistance if request for assistance is not answered within 30 days or other time periods. The GDPR also requires international mutual assistance with third countries and international organizations in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms.

National Archives and Records Administration

NARA is charged with providing guidance and assistance with respect to records management and maintaining those records that are of sufficient value to warrant permanent preservation. Further, NARA establishes general records schedules, which provide mandatory disposal authorization for temporary administrative records common to several or all agencies of the federal government. These include records relating to civilian personnel, fiscal accounting, procurement, communications, printing and other common functions and certain nontextual records.

Link to: National Archives and Records Administration

Acronym(s): NARA

National Do-Not-Call Registry (U.S.)

Allows U.S. consumers to place their phone number on a national list, preventing calls from unsolicited telemarketers. This registration is now permanent and can be enforced by the Federal Trade Commission, Federal Communication Commission and state attorneys general with up to a $16,000 fine per violation. Cell phones are protected from any unsolicited automatic-dialed calls through other FCC regulations.

Link to: National Do-Not-Call Registry

Associated term(s): Federal Trade Commission, Federal Communication Commission, Do-Not-Call Implementation Act, Do-Not-Call Improvement Act

National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework (NICE)

The NICE framework establishes common terminology to describe cybersecurity work and is intended to be applied in all sectors: public, private and academic.

National Institute of Standards and Technology

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.

Link to: National Institute of Standards and Technology

Acronym(s): NIST

Associated term(s): FISMA

Associated law(s): FISMA

National Institute of Standards and Technology (NIST) framework

NIST is a voluntary risk management tool alongside the NIST Cyber-security Framework. It provides standard, guidelines and best practices for managing cybersecurity-related risks and is intended to assist organizations in communicating and organizing privacy risk as well as rationalizing privacy to build or evaluate a privacy governance program.

National Labor Relations Board, The

A U.S. federal agency that administers the National Labor Relations Act. The board conducts elections to determine if employees want union representation and investigates and remedies unfair labor practices by employers and unions.

Link to: National Labor Relations Board

Acronym(s): NLRB

Associated law(s): National Labor Relations Act

National Security Letter

A category of subpoena. The USA PATRIOT Act expanded the use of national security letters. Separate and sometimes differing statutory provisions now govern access, without a court order, to communication providers, financial institutions, consumer credit agencies and travel agencies.

Acronym(s): NSL

Associated law(s): USA-PATRIOT Act

Nationwide Consumer Reporting Agency

A consumer reporting agency that regularly assembles, evaluates, and maintains consumer files on consumers who reside nationwide using public record information and "credit account information from persons who furnish that information regularly and in the ordinary course of business." Such agencies compile such information to create and disseminate reports about consumer credit worthiness, credit standing, or credit capacity.

Nationwide Specialty Consumer Reporting Agency

A consumer reporting agency that compiles information about consumers on a nationwide basis related to (1) medical records or payments; (2) residential or tenant history; (3) check writing history; (4) employment history; or (5) insurance claims.

Natural language generation

Information is transformed into content, enabling such functions as text-to speech, automation of reports and the production of content for awe or mobile applications.

Natural language understanding

Utilizes machine reading comprehension through algorithms to identify and extract natural language that the computer can understand.

Necessity

Necessity along with proportionality (see Proportionality), is one of two factors data controllers should consider as they apply the principle of data minimization (see Data Minimization), as required by the General Data Protection Regulation. Necessity considers the amount of data to be collected and whether it is necessary in relation to the stated purposes for which it is being processed.

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

Network Centricity

The extent to which personal information remains local to the client.

Network Devices

The components used to link computers and other devices so they may share files and utilize other electronic resources, e.g. printers and fax machines. The most common network devices are those used to create Local Area Networks (LAN), which require a hub, router, cable or radio connection devices, network cards, and (for access to the internet) a modem.

Network Encryption

A type of network security that protects data traffic by providing encryption at the network transfer layer. This form of encryption operates independently of other security measures and is invisible to the ender user as data is only encrypted while in transit.

Network-Layer Attacks

Attacks that exploit the basic network protocol in order to gain any available advantage. These attacks generally involve "spoofing" a network address so that a computer sends data to an intruder rather than their proper recipient or destination. Other attacks can involve service disruptions through a denial of service (DOS) attack—a brute force method that overloads the capacity of a website's domain to respond to incoming requests such that it renders the server inoperable.

Noise addition

Blurring data to ensue that aggregated data is useful, yet nonspecific enough to avoid revealing identifiers.

Non-Functional System Requirements

Abstracted concepts of the operation of a new software system or product being developed that inform functional requirements. These requirements describe how a system should work rather than specific technical processes the system completes. For example "the system shall be able to create user profiles for individuals using the system."

Associated term(s): Plan-driven Development Model, Agile Development Model, Functional System Requirements, SRS

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

Non-Repudiation

The ability to ensure that neither the originator nor the receiver in a transaction can dispute the validity of the transaction or access request. An independent verification takes place which allows the sender's identity to be verified, typically by a third party, and also allows the sender to know that the intended recipient of the message actually received it. Non-repudiation of origin proves that data has been sent and non-repudiation of delivery proves that the data has been received.

Obfuscation

To make (something) more difficult to understand; to hide the true meaning. For Data Obfuscation see Data Masking.

Associated term(s): Data Masking

Objective Harm

Measurable and observable, wherein a person's privacy has been violated and a direct harm is known to exist.

OECD Guidelines

First released in 1980, and then updated in 2013, these guidelines represent perhaps the most widely accepted and circulated set of internationally agreed upon privacy principles along with guidance for countries as they develop regulations surrounding cross-border data flows and law-enforcement access to personal data. The principles, widely emulated in national privacy laws, include Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability (see entries for each principle under their own listing elsewhere in the glossary).

Link to text of: OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data

Office of Management and Budget

Under the Privacy Act, the OMB is charged with the responsibility to supervise agencies' implementation of the act's provisions. In order to perform this task, the act provides that the director of the OMB shall develop and prescribe guidelines and regulations, as well as provide assistance and oversight of their implementation by agencies.

Acronym(s): OMB

Office of the Director of National Intelligence

Overseeing the intelligence community is the Office of the Director of National Intelligence. The IRTPA established the director of National Intelligence as the head of the intelligence community and the principal advisor to the president and the National Security Council.

Link to: Office of the Director of National Intelligence

Acronym(s): ODNI

Associated law(s): Intelligence Reform and Terrorism Prevention Act

OMB Memorandum M-03-22

This memorandum provides agencies with specific implementation guidance for conducting PIAs and developing website privacy policies. It applies to all executive branch agencies and departments, contractors and cross-agency initiatives that use websites or other information technology for interacting with the public. It requires agencies to: conduct PIAs and make them publicly available; post privacy policies on agency websites; translate privacy policies into a standardized machine-readable format; ensure privacy responsibilities are properly executed for information in identifiable form (IIF) processed by information technology; report annually to OMB on Section 208 compliance.

Link to text of: OMB Memorandum M-03-22

Associated law(s): Privacy Act

Omnibus Laws

Used to distinguish from sectorial laws (see Sectorial Laws), to mean laws that cover a broad spectrum of organizations or natural persons, rather than simply a certain market sector or population.

One-stop Shop

A colloquial description of the EU's General Data Protection Regulation's consistency mechanism that allows a specific Data Protection Authority (see DPA) to function as a business's single point of contact—or lead supervisory authority—for a complaint or investigation. This saves businesses from the need to potentially engage with DPAs from 28 EU Member States.

Online Behavioral Advertising

Websites or online advertising services that engage in the tracking or analysis of search terms, browser or user profiles, preferences, demographics, online activity, offline activity, location data, etc., and offer advertising based on that tracking.

Online Data Storage

Refers to the storage of data by a third-party vendor made accessible through the Internet.(Hosted storage, Internet storage, cloud storage) This is a common data storage alternative to local storage, such as on a hard drive, and portable storage, such as a flash drive.

Associated term(s): Cloud Computing

Online Privacy Alliance

A coalition composed of numerous online companies and trade associations specifically established to encourage the self-regulation of online privacy. The OPA introduced the Online Privacy Guidelines.

Link to: Online Privacy Alliance

Link to: Online Privacy Guidelines

Acronym(s): OPA

Associated term(s): Self-regulation

Onward Transfer

A transfer of personal data to a fourth party or beyond. For instance, the first party is the data subject, the second party is the controller, the third party is the processor, and the fourth party is a sub-contractor of the processor. In the context of binding corporate rules, this might mean the third party is another unit of the controller organization outside of the EEA and the fourth party is a processor. If an onward transfer occurs, the controller remains accountable for processing of the personal data.

Open Government Directive

When President Obama entered into office he issued a memorandum calling for an unprecedented level of openness in government, which launched the Open Government Initiative. In December 2009, the Director of the OMB issued the Open Government Directive, which set forth detailed requirements focused on implementing the president's vision. The president required the OMB to issue a directive to federal departments and agencies to take certain steps to implement the underlying principles of transparency, participation and collaboration discussed in the president's memorandum.

Link to: Open Government Initiative

Link to text of: Open Government Directive

Associated term(s): OMB

Open-source vs. closed-source

Easily viewed, shared and modified software is considered open-source. Closed-source software must by fixed and updated by the vendor.

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.

Opinions of the Article 29 Working Party

Various opinions of the Article 29 Working Party (see Article 29 Working Party) continue to be relevant even after the body's transition into the European Data Protection Board (EDPB). They continue to provide guidance and context as to the stance of European Union member state regulators in how data protection law should be interpreted.

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-In (EU specific)

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. The General Data Protection Regulation's definition of consent as requiring a "clear affirmative act" makes opt-in the default standard for consent acquisition.

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

Opt-Out (EU Specific)

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. The General Data Protection Regulation's definition of consent as requiring a "clear affirmative act" makes opt-out unacceptable for the acquisition of consent.

Organization for Economic Cooperation and Development

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.

Link to: Organization for Economic Cooperation and Development

Acronym(s): OECD

Outsourcing

Contracting business processes, which may include the processing of personal information, to a third party.

Outsourcing (EU-specific)

Contracting business processes, which may include the processing of personal information, to a third party. The General Data Protection Regulation establishes direct legal obligations applicable to service providers acting as "processors" and places an increased emphasis to the contractual obligations that must be established between organizations and their data processing service providers.

Paperwork Reduction Act

The PRA concerns information that is created, collected, disclosed, maintained, used, shared, and disseminated by or for the federal government, regardless of whether it is PII. The primary goal is to calculate and reduce as much as possible the burden of providing information to the government while maintaining the quality of that information. The requirements of the PRA cover collections of information, which may exist in any format, and could include surveys, applications, questionnaires, and reports or any scenario in which 10 or more persons are asked to provide the same information within a 12-month period.

Link to text of Act: Paperwork Reduction Act

Acronym(s): PRA

Passive Collection

Collecting data from a data subject that is unaware of such collection.

Associated term(s): Active Collection, First-party Collection, Surveillance Collection, Repurposing, Third-party Collection

Passive Data Collection

Data collection in which information is gathered automatically—often without the end user's knowledge—as the user navigates from page to page on a website. This is typically

accomplished through the use of cookies, web beacons or other types of identification mechanisms.

Associated term(s): Observational Study; Cookie; Web Beacons; Active Data Collection

Patches

Changes to a program that aim to fix, update or improve a system.

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

PCI Security Standards Council

The PCI Security Standards Council is a council that is responsible for the development and management of the Payment Card Industry Security Standards, most notably the PCI Data Security Standard. The council is made up of American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. and other affiliate members.

Link to: PCI Security Standards Council

Associated term(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

Perimeter Controls

Technologies and processes that are designed to secure an entire network environment by preventing penetration from the outside.

Associated term(s): Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Internet Protocol Security (IPSEC), Secure Sockets Layer (SSL)

Persistent Storage

The storage of data in a non-volatile storage medium such as a hard drive. In the absence of persistent data storage, data would only be stored in RAM (random access memory) and would be lost whenever the device lost power.

Associated term(s): Transient Storage

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 Data (EU specific)

Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly — in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

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.

Acronym(s): PI

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

Personal Information (EU specific)

A synonym for "personal data," which is any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly — in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

Personal Information Protection and Electronic Documents Act

A Canadian act with two goals: (1) to instill 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.

Link to text of law: Personal Information Protection and Electronic Documents Act

Acronym(s): PIPEDA

Personally Identifiable Information

Any information about an individual, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linkable to an individual, such as medical, educational, financial, and employment information.

Perturb

Perturbing adds approximation or "noise" to data to reduce its specificity.

For example, technology architects might introduce "noise" into data by dropping the last octet of an IP address, or the last specific digits of a geolocation in cases where analysis can still be done without the full (identifiable) data set.

Pharming

Redirecting a valid internet request to a malicious website by modifying a Hosts file or corrupting a network router domain name system.

Associated term(s): Phishing, Spear Phishing, Whaling

Phishing

E-mails or other communications that are designed to trick a user into believing that he or she should provide a password, account number or other information. The user then typically provides that information to a website controlled by the attacker. "Spear phishing" is a phishing attack that is tailored to the individual user, such as when an e-mail appears to be from the user's boss, instructing the user to provide information.

Associated term(s): Spear Phishing; Social Engineering

PIA Triggers

These events constitute triggers for an organization to conduct a privacy impact assessment: Conversion of records from paper-based to electronic form; Conversion of information from anonymous to identifiable form; System management changes involving significant new uses and/or application of new technologies; Significant merging, matching or other manipulation of multiple databases containing PII; Application of user-authenticating technology to a system accessed by members of the public; Incorporation into existing databases of PII obtained from commercial or public sources; Significant new inter-agency exchanges or uses of PII; Alteration of a business process resulting in significant new collection, use and/or disclosure of PII; Alteration of the character of PII due to the addition of qualitatively new types of PII.

Associated law(s): FISMA

Plan-Driven Development Model

A strategy used when creating new software products and systems. Plan-driven models focus on designing the entirety of the system and system functions before actual creation of the system, as opposed to the Agile Development Model. An example of a plan-driven model is the Spiral model.

Associated term(s): Agile Development Model, CONOPS

Platform for Privacy Preferences

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

Acronym(s): P3P

Platform for Privacy Preferences Project

A project with the goal of designing web protocols with user privacy in mind. Several protocols have been developed out of this project including the most successful, XACML.

Link to: Platform for Privacy Preferences Project

Acronym: P3P

Policy Framework

The repository of all an organization's rules and procedures for implementing policies surrounding, for example, privacy and security. It is the natural reference point for anyone, such as a regulator or auditor, who wants to understand an organization's position regarding a particular policy area.

Polygraph

A device used for the purpose of rendering a diagnostic opinion regarding an individual's honesty.

Associated term(s): Lie Detector

Associated law(s): Employee Polygraph Protection Act of 1988 (EPPA)

Polymorphic

The algorithm is mutated with each copy of the code, while the outcome of the encryption remains the same for any given key.

POST Method

The GET and POST HTML method attributes specify how form data is sent to a web page. The POST method is more secure than GET as the GET method appends the form data to the URL allowing passwords and other sensitive information collected in a form to be visible in the browser's address bar.

Associated term(s): GET Method

Postal Marketing

Direct marketing (see Direct Marketing) to postal addresses.

Associated term(s): Direct Marketing

Postal Marketing (EU specific)

Direct marketing (see Direct Marketing) to postal addresses. Just as with other forms of direct marketing, marketers must ensure they establish the lawful basis for processing personal data when postal marketing to those in the EEA under the General Data Protection Regulation.

Predictability

Characterizes reliable assumptions about a system particularly its data and the processing of that data by all stakeholders.

Preemption

A superior government's ability to have its law(s) supersede those of an inferior government. For example, the U.S. federal government has mandated that no state government can regulate consumer credit reporting.

Premium Advertising

The most expensive and most visible type of web advertising, typically on the homepage of a website and priced so that only big name companies/products use them.

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

Pretty Good Privacy (PGP)

An encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

Prior Authorization

Under the General Data Protection Regulation, a processor (see Processor) may not engage another processor without prior authorization of the data controller (see Controller). This authorization may be general or specific. If it is general, the processor is required to give the controller an opportunity to object to the addition or replacement of other processors.

Associated term(s): Notification; Data Protection Authority

Privacy

A nebulous philosophical, legal, social and technological concept which means different things to different observers. In an influential 1890 Harvard Law Review article, Samuel Warren and Louis Brandeis, who later became a Supreme Court Justice, famously defined privacy as "a right to be let alone." Common areas of privacy that are of particular interest with regard to data protection and privacy laws include information privacy, bodily privacy, territorial privacy, and communications privacy.

Four main areas of privacy are of particular interest with regard to data protection and privacy laws and practices: information privacy, bodily privacy, territorial privacy, and communications privacy.

Privacy Act Exceptions

Among the exception to the Privacy Act of 1974 are: (1) Performance of regular duties of an agency employee; (2) FOIA disclosures; (3) Routine uses as specified in the applicable SORN; (4) Census Bureau census or survey functions; (5) Statistical research if not individually identifiable; (6) Data held by the National Archives; (7) Law enforcement activity; (8) Compelling health or safety circumstances; (9) Congressional committee with appropriate jurisdiction; (10) GAO duties; (11) Court order, and (12) Consumer reporting agencies.

Associated term(s): The Privacy Act of 1974

Privacy Act of 1974

A U.S. law that regulates the federal government's use of computerized databases of information about U.S. citizens and permanent legal residents. It also establishes fair information practices that each agency must follow when collecting, using or disclosing personal information, including rights of citizen action and redress for violations. It guarantees that U.S. citizens and lawful permanent residents have: (1) the right to see records about themselves that are maintained by the federal government (provided that information is not subject to one or more of the Privacy Act's exemptions); (2) the right to amend inaccurate, irrelevant, untimely or incomplete records; and (3) the right to sue the government for failure to comply with its requirements. It also contains fair information practices that: (1) require that information about a person be collected from that person to the greatest extent practicable; (2) require agencies to ensure that their records are relevant, accurate, timely and complete, and (3) prohibit agencies from

maintaining information describing how an individual exercises his or her First Amendment rights (unless the individual consents to it, it is permitted by statute or is within the scope of an authorized law enforcement investigation).

Link to text of law: Privacy Act

Privacy Act, The (Canadian)

Enacted in 1983, the Act sets out rules for how institutions of the federal government must deal with personal information of individuals. It has been revised by many minor amendments, but remains substantially unaltered.

Link to text of law: The Canadian Privacy Act

Privacy and Civil Liberties Oversight Board

PCLOB is an independent, bipartisan agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act, Pub. L. 110-53, signed into law in August 2007. Comprised of four part-time members and a full-time chairman, PCLOB is vested with two fundamental authorities: (1) To review and analyze actions the executive branch takes to protect the Nation from terrorism, ensuring the need for such actions is balanced with the need to protect privacy and civil liberties and (2) To ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.

Acronym(s): PCLOB

Link to: Privacy and Civil Liberties Oversight Board

Link to text of law: Implementing Recommendations of the 9/11 Commission Act, Pub. L. 110-53

Privacy Assessment

An assessment of an organization's compliance with its privacy policies and procedures, applicable laws, regulations, service-level agreements, standards adopted by the entity and other contracts. The assessment or audit measures how closely the organization's practices align with its legal obligations and stated practices and may rely on subjective information such as employee interviews/questionnaires and complaints received, or objective standards, such as information system logs or training and awareness attendance and test scores. Audits and assessments may be conducted internally by an audit function or by external third parties. It is also common in some jurisdictions for the privacy/data protection officer to conduct assessments. The results of the assessment or audit are documented for management sign-off, and analyzed to develop recommendations for improvement and a remediation plan. Resolution of the issues and vulnerabilities noted are then monitored to ensure appropriate corrective action is taken on a timely basis. While assessments and audits may be conducted on a regular or scheduled basis, they may also arise ad hoc as the result of a privacy or security event or due to a request from an enforcement authority.

Privacy Breach (Canadian)

A privacy breach occurs when there is unauthorized access, collection, use or disclosure of personal information. Such activity is "unauthorized" if it occurs in contravention of applicable privacy legislation, such as PIPEDA or similar provincial privacy legislation.

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

Privacy Breach Response (Canadian)

The guidelines for privacy breach responses were drafted in 2007 and consist of four steps: (1) Containment of the breach and preliminary assessment; (2) evaluating the associated risks; (3) notifying affected parties; (4) taking adequate steps to prevent future breaches.

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

Privacy by Design

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.

Proactive not reactive; preventative not remedial, Privacy as the default, Privacy embedded into design, Full functionality—Positive-sum, not zero-sum, End-to-end security—life cycle protection, Visibility and transparency, Respect for user privacy

Acronym(s): PbD

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 Commissioner of Canada

The individual who is mandated by PIPEDA to enforce the act. The commissioner has broad power to examine documents, but some documents may be shielded by solicitor-client privilege. The commissioner conducts investigations under a cloak of confidentiality, but public reports with non-binding recommendations are ultimately issued. This individual is mandated by PIPEDA to enforce PIPEDA. Aggrieved individuals also have a right to complain to the commissioner.

Link to: Privacy Commissioner of Canada

Associated law(s): PIPEDA

Privacy engineering

Encompasses how privacy values and principles are applied in technology systems and programs while recognizing and maintaining security levels to mitigate risk. It brings the complementary perspectives and practices of software engineers and privacy professionals together.

Privacy Impact Assessment

"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.

Acronym(s): PIAs

Privacy Impact Assessments (Canadian)

The Canadian government requires all government institutions subject to the Privacy Act to conduct these assessments. The purpose behind a PIA is to evaluate whether program and service delivery initiatives that involve the collection, use or disclosure of personal information are in compliance with statutory obligations.

Acronym(s): PIAs

Privacy Maturity Model

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

Acronym(s): PMM

Privacy Notice

A statement made to a data subject that describes how an organization collects, uses, retains and discloses personal information. A privacy notice may be referred to as a privacy statement, a fair processing statement or, sometimes, a privacy policy. Numerous global privacy and data protection laws require privacy notices.

Privacy Notice (EU specific)

A statement made to a data subject that describes how an organization collects, uses, retains and discloses personal information. A privacy notice may be referred to as a privacy statement, a fair processing statement or, sometimes, a privacy policy. The General Data Protection Regulation requires a controller to provide a privacy notice prior to processing and to specify in the privacy notice the legal basis for the processing, in addition to other details, such as the contact information for the organization's Data Protection Officer. When relying on the legitimate interest ground, the controller must describe the legitimate interests pursued.

Privacy Nutrition Label

A standard form label intended to make privacy policies easily and quickly understandable. Privacy Nutrition Labels where developed by the Cylab Usable Privacy and Security Laboratory (CUPS) at Carnegie Mellon University.

Link to: Cylab Usable Privacy and Security Laboratory

Associated term(s): Privacy Policy

Privacy of the Person

Protects bodily integrity, and in particular the right not to have our bodies touched or explored to disclose objects or matters we wish to conceal.

Privacy Officer

A general term in many organizations for the head of privacy compliance and operations. In the United States federal government, however, it is a more specific term for the official responsible for the coordination and implementation of all privacy and confidentiality efforts within a department or component. This official may be statutorily mandated as a political appointment, as in the Department of Homeland Security, or a career professional.

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 Patterns

Based on the concept of "Design Patterns" developed by Erich Gamma, Richard Helm, Ralph Johnson and John Vlissides, Privacy Patterns are a set of solutions to common privacy problems in designing software. Each Privacy Pattern describes a privacy concern that occurs when developing software and a uniform way to alleviate that concern.

Associated term(s): UML, Plan-driven Development Model, Agile Development Model

Privacy Policy

An internal statement that governs an organization or entity's handling of personal information. It is directed at those members of the organization who might handle or make decisions regarding the personal information, instructing them on the collection, use, storage and destruction of the data, as well as any specific rights the data subjects may have. May also be referred to as a data protection policy.

Privacy Policy in Standardized Machine-Readable Format

Defined by the U.S. Office of Management and Budget Memorandum M-03-22, "[a] statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser."

Link to text of Memo: U.S. Office of Management and Budget Memorandum M-03-22

Privacy Program Framework

An implementation roadmap that provides the structure or checklists (documented privacy procedures and processes) to guide the privacy professional through privacy management and prompts them for the details to determine all privacy-relevant decisions for the organization.

Privacy Review

An analysis of all new projects for their compliance with the privacy standard and privacy policy of an organization. Reviews should be performed multiple times beginning at the early stages of new project development to minimize potential privacy risks.

Associated term(s): Privacy Standard, Privacy Policy, Privacy by Design, Privacy Risk

Privacy Risk

A formula to calculate the impact of a new project on the privacy of the consumer base that will use the new systems. To evaluate the risk, one must consider the likelihood of the threat occurring, multiplied by the potential impact if the threat occurs. It may be

difficult to quantify, so a comparison between projects may be the best way to understand privacy risks.

Associated term(s): Privacy Standard, Privacy Policy, Privacy by Design, Privacy Review

Privacy Rule, The

Under HIPAA, this rule establishes U.S. national standards to protect individuals' medical records and other personal health information and applies to health plans, healthcare clearinghouses and those healthcare providers that conduct certain healthcare transactions electronically. The rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records and to request corrections.

Link to text of rule: Privacy Rule

Associated law(s): HIPAA

Privacy Standard

The minimum level at which privacy should be protected in all new projects, applications and services. This includes the expectations of privacy in the new programs and guidelines for adherence to those standards. The standard is set based on both internal organizational policy and external regulations etc.

Associated term(s): Privacy by Design, Privacy Review, Privacy Policy, Privacy Risk

Privacy Technlologist

A term used to reference the many technology professionals that play a role in protecting privacy in or with technology. Includes but is not limited to: audit, risk and compliance managers; data professionals; data architects; data scientists, system designers and developers; software engineers, privacy engineers.

Privacy Threshold Analysis

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

Acronym(s): PTA

Privacy-Enhancing Technologies

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).

Acronym(s): PETs

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

Professional Regulatory Body

A body enacted pursuant to an act under which a professional or occupational group or discipline is organized and that provides for the membership in the regulation of the members of the professional or occupation group or discipline, including the registration, competence, conduct, practice and discipline of its members.

Profiling

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects, in particular to analyze or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Programmatic Buying

Buying through automated means, for example, by setting up a campaign in an RTB exchange or other automated system.

Proportionality

Proportionality, along with necessity (see Necessity), is one of two factors data controllers should consider as they apply the principle of data minimization (see Data Minimization), as required by the General Data Protection Regulation. Proportionality considers the amount of data to be collected and whether it is adequate and relevant in relation to the purposes for which it is being processed. Is the processing suitable and reasonably likely to achieve the stated objectives? Are any adverse consequences that the processing creates justified in view of the importance of the objective pursued?

Associated law(s): EU Data Protection Directive

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

Protect America Act, The

The PAA restored FISA to its original focus of protecting the rights of persons in the United States, while not acting as an obstacle to gathering foreign intelligence on targets located in foreign countries. The act also modernized FISA in four important ways: It clarifies FISA's definition of electronic surveillance; It provides a role for the FISA court in reviewing the procedures the intelligence community uses to ensure that collection remains direct at persons located overseas; It provides a mechanism for the FISA court to direct third parties to assist the intelligence community in its collection efforts, and; it protects third parties from private lawsuits arising from assistance they provide the government in authorized foreign intelligence activities targeting individuals located outside the United States.

Link to text of law: Protect America Act

Acronym(s): PAA

Associated term(s): FISA

Associated law(s): FISA

Protected Health Information

Any individually identifiable health information transmitted or maintained in any form or medium that is held by an entity covered by the Health Insurance Portability and Accountability Act or its business associate; identifies the individual or offers a reasonable basis for identification; is created or received by a covered entity or an employer; and relates to a past, present or future physical or mental condition, provision of healthcare or payment for healthcare to that individual.

Acronym(s): PHI

Protecting Canadians from Online Crime Act

Criminalizes cyber bullying and loosens restraints on police to obtain warrants for telecommunications and internet data, as well as allows police to compel the preservation of electronic evidence.

Link to text of law: Protecting Canadians from Online Crime Act

Protective Order

With a protective order, a judge determines what information should not be made public and what conditions apply to who may access the protected information.

Associated term(s): Redaction

Pseudonymisation

The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and

organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

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.

Psychographic Advertising

Based on a user's interest as accounted for by their preferences online. Different from behavioral because it simply accounts for known preferences rather than taking into account different interactions with web pages and advertisements.

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

Public Interest

One of the six legal bases for processing personal data outlined by the General Data Protection Regulation is processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Public Key Infrastructure

A system of digital certificates, authorities and other registration entities that verifies the authenticity of each party involved in an electronic transaction through the use of cryptography.

Acronym(s): PKI

Associated term(s): Cryptography

Public Records

Information collected and maintained by a government entity and available to the general public.

Public Records (EU specific)

Information collected and maintained by a government entity and available to the general public. In the General Data Protection Regulation, one of the derogations left to member states is an allowance for restrictions on certain data subject rights, such as the

right to erasure, for the keeping of public records kept for reasons of general public interest.

Publicity Given to Private Life

A U.S. common law tort that states: "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person and (b) is not of legitimate concern to the public." (Restatement (Second) of Torts § 652D)

Link to text of: Restatement (Second) of Torts § 652D

Associated term(s): Common Law

Publicly Available Information

Information that is generally available to a wide range of persons. Some traditional examples include names and addresses in telephone books and information published in newspapers or other public media. Today, search engines are a major source of publicly available information.

Purpose Limitation

A fair information practices principle, part of the original OECD Guidelines, and a piece of many privacy and data protection regulations, this is the principle that the purposes for which personal data are collected should be specified no later than at the time of data collection and the subsequent use of that personal data is limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified to the individual on each occasion of change of purpose, or for which there is a further legal basis that would not require notification.

Associated term(s): Principle of Finality

Associated law(s): EU Data Protection Directive

Purpose Specification

See "Purpose Limitation".

Associated term(s): FIPs

Qualified Protective Order

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.

Acronym(s): QPO

Associated law(s): HIPAA

Associated terms: PHI

Quality Attributes

Concerns in software development that cannot be alleviated with a single design element or function. Privacy is an example of a quality attribute that can be divided up into further quality attributes (think about the Fair Information Practices). Using Privacy by Design in all software development allows these quality attributes to be accounted for in all system functions as they are being developed.

Associated term(s): Privacy by Design, Fair Information Practices

Quantum encryption

Uses the principles of quantum mechanics to encrypt messages in a way that prevents anyone other than the intended recipient from reading them.

Radio-Frequency Identification

Technologies that use radio waves to identify people or objects carrying encoded microchips.

RFID chips are tiny microchips that can be as small as a fraction of a millimetre. Each microchip is identified by a unique serial number and contains an antenna with which it transmits information, such as its serial number, to an RFID reader. RFID chips can be placed on products or cards…for tracking purposes. They are commonly used in supply chain management to allow companies to track inventory.

Acronym(s): RFID

Random Testing

Substance testing sometimes required by law, prohibited in certain jurisdictions, but acceptable where used on existing employees in specific, narrowly defined jobs, such as those in highly regulated industries where the employee has a severely diminished expectation of privacy or where testing is critical to public safety or national security.

Associated term(s): Substance Testing

Re-identification

The action of reattaching identifying characteristics to pseudonymized or de-identified data (see De-identification and Pseudonymization) . Often invoked as a "risk of re-identification" or "re-identification risk," which refers to nullifying the de-identification actions previously applied to data (see De-identification).

Associated term(s): De-identification; Anonymization; Anonymous Data, Pseudonymous Data

REAL ID Act

The REAL ID Act of 2005 is a nationwide effort intended to prevent terrorism, reduce fraud and improve the reliability and accuracy of identification documents issued by U.S. state governments. The act has many varying provisions, but the one generating the most interest and controversy concerns the establishment and implementation of national standards for state-issued driver's licenses and non-driver ID cards. On January 11, 2008, the U.S. Department of Homeland Security issued a final rule establishing the minimum-security standards for state-issued identification cards. The new standards purportedly enhance the card's integrity and reliability, strengthen issuance capabilities, increase security at card-production facilities and reduce state implementation costs.

Link to text of law: REAL ID Act of 2005

Reasonable Suspicion

A determining factor in substance testing where testing is allowed as a condition of continued employment if there is "reasonable suspicion" of drug or alcohol use based on specific facts as well as rational inferences from those facts; i.e., appearance, behavior, speech, odors.

Associated term(s): Substance Testing

Record-Keeping Obligation

Article 30 of the General Data Protection Regulation specifies circumstances that will trigger the record-keeping obligation. These include, for organizations of 250 or more employees, all processing of personal data. Or, regardless of the organization's size, controllers and processors are obligated to keep records of the processing if it is likely to result in a risk to the rights and freedoms of data subjects; is not occasional; or includes special categories of data or data relating to criminal convictions and offences.

Rectification

An individual's right to have personal data about them corrected or amended by a business or other organization if it is inaccurate.

Associated term(s): Access

Associated law(s): EU Data Protection Directive; FCRA

Rectification (EU specific)

Closely intertwined with access, rectification is the right or ability of a data subject to correct erroneous information that is stored about them. Under the General Data Protection Regulation, data subjects have the right to rectification of inaccurate personal data, and controllers must ensure that inaccurate or incomplete data is erased, amended or rectified.

Red Flags Rule

A regulation created by the Federal Trade Commission (FTC) under the authority of the Fair and Accurate Credit Transactions Act of 2003. This regulation requires financial institutions and creditors to implement measures to detect and prevent identity theft. The original FTC rule was circumscribed by the Red Flag Program Clarification Act of 2010, which limited the definition of "creditors" to exclude any creditor "that advances funds on the behalf of a person for expenses incidental to a service." The act in effect allowed lawyers, some doctors and other service type companies to avoid implementing Red Flag credit measures.

Link to text of law: Red Flag Program Clarification Act of 2010

Associated term(s): Federal Trade Commission

Associated law(s): Fair and Accurate Credit Transactions Act of 2003

Redaction

The practice of identifying and removing or blocking information from documents being produced pursuant to a discovery request or as evidence in a court proceeding. Specifically, attorneys are required to redact documents so that no more than the following information is included in court filings: (1) The last four digits of the Social Security number and taxpayer-identification number; (2) the year of the individual's birth; (3) if the individual is a minor, only the minor's initials, and (4) the last four digits of the financial account number.

Associated term(s): Protective Order

Remarketing

An advertising strategy that leverages information learned from an initial consumer interaction to market to the same consumer multiple times in a digital or physical environment.

Remedies, Liability and Penalties

Chapter VII of the General Data Protection Regulation outlines the remedies available to data subjects and their right to compensation, the liability for damage caused by processing for both controllers and processors, and the penalties available to supervisory authorities for infringement of the law.

Remnant Advertising

The most basic, stripped down form of web advertising that occurs when no data about the user or webpage is available. Advertising of this sort has no personalization.

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

Repurposing
Taking information collected for one purpose and using it for another purpose later on.

Associated term(s): Active Collection, First-party Collection, Passive Collection, Surveillance Collection, Third-party Collection

Resilience
The ability to withstand and recover from threats. The General Data Protection Regulation requires that controllers and processors, in proportion to risk, be able to ensure the resilience of processing systems and services.

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

Retargeting
A type of online advertising where visitors to a website are targeted with ads related to that website as they browse elsewhere. The most common form of retargeting is a digital advertising network, which leverages retargeting to display advertisements to a user related to a website previously visited by the user across all third-party websites in a network.

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

Retention (EU specific)
Within the information life cycle the concept that organizations should retain personal information only as long as necessary to fulfill the stated purpose. Under the General Data Protection Regulation, the "right to be forgotten" exists where the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, where a data subject has withdrawn their consent or objects to the processing of personal data concerning them, or where the processing of their personal data does not otherwise comply with the GDPR, unless there are other legal obligations or reasons of the public interest to retain their personal data.

Return on Investment

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.

Acronym(s): ROI

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

Right of Access

An individual's right to request and receive their personal data from a business or other organization.

Right To Be Forgotten

An individual's right to have their personal data deleted by a business or other organization possessing or controlling that data.

Associated term(s): le droit à l'oubli; right of oblivion

Right To Correct

The right for individuals to correct or amend information about themselves that is inaccurate.

Right to Deletion

An individual's right to have their personal data deleted by a business or other organization possessing or controlling that data.

Right to Financial Privacy Act of 1978

Governs the release of customer financial information to federal government authorities. The act defines both the circumstances under which a financial institution can volunteer information about customers' financial records to federal government authorities and the applicable procedures and requirements to follow when the federal government is requesting customers' financial information.

Link to text of law: Right to Financial Privacy Act of 1978

Acronym(s): RFPA

Right to No Sale

An individual's right to prohibit or restrict the transfer of information for value from a business to a third party.

Right to Object

An individual's right to object to the processing of their personal data by a business or other organization. An entity is obligated to review an individual's objection and respond to it.

Right To Object to Automated Decision-Making

In the General Data Protection Regulation, the right not to be subject to automated decision-making applies if such a decision is based solely on automated processing and produces legal effects concerning the data subject or similarly significantly affects them. If a decision-making process falls within these parameters, the underlying processing of personal data is only allowed if it is authorized by law, necessary for the preparation and execution of a contract, or done with the data subject's explicit consent, provided that the controller has put sufficient safeguards in place.

Right to Privacy, The

An 1890 law review article by Louis Brandeis and Samuel Warren arguing that privacy is the right to be left alone, and that the violation of this right should give rise to a tort.

Link to article: Right to Privacy

Associated term(s): Right To Be Forgotten

Right to Restriction

An individual's right to limit or prohibit a business or other organization from processing their personal data.

Risk Assessment Factors

The following constitute risk assessment factors: Number of breaches; number of outages; unauthorized access; lost assets; software viruses; investigations.

Role-Based Access Controls

Access policies that espouse the view that no employee should have greater information access than is necessary to capably perform his or her job function.

RSA Encryption

RSA (Rivest-Shamir-Adleman) is the most common internet encryption and authentication system. The system used an algorithm that involves multiplying two large prime numbers to generate a public key, used to encrypt data and decrypt an authentication, and a private key, used to decrypt the data and encrypt an authentication.

Associated term(s): Encryption

Run time behavior monitoring

Monitoring and analyzing usage and data collected from a running system.

Safe Harbor

See EU-U.S. Safe Harbor Agreement

Sarbanes-Oxley Act

A United States law, passed in 2002, regulating the transparency of publicly held companies. In particular, public companies must establish a way for the company to confidentially receive and deal with complaints about actual or potential fraud from misappropriation of assets and/or material misstatements in financial reporting from so-called "whistle-blowers."

Link to text of law: Sarbanes-Oxley Act

Acronym(s): SOX

Related term(s): Whistle-Blowing

Sarbanes-Oxley Act (EU specific)

A United States law, passed in 2002, regulating the transparency of publicly held companies. In particular, public companies must establish a way for the company to confidentially receive and deal with complaints about actual or potential fraud from misappropriation of assets and/or material misstatements in financial reporting from so-called "whistle-blowers." U.S. companies with EU subsidiaries or affiliates are bound by both SOX and EU data protection law, thus potentially leading to conflicting obligations, specifically in regards to protecting the identity of the whistle-blower (SOX) vs. protecting the personal data of the employee accused of wrongdoing (EU data protection law).

Schrems I

Colloquial term for Maximillian Schrems v Data Protection Commissioner. See "Max Schrems." The case challenged the Irish DPC's refusal to investigate a complaint by Max Schrems asking the DPC to suspend data transfers from Facebook Ireland to Facebook Inc. due to Mr. Schrems' concern that the Snowden revelations suggested his personal

data could be accessed by U.S. intelligence authorities and that his EU data protection rights would be violated. At the time, Facebook relied on the U.S.-EU Safe Harbor Framework as the legal basis for personal data transfers under the EU Data Protection Directive. The Irish High Court referred the case to the CJEU. In 2015, the CJEU ruled that the European Commission's adequacy determination for the U.S.-EU Safe Harbor Framework was invalid, which led to the creation of the EU-U.S. Privacy Shield (see "EU-U.S. Privacy Shield"). In a separate case, often referred to as "Schrems II" (see "Schrems II"), the CJEU invalidated the European Commission's adequacy determination for Privacy Shield after Schrems amended his complaint of Facebook Ireland to the Irish Data Protection Commissioner.

Schrems II (aka Schrems 2.0)

Colloquial term for Data Protection Commission (Ireland) v. Facebook & Schrems. See "Max Schrems." The Irish Data Protection Commission brought the case to the Irish High Court seeking a referral to the CJEU (see "CJEU"). The Irish High Court referred 11 specific questions to the CJEU related to the use of EU-approved data transfer mechanisms, which the DPC felt required answers before completing its investigation into the validity of Facebook Ireland's transfers of Max Schrems' personal data to Facebook Inc, using standard contractual clauses as the legal basis for transfers. The case challenged the validity of standard contractual clauses for the transfer of personal data from the EU to the United States, on the same grounds Schrems used to challenge the Safe Harbor adequacy agreement (see "Schrems I"). On July 16, 2020, the Court of Justice of the European Union invalidated the European Commission's adequacy determination for Privacy Shield, and placed additional requirements for companies using standard contractual clauses to third countries outside the EU.

Seal Programs

Programs that require participants to abide by codes of information practices and submit to monitoring to ensure compliance. In return, companies that abide by the terms of the seal program are allowed to display the programs seal on their website.

Associated term(s): Self-regulatory Model, WebTrust

Secondary use

Using an individual's information without consent for purposes unrelated to the original reasons for which it was collected.

Secret Key

"A cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities and which shall not be made public. The use of the term "secret" in this context does not imply a classification level, rather the term implies the need to protect the key from disclosure or substitution." (Federal Information Processing Standards Publication 140-1, Security Requirements for Cryptographic Modules)

Section 208 of the E-Government Act

Section 208 requires agency website privacy policies to include the following information: what information is to be collected through use of the website; why the information is being collected; the intended use by the agency of the information; with whom the information will be shared; what notices or opportunities for consent will be provided; how the information will be secured; the rights of individuals under the Privacy Act and other privacy laws.

Link to text of law: Section 208 of the E-Government Act

Link to text of law: E-Government Act

Associated term(s): E-Government Act

Sectoral Laws/Model

Laws that exist only in areas where the legislative body has found a particular need.

Related term(s) Comprehensive Laws, Co-regulatory Model, Self-regulatory Model, Technology Based Model

Sectorial Laws

Used to distinguish from omnibus laws (see Omnibus Laws), to mean laws that cover a a specific market sector or population, rather than a broad portion of the market or citizenry.

Secure Sockets Layer

A protocol for establishing a secure connection for transmission that facilitates much of the online commerce that occurs on the Internet today. For example, HTTPS, a secure form of HTTP, is an SSL application used in password exchanges or e-commerce. “The primary goal of the SSL protocol is to provide privacy and reliability between two communicating applications.” The protocol has three main properties: (1) The connection is private; (2) the peer’s identity can be authenticated using asymmetric, or public key, cryptography, and (3) the connection is reliable.

Acronym(s): SSL

Related term(s): HTTP, HTTPS, TLS

Security Policy

Encompasses internal security measures such as the prevention of unauthorized or unnecessary access to corporate data or resources. Includes intellectual property, financial data and personal information. Physical security measures, such as locks, safes, cameras and fences are security measures that protect against both internal and external threats.

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.

Sedona Conference

An important source of standards and best practices for managing electronic discovery compliance through data retention policies. Regarding email retention, the Sedona Conference offers four key guidelines:

Email retention policies should be administered by interdisciplinary teams composed of participants across a diverse array of business units;

such teams should continually develop their understanding of the policies and practices in place and identify the gaps between policy and practice;

interdisciplinary teams should reach consensus as to policies while looking to industry standards;

technical solutions should meet and parallel the functional requirements of the organization.

Link to: Sedona Conference

Associated term(s): Data retention, e-Discovery

Self-Regulation Model, The

Self-regulation refers to stakeholder-based models for ensuring privacy. The term "self-regulation" can refer to any or all of three pieces: legislation, enforcement and adjudication. Legislation refers to question of who defines privacy rules. For self-regulation, this typically occurs through the privacy policy of a company or other entity, or by an industry association. Enforcement refers to the question of who should initiate enforcement action. Actions may be brought by data protection authorities, other government agencies, industry code enforcement or, in some cases, the affected individuals. Finally, adjudication refers to the question of who should decide whether an organization has violated a privacy rule. The decision maker can be an industry association, a government agency or a judicial officer. These examples illustrate that the term "self-regulation" covers a broad range of institutional arrangements. For a clear understanding of data privacy responsibilities, privacy professionals should consider who defines the requirements, which organization brings enforcement action and who actually makes the judicial decisions.

Associated term(s): Comprehensive Laws, Co-regulatory Model, Online Privacy Alliance, Sectoral Laws, Seal Programs, Technology Based Model

Semayne's Case

A case recognized as establishing the "knock-and-announce rule," an important concept relating to privacy in one's home and Fourth Amendment search and seizure jurisprudence in the U.S.

Link to: Fourth Amendment

Senate (Canadian)

One of two chambers of the Canadian Parliament, along with the House of Commons. Unlike the House of Commons, whose members are elected, the Senate is appointed by the governor in council based upon the recommendations of the prime minister.

Associated term(s): Canadian Parliament, House of Commons

Senior Agency Official for Privacy

Under OMB Memorandum M-05-08, each executive agency should identify the senior official who has agency-wide responsibility for information privacy. The agency's chief information officer (CIO) may perform this role, or it may be performed by another senior official at the assistant secretary or equivalent level. Agencies are also advised that the official given this role should have the authority to address information privacy policy issues at a national and agency-wide level. The official has overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including full compliance with federal laws, regulations and policies relating to information security, such as the Privacy Act.

Link to text of: Memorandum M-05-08

Acronym(s): SAOP

Sensitive Personal Information

Data which is more significantly related to the notion of a reasonable expectation of privacy, such as medical or financial information. However, data may be considered more or less sensitive depending on context or jurisdiction. Recently the U.S. Federal Trade Commission classified TV-viewing data as "sensitive."

Acronym(s): SPI

Separate

Separating personal data during processing to prevent correlating information that may lead to the identification of the individual. This is done via processing data in physically separate locations (distribute) or isolating the data by processing personal data that is used for different purposes in separate databases.

Single-Factor Authentication
The standard authentication mechanism that requires a user name and password for access.

Associated term(s): Multi-factor authentication, Authentication, Authorization

Single-Sign-On (SSO)

An authentication process that allows the user to enter a single set of credentials to access multiple applications.

Six Major European Union Institutions, The
The European Parliament, the European Council, the European Commission, the Court of Justice of the European Union, the European Central Bank and the Court of Auditors.

Smart Grid
An energy system that manages electricity consumption through continuous monitoring, remote computerization and automation. The traditional electric transmission system required physically sending workers into the field to periodically read customer meters and find where problems existed in the grid. Smart grid operators; however, can remotely monitor and control the use of electricity to each home or business.

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

Software Requirements Specification
A formal documentation of a software system or product to be developed that includes both functional and nonfunctional requirements. These are used so that the individual tasked with creating the system or product is aware of the needs of the individual seeking the creation.

Acronym: SRS

Associated term(s): Functional Requirements, Non-functional requirements, Plan-driven Development Model, Agile Development Model

SPAM
Unsolicited commercial e-mail.

Associated law(s): CASL; CAN-SPAM Act

Spear Phishing

Phishing targeted at a particular group of people with a known affiliation to some organization.

Associated term(s): Phishing, Whaling, Pharming

Special Categories of Data

As defined in Article 9 of the General Data Protection Regulation, personal information that reveals, for example, racial origin, political opinions or religious or other beliefs, as well as personal data that concerns health or sexual life or criminal convictions is considered to be in a special category and cannot be processed except under specific circumstances.

Associated term(s): Sensitive Personal Data

Speech recognition

Voice command technology that allows users to interact with and control technologies by speaking to them.

SQL Injection

Taking advantage of SQL forms by inserting commands in information entry boxes. SQL is transferred in such a way that commands placed in forms can be seen as valid commands and affect the system in whatever way that command operates. Hackers can use SQL Injections to erase data banks, over load servers, etc. if the SQL isn't properly set up to avoid such attacks.

Associated term(s): SQL

Stakeholders

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

Standard Model Clauses

See "Contractual Clauses."

Associated term(s): European Data Protection Directive

Standardized Icons

The General Data Protection Regulation permits "visualisation" to be used to provide fair processing information to data subjects where appropriate and makes provision for the use of standardized icons to give an easily visible, understandable and meaningful overview of the processing.

Storage Encryption

The use of encryption to protect stored or backed-up data both in transit and in the storage medium to provide an additional layer of security.

Storage Limitation

The principle that personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods if it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organizational measures required to safeguard the rights and freedoms of the data subject.

Stored Communications Act

The Stored Communications Act was enacted as part of Electronic Communications Privacy Act in 1986 in the United States. It generally prohibits the unauthorized acquisition, alteration or blocking of electronic communications while in electronic storage in a facility through which an electronic communications service is provided.

Link to text of law: Stored Communications Act

Acronym(s): SCA

Associated law(s): The Electronic Communications Privacy Act of 1986 (ECPA)

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.

Structured Query Language

A special-purpose programming language that allows for the creation of interactive forms which users can insert, alter and delete data they have input, and the system administrators can easily transfer information into usable data banks of user

information. Originally developed by IBM, SQL has become an international standard for data collection and use.

Acronym: SQL

Associated term(s): SQL Injection

Subjective Harm

Exists without an observable or measurable harm, but where an expectation of harm exists.

Subpoena

A written court order issued in an administrative, civil or criminal action that requires the person named in the subpoena to appear in court in order to testify under oath on a particular matter which is the subject of an investigation, proceeding or lawsuit. A subpoena may also require the production of a paper, document or other object relevant to an investigation, proceeding or lawsuit that discloses personal information.

Substance Testing

A screening to identify drug use. Substance testing can be used in a variety of settings such as preemployment, reasonable suspicion, routine testing, post-accident testing or randomly.

Associated terms(s): Americans with Disabilities Act, Random Testing, Reasonable Suspicion

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

Super Cookie

A tracking mechanism that persists even after all cookies have been deleted, usually using several varying types of storage to remain within a device.

Associated term(s): Cookie

Supervisory Authority

An independent public authority established by an EU member state, responsible for monitoring the application of the General Data Protection Regulation.

Supply Side Platform (SSP)

Analogous to a demand side platform (DSP), an SSP enables publishers to access demand from a wide variety of networks, exchanges, and platforms via one interface.

Surveillance

The observation and/or capturing of an individual's activities.

Surveillance Collection

Collection by way of observing the data stream produced by a given data subject without interference in the data subject's activity.

Associated term(s): Active Collection, First-Party Collection, Passive Collection, Repurposing, Third-party Collection

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

Symmetric Key Encryption

Also known as Secret Key Encryption is a form of encryption using a single secret key to both encrypt and decrypt data.

Associated term(s): Asymmetric Key Encryption, Encryption

Syndicated Content

Content that is not actually created by the host site, but is developed, purchased or licensed from a third party. A concern associated with this content is that it can contain malicious code that is then unwittingly incorporated into the organization's own website

source code. For example, cross-site scripting (XSS) attacks attempt to take advantage of the trust that users have for a given site.

Associated term(s): XSS

System of Records Notice

A notice required when a federal agency creates, modifies or destroys a system of records. When the agency collects and stores Personally Identifiable Information in records, the agency is required to establish the statutory need for the collection, disclose the collection, describe its contents and declare the routine uses for that agency or any other agency that will use the information. This disclosure must be made to the Office of Management and Budget and Congress and must be published in the Federal Register in advance of the system becoming operational.

Acronym(s): SORN

Associated law(s): Privacy Act

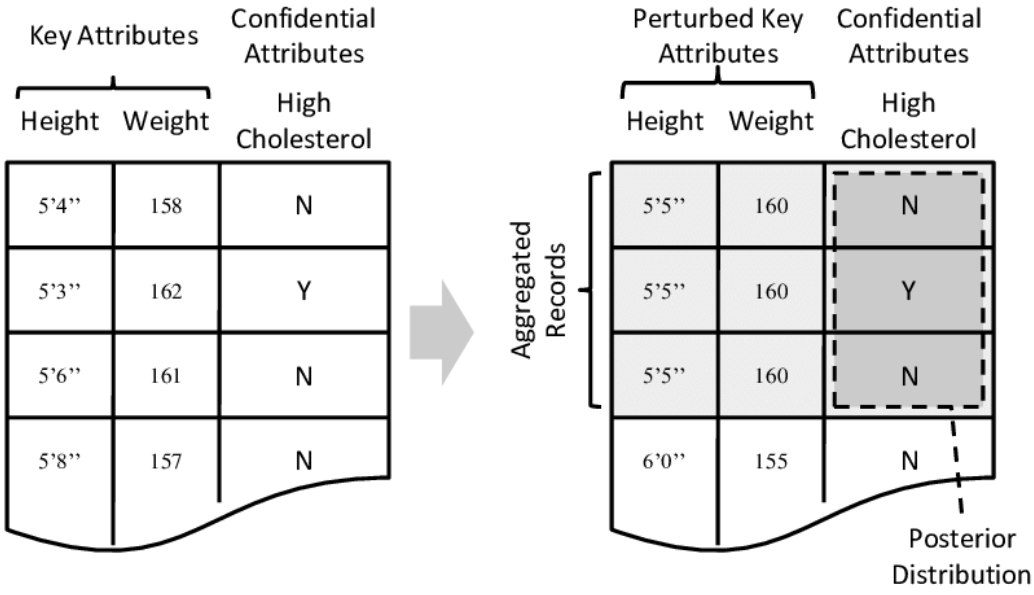
Systems Development Life Cycle (SDLC)

A conceptual model used to describe the stages in an information system development project.

Associated term(s): Privacy by Design, Privacy Standard, Privacy Review

t-closeness

Extends l-diversity by reducing the granularity of data in a data set. It protects attribute disclosure. Whereas, k-anonymity protects identity disclosure.



Credit: ResearchGate.net

Technology-Based Model

The technology-based model for data protection utilizes technological security measures to protect individual's personal data. While it is commonplace for companies to utilize technology to protect data, developments in commercially available hardware and software have enabled consumers to establish privacy protections for their own online activity.

Associated term(s): Comprehensive Laws, Co-regulatory Model, Sectoral Laws, Self-Regulation Model

Telephone Consumer Protection Act of 1991

The first enactment of laws limiting unsolicited and automated telemarketing for both telephone and fax communications. Most notably the act creates a private right of action for those receiving unsolicited faxes, carrying a $500 fine per violation and any damages sustained because of the fax. The Telephone Consumer Protection Act also gives rule-making authority to the Federal Communications Commission, allowing it to make further regulations in this area. Among other provisions, the act prevents faxing without consent from the recipient (this requirement was amended by the Junk Fax Prevention Act of 2005 to not include customers with an existing business relationship) and requires companies to create and honor internal do-not-call registries (in 2003 the National Registry was created by the Federal Trade Commission).

Link to text of law: Telephone Consumer Protection Act

Acronym: TCPA

Associated term(s): Junk Fax Prevention Act of 2005, Federal Communications Commission, Federal Trade Commission

Terms of Service

The set of rules which govern the use of a service and must be agreed to, either implicitly through the use of that service or explicitly, in order to make use of that service.

Associated term(s): EULA

Territorial Privacy

One of the four classes of privacy, along with information privacy, bodily privacy and communications privacy. It is concerned with placing limitations on the ability of one to intrude into another individual's environment. Environment is not limited to the home; it may be defined as the workplace or public space and environmental considerations can be extended to an international level. Invasion into an individual's territorial privacy

typically comes in the form of video surveillance, ID checks and use of similar technology and procedures.

Associated term(s): Home Privacy

Territorial Scope

"The jurisdictional reach of a law or regulation. In the case of the General Data Protection Regulation, it applies to organizations

established in the EU and to their third-party processors of personal data, wherever they happen to be located, and to those organizations that offer goods or services to, or monitor, individuals in the EU."

The Data Quality Act

In light of the increased use of the Internet by federal agencies as an easy, inexpensive and expedient way to disseminate information to the public, Congress passed the Data Quality Act of 2000. This act was designed to ensure the quality of information released by federal agencies. The DQA's impact on individual privacy is limited and indirect, as its principal focus is on the quality, and not the confidentiality, of information intended for publication. That said, DQA data quality procedures overlap with the data quality and integrity requirements of the Privacy Act when an agency collects, generates or uses individual-level data in an agency system of records to prepare or support published studies or research covered by the DQA.

Link to text of law: The Data Quality Act

Acronym(s): DQA

Associated term(s): Terms

Associated law(s): Privacy Act

Third-Party Collection

Data acquired from a source other than directly from the subject of the data.

Associated term(s): Active Collection, First-party Collection, Passive Collection, Repurposing, Surveillance Collection

Tokenization

A system of de-identifying data which uses random tokens as stand-ins for meaningful data. Tokenization is a variation of pseudonimization.

Traffic Data

This refers to any data processed for the purpose of the conveyance of a communication on an Electronic Communications Network or for the billing thereof. Traffic data includes information about the type, format, time, duration, origin, destination, routing, protocol used and the originating and terminating network of a communication. For example, in relation to a telephone call, traffic data includes, among other information, the phone numbers of the caller and call recipient; in relation to an e-mail, the e-mail addresses of the sender and recipient' and the size of any attachments.

Transfer

The movement of personal data from one organization to another.

Transient Storage

Short lifespan data storage such as a session cookie stored on a browser that is purged from the system when the browser is closed.

Associated term(s): Persistent Storage, Cookies

Transit

The automatic forwarding of data packets from one server to another.

Transmission Control Protocol

A protocol which enables two devices to establish a connection and exchange data. A combination of TCP and IP is used to send data over the Internet. Data are sent in the form of a packet, which is a portion of a message sent over the TCP/IP network. It contains content and a heading that specifies the destination.

Acronym(s): TCP; TCP/IP

Transparency

Taking appropriate measures to provide any information relating to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language.

Transport Layer Security

A protocol that ensures privacy between client-server applications and Internet users of the applications. When a server and client communicate, TLS secures the connection to ensure that no third party can eavesdrop on or corrupt the message. TLS is a successor to SSL.

Acronym(s): TLS

Associated term(s): Secure Sockets Layer (SSL)

Treaty of Lisbon

Signed in 2007, and effective in 2009, its main aim was to strengthen and improve the core structures of the European Union to enable it to function more efficiently. The Lisbon Treaty amends the EU's two core treaties, the Treaty on European Union and the Treaty Establishing the European Community. The treaty ensures that all institutions of the European Union must protect individuals when processing personal data. It also established a European Data Protection Supervisor whose role is to regulate compliance with data protection law within the institutions of the European Union, but its references to "authorities"' implies that the national data protection authorities may also have jurisdiction in such matters.

Link to: Treaty of Lisbon

Link to: Treaty on European Union

Link to: Treaty Establishing the European Community

Associated term(s): Lisbon, EDPS

Trojan Horse

A form of malware in which bad software masquerades as beneficial software.

Associated term(s): Malware

U.S. Department of Labor

A U.S. federal agency that oversees "the welfare of the job seekers, wage earners and retirees of the United States by improving their working conditions, advancing their opportunities for profitable employment, protecting their retirement and healthcare benefits, helping employers find workers, strengthening free collective bargaining and tracking changes in employment, prices and other national economic measurements." To achieve this mission, the department administers a variety of federal laws including, but not limited to, the Fair Labor Standards Act (FLSA), the Occupational Safety and Health Act (OSHA) and the Employee Retirement Income Security Act (ERISA).

Link to: U.S. Department of Labor

Link to text of act: Fair Labor Standards Act

Link to text of act: Occupational Safety and Health Act

Link to text of act: Employee Retirement Income Security Act

Acronym(s): DOL

Associated law(s): FLSA; ERISA, OSHA

Ubiquitous computing

The processing of information is linked with the activity or object it encounters.

Unambiguous Consent

Where actions by a data subject lead to an unmistakable conclusion that consent has been provided; where consent meets the standard of being a "freely given, specific and informed" indication of an individual's wishes. This is the baseline standard for consent in the General Data Protection Regulation.

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

Unified Modeling Language

A notation language that is used to describe system design elements in software development.

Acronyms: UML

Associated term(s): Plan-driven Design Model, Agile Design Model

Uniform Resource Locator

The address of content located on a web server. Specifically, it is the letter and number coordinates that an end user submits to the web browser to instruct it to connect with the desired website. An example of a URL is "https://iapp.org."

Acronym(s): URL

United States Department of Health, Education and Welfare Fair Information Practice Principles (1973)

A code of fair information practices that contains five principles:

There must be no personal data record keeping systems whose very existence is secret.

There must be a way for an individual to find out what information about him (or her) is in a record and how it is used.

There must be a way for an individual to prevent information about him (or her) that was obtained for one purpose from being used or made available for other purposes without his (or her) consent.

There must be a way for an individual to correct or amend a record of identifiable information about him (or her).

Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Link to text of: United States Department of Health, Education and Welfare Fair Information Practice Principles (1973)

Associated term(s): HEW Principles; HEW Report, The

Universal Declaration of Human Rights

Also called the Human Rights Declaration, the declaration recognized the universal values and traditions of inherent dignity, freedom, justice and peace. It was adopted by the General Assembly of the United Nations on 10 December 1948. In December 1948, the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights. This declaration formally announced that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence [.]" The statement was intended to encompass a wide range of conduct, as evidenced by Article 12 of the Declaration, which describes both the territorial and the communications notions of privacy.

Link to text of: Universal Declaration of Human Rights

Associated term(s): Declaration of Human Rights

Urgency Procedure

According to the General Data Protection Regulation, in exceptional cases where there is an urgent need to protection individuals' rights and freedoms, a supervisory authority can bypass the cooperation procedures and consistency mechanism (see Consistency Mechanism) to adopt provisional measures in its country, after which it should notify other regulators who have an interest in the matter, the Commission and the European Data Protection Board. The supervisory authority can apply to the EDPB for an urgent opinion or decision where it feels that final measures are needed, and any regulator can apply for an urgent opinion or decision where it feels that another regulator has failed to take appropriate action in a case of urgency.

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.

Link to: National Cyber Alert System

Link to: U.S. Computer Emergency Readiness Team

Acronym(s): US-CERT

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

USA PATRIOT Act

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 is a broad-ranging act designed to counter terrorism that expanded U.S. law enforcement authority to surveillance and capturing communications and records. Commonly referred to as the Patriot Act.

Link to text of act: USA PATRIOT Act

Use Limitation

See "Purpose Limitation."

Link to text of memo: Fair Information Practice Principles

Associated term(s): Fair Information Practices

User Stories

Requirements of new software systems or products as they are implemented in an Agile Development Model. Usually they consist of a few sentences that describe how a consumer would interact with the system or product and what the ideal functionality

would look like. These are used to inform the developers of how a system or product should work while they are designing a given portion of the system.

Associated term(s): Agile Development Model, SRS

User-based access controls

Rely on the identity of the user to determine whether to grant or deny access to a desired resource.

Value-Added Services

A telecommunications industry term for non-core services; i.e., services beyond voice calls and fax transmissions. More broadly, the term is used in the service sector to refer to services, which are available at little or no cost, and promote their primary business. For mobile phones, while technologies like SMS, MMS and GPRS are usually considered value-added services, a distinction may also be made between standard (peer-to-peer) content and premium-charged content. These are called mobile value-added services (MVAS), which are often simply referred to as VAS. Value-added services are supplied either in-house by the mobile network operator themselves or by a third-party value-added service provider (VASP), also known as a content provider (CP) such as Headline News or Reuters. VASPs typically connect to the operator using protocols like short message peer-to-peer protocol (SMPP), connecting either directly to the short message service centre (SMSC) or, increasingly, to a messaging gateway that gives the operator better control of the content.

Associated term(s): MVAS, VASP

Value-Sensitive Design

A design approach that accounts for moral and ethical values. Values include privacy, trust, fairness, informed consent, courtesy or freedom from bias. Assess the values in relation to specific technologies and stakeholders.

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.

Verification

Refer to definition for Authorization.

Video Surveillance

Recordings that do not have sound.

Associated term(s): Video Surveillance Guidelines

Associated law(s): FISA

Video Surveillance Guidelines

Guidelines discouraging video as an initial security option with the following constraints: (1) Video should be taken only in the absence of less intrusive alternatives; (2) the use should be disclosed to the public; (3) individuals should have access to their personal information; (4) video surveillance should be subject to independent audit, and (5) fair information practices should be respected.

Virtual Private Network

A network that uses primarily public telecommunication infrastructure, such as the Internet, to provide remote offices or traveling users an access to a central organizational network. VPNs typically require remote users of the network to be authenticated and often secure data with encryption technologies to prevent disclosure of private information to unauthorized parties.

Acronym(s): VPN

Associated term(s): Remote Access Connectivity

Vital Interests

Protecting "vital interests" refers to circumstances of life or death — in other words, where the processing of personal data contemplated is vital to an individual's survival. For example, under the European General Data Protection Regulation, processing of personal data that necessary in order to protect the vital interests of the data subject or of another natural person is one of the six legal bases for processing personal data. This criterion will be relevant only in rare emergency situations such as health care settings, humanitarian response, and law enforcement.

Voice Over Internet Protocol

A technology that allows telephone calls to be made over a LAN or the Internet itself. Skype is a well-known example. VoIP poses the same risk as network-connected PBX systems but also poses the additional risk of data interception when such data travel over an unsecured connection. VoIP functionality should be encrypted where possible and equipment monitored with intrusion-detection systems.

Acronym(s): VoIP

Vulnerability management

Assessing and developing plans for the capability and probability that a threat actor's acts will succeed.

Web Beacon

Also known as a web bug, pixel tag or clear GIF, a web beacon is a clear graphic image (typically one pixel in size) that is delivered through a web browser or HTML e-mail. The web beacon operates as a tag that records an end user's visit to a particular web page or viewing of a particular e-mail. It is also often used in conjunction with a web cookie and provided as part of a third-party tracking service. Web beacons provide an ability to produce specific profiles of user behavior in combination with web server logs. Common usage scenarios for web beacons include online ad impression counting, file download monitoring, and ad campaign performance management. Web beacons also can report to the sender about which e-mails are read by recipients. Privacy considerations for web beacons are similar to those for cookies. Some sort of notice is important because the clear pixel of a web beacon is quite literally invisible to the end user.

Associated term(s): Web Bug, Pixel Tag, Tracking Bug, Clear GIF

WebTrust

Created by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). It is a self-regulating seal program which licenses qualifying certified public accountants.

Associated term(s): Seal Programs

Whaling

Phishing targeted at a specific individual or individuals known to be wealthy.

Associated term(s): Spear Phishing, Phishing, Pharming

Whistleblowing

If illegal or improper activity is taking place within an organization, employees may first observe it and report it to individuals with more authority or an agency outside of the organization. In setting up procedures to make it possible for an employee to report such activity, per laws in a variety of jurisdictions that protect the rights of these so-called whistleblowers, an organization will want to be sure that appropriate privacy safeguards are put in place.

Associated term(s): Whistleblower

Associated law(s): Sarbanes-Oxley Act

Wide Area Network

A non-localized telecommunications network that can be used to transmit data across large regions.

Acronym(s): WAN

Associated term(s): LAN; Local Area Network

Work Product Information

A Canadian term referring to information about an individual that is related to that individual's position, functions and/or performance of his or her job. A term that is undefined by PIPEDA, the privacy commissioner has decided that work product may at times fall under the definition of personal information. Access to such information by the commissioner is addressed on a case-by-case basis. Not to be confused with the American legal term "work product," which refers to legal materials prepared in anticipation of litigation.

Associated term(s): Employee Information

Associated law(s): PIPEDA

Works Councils

Works councils, primarily in the European Union, are bodies that represent employees and have certain rights under local law that affect the use of employee data by employers. Works councils can have a role in deciding whether employees' personal data can be processed because they typically have an obligation to safeguard employee rights, which include data protection and privacy rights. They are most likely to be encountered in a data protection setting in Germany.

Associated term(s): Labor Unions; Unions; Labour Unions

Worm

A computer program or algorithm that replicates itself over a computer network, usually performing malicious actions.

Associated term(s): Flash Worm

For the acronym WORM, see Write Once Read Many.

Write Once Read Many

A data storage device in which information, once written, cannot be modified. This protection offers assurance that the data originally written to the device has not been tampered with. The only way to remove data written to a WORM device is to physically destroy the device.

Acronym(s): WORM