DATA PRIVACY LAWS (GLOSSARY)

A useful guide for Data Privacy Professionals

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

Organisations 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 organisation 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.

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

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

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

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.

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 pseudonymisation, 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 Organisational Measures

The General Data Protection Regulation requires a risk-based approach to data protection, whereby organisations 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.

Article 29 Working Party

The Article 29 Working Party (WP29) was a European Union organisation 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

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

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 organisation 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

Organisations 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.

Behavioural 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 behavioural 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 Behavioural Advertising, Behavioural Targeting, Contextual Advertising, Demographic Advertising, Premium Advertising, Psychographic Advertising, Remnant Advertising

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 organisational group by

means of a single set of binding and enforceable rules. BCRs compel organisations 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 organisations 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 behavioural 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

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 (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).

Bring Your Own Device (BYOD) Policy

A BYOD policy, or bring-your-own-device policy, is a set of rules governing a corporate IT department's level of support for employee-owned PCs, smartphones and tablets.

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.

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

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 organisations 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

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

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.

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 organisations 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.

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 behaviour and apparatus.

Confidentiality

Data is "confidential" if it is protected against unauthorised or unlawful processing. The General Data Protection Regulation requires that an organisation 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.

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.

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.

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.

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.

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 organisations 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.

Case of Copland v United Kingdom [2007] ECHR 253

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 organisation 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.

Reference: Council of the European Union
Associated term(s): Council of Ministers

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
Reference: Court of Justice of the European Union

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, organisations must use other mechanisms, such as binding corporate rules, contractual clauses, or certification, for lawful transfer.

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 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 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 organisation can be both a controller and a processor at the same time, depending on the function the organisation is performing.

Associated term(s): Data Controller, Processor

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 organisational 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).

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 organisations, 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 organisation 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 organisation 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 (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 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.

Reference: Directive 2006/24/EC

Data Subject

An identified or identifiable natural person.

De-identification

An action that one takes to remove identifying characteristics from data.
Acronym(s): De-ID

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.

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 organisation, 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.

Disclosure

The provision of access to personal data.

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.

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

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 organisations, to create an official Do Not Track standard for HTTP headers has of yet led to naught.

Acronym(s): DNT

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.

Reference: Case of Durant v. Financial Services Authority

eCommerce Directive

The Electronic Commerce Directive 2000/31/EC is a European Union Directive of the European Parliament and of the Council from 8 June 2000. It regulates certain legal aspects of information society services in the Internal Market, in particular electronic commerce and mere conduit.

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 Service

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

Acronym(s): ECS

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.

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.

ePrivacy Directive

Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications, otherwise known as ePrivacy Directive, is an EU directive on data protection and privacy in the digital age. It presents a continuation of earlier efforts, most directly the Data Protection Directive.

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 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 EU-U.S. Safe Harbor agreement, the Privacy Shield is an adequacy agreement that allows for the transfer of personal data from the EU to the United States for companies participating in the program. Only those companies that fall under the jurisdiction of the U.S. Federal Trade Commission may certify to the Shield principles and participate, which notably excludes health care, financial services, and non-profit institutions.

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 "everyone 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).

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.

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

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).

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.

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.

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.

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

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.
Case of The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and others (C-213/89)

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

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.

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.

Case of Gaskin v. United Kingdom (Application no. 10454/83)

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

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

Organised 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

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.

Reference: Case of Haralambie v. Romania (21737/03)

Individual Participation

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

Associated term(s): FIPs

Information Life Cycle

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

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

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).

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

ISO 27001

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

ISO 27002

The ISO (International Organisation 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 "organisational security standards and effective security management practices and to help build confidence in inter-organisational activities". It can be considered a guide to implementing ISO 27001 (see ISO 27001).

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).

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.

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

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.

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

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

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.

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).

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 General Data Protection Regulation. Schrems first came notoriety as an Austrian law student, who complained 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 caused the invalidation of the Safe Harbor data-transfer agreement between the EU and U.S. (see "Safe Harbor" and "Privacy Shield"). At the time of this writing, a second case brought by Schrems, known as Schrems 2.0 or Schrems II, seeks to invalidate standard contratual clauses when used to transfer data to the United States from the EU.

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.

Acronym(s): MEPs

Metadata

data that provides information about other data". In short, it's data about data. Meta data can be used to identify individuals. (Traffic data, location data, subscriber data).

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 organisations 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.

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.

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).

Omnibus Laws

Used to distinguish from sectorial laws (see Sectorial Laws), to mean laws that cover a broad spectrum of organisations 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 Behavioural 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.

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 organisation 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.

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 (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 signalling 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 (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.

Organisation for Economic Cooperation and Development

An international organisation 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.

Acronym(s): OECD

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 organisations and their data processing service providers.

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 (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.

Policy Framework

The repository of all an organisation'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 organisation's position regarding a particular policy area.

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.

Prior Authorisation

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

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 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.

Acronym(s): PbD

Privacy Notice (EU specific)

A statement made to a data subject that describes how an organisation 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 organisation's Data Protection Officer. When relying on the legitimate interest ground, the controller must describe the legitimate interests pursued.

Privacy Policy

An internal statement that governs an organisation or entity’s handling of personal information. It is directed at those members of the organisation 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.

Profiling

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

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

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

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 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.

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 fulfilment 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

Record-Keeping Obligation

Article 30 of the General Data Protection Regulation specifies circumstances that will trigger the record-keeping obligation. These include, for organisations of 250 or more employees, all processing of personal data. Or, regardless of the organisation'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 (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.

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.

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.

Retention (EU specific)

Within the information life cycle the concept that organisations should retain personal information only as long as necessary to fulfil 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.

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 organisation.

Right To Be Forgotten

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

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

Right to Object

An individual's right to object to the processing of their personal data by a business or other organisation. 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 Restriction

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

Safe Harbor

See EU-U.S. Safe Harbor Agreement

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 Schrems v. Data Protection Commission (Ireland). See "Max Schrems." After revelations by Edward Snowden of NSA surveillance in the U.S. allegedly involving Facebook's cooperation, Schrems complained to the Irish DPC that Facebook Ireland, the company's European subsidiary, was improperly transferring his data to the U.S. where it could be accessed by the NSA. The data transfers from Facebook Ireland to the U.S. were allowed under the Safe Harbor adequacy decision. However, because Safe Harbor did not limit such U.S. government access for national security purposes, the CJEU (see "CJEU") struck down the Safe Harbor agreement as inconsistent with the European right to privacy. As a result, adequacy is based on the concept of essential equivalence: There must be an adequate level of protection of personal data essentially equivalent to the protection of personal data in the EU.

Schrems II (aka Schrems 2.0)

Colloquial term for Data Protection Commission (Ireland) v. Facebook & Schrems. See "Max Schrems." Being considered by the CJEU (see "CJEU") at the time of this writing, the case challenges 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").

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.

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.

Six Major European Union Institutions

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.

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

Standard Model Clauses

See "Contractual Clauses."

Associated term(s): European Data Protection Directive

Standardised 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 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 organisational measures required to safeguard the rights and freedoms of the data subject.

Supervisory Authority

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

Territorial Scope

"The jurisdictional reach of a law or regulation. In the case of the General Data Protection Regulation, it applies to organisations established in the EU and to their third-party processors of personal data, wherever they happen to be located, and to those organisations that offer goods or services to, or monitor, individuals in the EU."

Traffic Data

This refers to any data processed for the purpose of the conveyance of a communication on a n 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 organisation to another.

Transit

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

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.

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.

Reference: Treaty of Lisbon
Reference: Treaty on European Union
Reference: Treaty Establishing the European Community
Associated term(s): Lisbon, EDPS

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.

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.

Reference: 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.

Use Limitation

See "Purpose Limitation."

Reference: Fair Information Practice Principles
Associated term(s): Fair Information Practices

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.

Whistleblowing

If illegal or improper activity is taking place within an organisation, employees may first observe it and report it to individuals with more authority or an agency outside of the organisation. 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 organisation will want to be sure that appropriate privacy safeguards are put in place.

Associated term(s): Whistleblower
Associated law(s): Sarbanes-Oxley Act

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): Labour Unions; Unions; Labour Unions