GDPR | Glossary of Terms

Article 4 GDPR Definitions

Binding Corporate Rules (BCRs) – a set of binding rules put in place to allow multinational companies and organizations to transfer personal data that they control from the EU to their affiliates outside the EU but within the organization.

Biometric Data – personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that person, such as facial images or dactyloscopic data.

Consent – any 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.

Dactyloscopic Data – identification by comparison of fingerprints.

Data Concerning Health – personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Controller – the natural or legal person, public authority, agency or 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 Union or Member State law.

Data Erasure – also known as the **Right to be Forgotten**, entitles the data subject to have the data controller erase data subject's personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.

Data Portability – the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.

Processor – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Protection Officer (DPO) – An enterprise security leadership role required by the General Data Protection Regulation responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

Data Subject – a natural person whose personal data is processed by a controller or processor.

Derogation – a lessening, weakening or sometimes exemption from a section or requirement in the legislation.

Encrypted Data – personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access.

Genetic Data – personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Identifiable Natural Person – also known as a **Data Subject**. One who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Main Establishment – the place within the Union that the main decisions surrounding data processing are made; with regard to the processor.

Personal Data – any information relating to an identified or identifiable natural person (data subject).

Personal Data Breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy by Design – a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

Privacy Impact Assessment (PIA) – a risk assessment of proposed processing of personal data. If your organization is processing personal data that is likely to result in a high risk to the data subject's rights, a PIA must be carried out prior to commencing that processing.

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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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

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.

Recipient – a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Representative – a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this regulation.

Right to be Forgotten – also known as **Data Erasure**, entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data if the data is no longer needed for its original purpose. Data subject withdraws consent or data has been processed unlawfully.

Right to Access – also known as **Subject Access Right**, entitles the data subject to have access to and information about whether and where the controller is processing their personal data. Information about the purposes of the processing; the categories of data being processed; whom the data may be being shared with; the period for which the data will be stored; how the data was originally collected; explanation of the logic involved in any automated processing that has a significant effect on data subjects.

Restriction of Processing – the marking of stored personal data with the aim of limiting their processing in the future.

Sensitive Personal Data – personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).

Supervisory Authority – a public authority which is established by a member state in accordance with article 51.

Third Party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.