QX GLOBAL GROUP

QX's Data Protection Officer Amit Simon provides you with an A-Z glossary of GDPR terms

A Quality Glossary to GDPR

It has been a year since GDPR meteored into the business landscape but let's admit it – most of us are still not as well-versed with the legislation – especially when it comes to the legal jargon surrounding the law.

We've put together a glossary covering some of the most-used terms in GDPR cases so that GDPR is no longer Greek to you:

Accountability: There's a great deal of responsibility that Data Controllers have to bear in the GDPR Era but one of them tops it all – ensuring compliance. Controllers must be able to demonstrate the steps they take to abide by GDPR before taking up any business.

Binding Corporate Rules (BCRs): These are many of rules that must be followed when multinational businesses transfer their personal data from the EU to their partners outside of the EU.

Consent: It is any freely given, specific, informed and unambiguous indication of the subject or client's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Cross-border processing:

a. Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of controller or processor in the Union where the controller or processor is established in more than one Member State; or

b. Processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member state.

Data Controller: It is a natural or legal person, public authority, agency or another 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, the controller or the specific criteria for this nomination may be provided for by Union or Member State law.

Data Processor: It means a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.

Data Recipient:	It means a natural or legal person, public authority, agency or another body, to which 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 public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
Data Subject:	The person whose personal data is being processed by a data controller or processor.
Data Protection Officer (DPO):	A representative for a controller/processor who oversees GDPR compliance and makes sure data-privacy rules are implemented and followed.
Data Privacy Impact Assessment (DPIA):	It is a process to help you identify and minimise the data protection risks of a project.
The ICO (Information Commissioner's Office):	It is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. ICO is the GDPR supervisory authority in the UK.
International Organisation:	It means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
Lawful basis of data processing:	It is the need to have a valid lawful reason to process personal data. This could be consent, a legitimate interest or contractual necessity.
Legitimate interest:	It is a valid alternative to consent as lawful basis for processing— but not for special categories of data. It will not be valid if it harms the rights, interests or freedoms of the individual. Records of your legitimate interest should be documented.
Personal data:	It is information that relates to a natural person or data subject, which can identify them directly or indirectly. For example, a name, ID number, IP address or health information.
Personal data breach:	It means 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.

Profiling:	It means a natural or legal person established in the Union who, designated by the controller or processor, represents the controller or the processor with regard to their respective obligations under this Regulation.
Representative:	It is the automated processing of personal data that a company uses to analyse and predict behaviour of data subjects.
Right to access:	It gives a data subject the right to have complete access to the personal data that a data controller has about them.
Right to be forgotten (Data erasure):	It gives a data subject the right to have a data controller delete all their personal data.
Right to be informed:	It is the right a data subject has to know how a data controller will process their personal data. Any information a company gives to the data subject must be concise, clear, understandable and easily accessible. It should also be written in clear, plain language and be free of charge.
Right to object data:	It gives a data subject the right to object to the processing of their information. They can object to: Processing based on authentic interests or the performance of a task in the public interest/ use of official authority. Direct marketing. Processing for purposes of research and statistics.
Right to rectification:	It gives a data subject the right to ask a company to change their personal data if it's inaccurate or incomplete.
Safe Harbour:	A Safe harbour is a list of countries that have an adequate level of security standards in terms of processing and handling personal information and acceptable to the European Union. The term originated during an agreement between EU and US department of commerce to maintain adequate level of data security. At the time that the General Data Protection Regulation became applicable, the third countries which ensure an adequate level of protection were: Andorra, Argentina, Canada (only commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and USA (if the recipient belongs to the Privacy Shield). Data transfer to these countries is expressly permitted.

Supervisory Authority:	An independent public authority responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedom of individuals in relation to processing personal data. Each State of the EU will designate at least one independent supervisory authority. (e.g, Ireland's Office of the Data Protection Commissioner, France's CNIL [The Commission nationale de l'informatique] and UK's Information Commissioner's Office)
Standard Contractual Clauses:	The SCCs or "model clauses" are standardized contract language (approved by the European Commission) and one method of permission for controllers/processors to send personal data to third countries.
Third Party:	It means 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 authorised to process personal data.

Is your outsourcing partner GDPR compliant?

As the 1st GDPR compliant outsourcing company in India, we've taken all the necessary steps to not only keep data secure but to only collect and hold what is required.

Insist on a GDPR compliant partner for your recruitment, finance & accounts or accounting outsourcing requirements.

- Questions about GDPR? **Ask our DPO**
- Visit: www.qxltd.com/general-data-protection-regulation-gdpr
- contact@qxglobalgroup.com