The following is a non-exhaustive list of terms related to the GDPR and what their meaning is.

Accountability

principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities.

Ad hoc clauses

means a set of clauses for Cross-Border Data Transfers, which require prior approval by a DPA.

Adequacy Decision

means a decision by the Commission to designate a third country as an Adequate Jurisdiction..

Adequate Jurisdiction

means one of the following jurisdictions that have been designated by the Commission as providing an adequate level of protection for personal data: Andorra, Argentina, Canada (for organisations that are subject to Canada's PIPEDA law), Switzerland, the Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay, and the US (for organisations that are certified to the EU-US Privacy Shield).

Anonymisation

means of processing data with the aim of irreversibly preventing the identification of the individual to whom it relates. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available.

Binding Corporate Rules (BCRs)

a set of binding rules put in place to allow multinational companies and organisations to transfer personal data that they control from the EU to their affiliates outside the EU (but within the organisation).

Biometric Data

any personal data relating to the physical, physiological, or behavioural characteristics of an individual which allows their unique identification.

CJEU

means the Court of Justice of the European Union.

Code of Conduct

means a code adhered to by an organisation, which may provide evidence of compliance with the requirements of EU data protection law.

Concerned DPA

means a DPA of a Member State, the residents of which are affected by an organisation's data processing activities (e.g., if Dutch residents are affected by the relevant processing, then the Dutch DPA is a Concerned DPA).

Consent

freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data.

Consistency Mechanism

means the mechanism set out in the GDPR which requires DPAs to ensure that they enforce the GDPR in a consistent manner.

Data Breach

means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Data Concerning Health

any personal data related to the physical or mental health of an individual or the provision of health services to them.

Data Controller

the entity that determines the purposes, conditions and means of the processing of personal data.

Data Erasure

also known as the Right to be Forgotten, it 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.

Data minimization

The principle of “data minimization” means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it.

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.

Data Processor

the entity that processes data on behalf of the Data Controller.

Data Protection Authority

national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data Protection Officer
an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

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

Data transfer
data transfer refers to the transmission / communication of data to a recipient in whatever way.

Delegated Acts
non-legislative acts enacted in order to supplement existing legislation and provide criteria or clarity.

Derogation
an exemption from a law.

Directive
a legislative act that sets out a goal that all EU countries must achieve through their own national laws.

ECHR
means the European Convention on Human Rights.

EDPB
means the European Data Protection Board.

EDPS
means the European Data Protection Supervisor, a body responsible for ensuring that the EU institutions comply with EU data protection law.

EEA
means the European Economic Area (which is made up of the 28 Member States, together with Iceland, Liechtenstein and Norway).

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

Enterprise
any entity engaged in economic activity, regardless of legal form, including persons, partnerships, associations, etc.

ePrivacy Directive
means Directive 2002/58/EC (as amended by Directive 2009/136/EC).

EU-US Privacy Shield
means the mechanism providing a lawful basis for transfers of personal data from the EU to US organisations that certify to the EU-US Privacy Shield, pursuant to Commission Decision C(2016) 4176.

European Parliament
means the Parliament of the European Union.

Filing System
any specific set of personal data that is accessible according to specific criteria, or able to be queried.

GDPR
means Regulation (EU) 2016/679 (the General Data Protection Regulation).

Genetic Data
data concerning the characteristics of an individual which are inherited or acquired which give unique information about the health or physiology of the individual.

One-Stop-Shop
principle that an organisation operating in multiple Member States should have a lead "DPA" that provides a single regulatory point of contact, based on the place of its main establishment in the EU.

Personal Data
any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person.

Personal Data Breach
a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data.

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
a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing
any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling
any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Pseudonymisation
the processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stays separate to ensure non-attribution.

Recipient
entity to which the personal data are disclosed.

Regulation
a binding legislative act that must be applied in its entirety across the Union.

Representative
any person in the Union explicitly designated by the controller to be addressed by the supervisory authorities.

Retention periods
data retention refers to all obligations on the part of controllers to retain personal data for certain purposes. To limit how long you keep personal data is part of data minimisation. The rule of thumb is "as long as necessary, as short as possible", although sometimes legal rules may impose fixed periods. Data that are no longer retained cannot fall into the wrong hands, nor be abused, meaning that defining and enforcing limited conservation periods helps to protect the people whose data are processed.

Right of access
the right of access is the right for any data subject to obtain from the controller of a processing operation the confirmation that data related to him/her are being processed, the purpose(s) for which they are processed, as well as the logic involved in any automated decision process concerning him or her. This right also allows the data subject to receive communication in an intelligible form of the data undergoing processing and of information regarding the processing.

Right of information
everyone has the right to know that their personal data are processed and for which purpose. The right to be informed is essential because it determines the exercise of other rights. The right of information refers to the information which shall be provided to a data subject whether or not the data have been obtained from the data subject. The information which must be provided relates to the identity of the controller, the purpose(s) of the processing, the recipients, as well as the existence of the right of access to data and the right to rectify the data.

Right of rectification
the right of rectification is the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data.

Right to object
the right to object has two meanings. First, it is the general right of any data subject to object to the processing of data relating to him or her, except in certain cases such as a specific legal obligation. Where there is a justified objection based on legitimate grounds relating to his or her particular situation, the processing in question may no longer involve those data.

It also refers to the specific right of any data subject to be informed, free of charge, before personal data are first disclosed to third parties or before they are used on their behalf for the purposes of direct marketing, and to object to such use without justification.

Right to be Forgotten
also known as Data Erasure, it 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.

Sensitive Personal Data

means personal data, revealing race or ethnicity, political opinions, religion or beliefs, trade union membership, genetic information, physical or mental health or sex life. Data relating to criminal convictions or related security measures are also treated as sensitive in many Member States.

Subject Access Right

also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

Supervisory Authority

a public authority which is established by a member state in accordance with article 46.

Trilogues

informal negotiations between the European Commission, the European Parliament, and the Council of the European Union usually held following the first readings of proposed legislation in order to more quickly agree to a compromise text to be adopted.

WP29

means the Article 29 Working Party (an EU-level advisory body made up of representatives from national DPAs and the EDPS, created under Art.29 of the Directive). Under the GDPR, the WP29 is effectively replaced by the EDPB.