Keywords Functionality QA

thetrust bridge™

GDPR

A GLOSSARY OF TERMS

AGE VERIFICATION

The age requirement at which data subjects can lawfully give consent introduces a need to verify children's ages. Rules for the language used in consent requests which are targeted at children, and the way online services obtain children's consent, is regulated. Under the GDPR changes, the default age at which a person is no longer considered a child is 16. However, member states can adjust that limit between 13 and 16. Data controllers need to know the age of consent in every member state, and cannot seek consent from anyone under that age. Consent must be obtained from a person holding "parental responsibility". Reasonable efforts are required to verify that the person providing that consent is indeed a parental figure. See **Parental Consent**.

ANONYMOUS DATA

Data from which no individuals can be identified and which is therefore outside the scope of GDPR.

BINDING CORPORATE RULES (BCRS)

A set of binding rules designed to allow multinational companies and organisations to transfer personal data from the EU to the organisation's affiliates based outside the EU but within the organisation. BCRs must demonstrate adequate safeguards and be authorised by the appropriate lead authority in the EU to vouch for data protection compliance.

BIOMETRIC DATA

Any data created during a biometric process. This includes physical samples, fingerprints as well as verification and identification data.

BREACH

A breach of security leading to the accidental or unlawful loss, destruction, unauthorised disclosure of, or access to, the personal data.

BREACH NOTIFICATION

Organisations are required to report data breaches to the ICO within 72 hours of the breach and/or the organisation becoming aware of the breach. In the case of Data Subjects being caused potential harm by the breach, they must also be notified.

CONSENT

Freely given, specific, informed and unambiguous consent given by the data subject either by statement or clear affirmative action which signifies agreement to the subject's personal data being processed.

CROSS BORDER PROCESSING

The processing of data by a Controller or Processor who operates in more than one EU member state, or the processing of data in one EU member state of subjects resident in one or more member state.

DATA

Information that is held manually or processed by computer.

DATA CONTROLLER	Any person or organisation [the legal entity or individual] that determines the purposes, conditions and methodology for the processing of personal data.
DATA ERASURE	Also known as the **Right to be Forgotten**. The right to have the Data Controller erase the personal data, stop publishing the data and cease processing the data.
DATA PORTABILITY	The right to allow individuals to obtain and reuse their personal data for their own purposes across different services so they can move, copy or transfer the data easily in a safe and secure way.
DATA PRIVACY IMPACT ASSESSMENT (DPIA)	A methodology or tool used to identify and reduce the privacy risks of individuals when planning projects or policies to protect the data.
DATA PROCESSOR	Any person or organisation [the entity or individual] that processes data on behalf of the Data Controller. Processing is defined very widely and includes collection, storage, use, recording, disclosure or manipulation of data whether or not by automated means.
DATA PROTECTION ACT (DPA)	The Data Protection Act 2018 was introduced in the UK to give effect to GDPR.
DATA PROTECTION AUTHORITY	The national authority in every EU member state that enforces data protection in that member state.
DATA PROTECTION OFFICER (DPO)	The role in an organisation which has responsibility for ensuring that individual's personal data is protected under data protection legislation and that the organisation is compliant with the legislation.
DATA PROTECTION PRINCIPLES	Personal data must be processed fairly and lawfully, only be collected for specified and lawful purposes. It must be adequate, relevant and not excessive in relation to the purpose(s) for which it is collected. It must be accurate and, where necessary, kept up to date and should be retained no longer than is necessary. It should be processed in accordance with the rights of data subjects, and using appropriate technical and organisational measures against unauthorised or unlawful processing of personal data.
DATA SOVEREIGNTY	The concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located.
DATA SUBJECT	A living person who is the subject of personal data.
ENCRYPTED DATA	Data that is secure as protected by translating the data into another form that can only be read by those with authorised access through a key or password.
GDPR	GDPR is the General Data Protection Regulation, which came into force on 25th May 2018. The GDPR further harmonises data protection rules across EU member states. It applies to data processing carried out by individuals and organisations operating within the EU, but also applies to organisations outside the EU that offer goods and services to EU citizens. The GDPR significantly enhances the rights of data subjects in the processing of their personal data.

GENETIC DATA	Data that is unique concerning the characteristics of an individual which are inherited or acquired. See **Biometric Data**.
GROUNDS FOR PROCESSING	An organisation's lawful basis for processing personal data – consent; contractual; legal basis; vital interests; public interest; legitimate interests.
INFORMATION COMMISSIONERS OFFICE (ICO)	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.
MEMBER STATE	Member State means a Member State of the European Union (i.e., 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). Following the UK's submission of a notice of withdrawal under Article 50 of the Treaty of Lisbon the United Kingdom will remain an EU Member State until midnight (Brussels time) on October 31 2019, unless there is an extension period. The United Kingdom will become a third country from the date of withdrawal.
PARENTAL CONSENT	Consent from a person holding parental authority over children under 16 (age varies across member states). It is the responsibility of the Data Controller to set up the verification procedures that guarantee the age of the child and the authenticity of the Parental Consent. See **Age Verification**.
PERSONAL DATA	Any information relating to the private, professional or public life of a living person or Data Subject, that can be used to directly, or when combined with other information, indirectly identify the person. It includes any expression of opinion about an individual.
PERSONAL DATA BREACH	A breach of security leading to the accidental or unlawful destruction, loss, disclosure or access to, personal data. See **Breach**.
PRIVACY BY DESIGN	The principle of the inclusion of data protection from the onset of the designing and planning of systems, rather than as a later addition (also Privacy by Default).
PRIVACY NOTICE	A notice informing Data Subjects how their personal information is going to be used and their rights when their data is provided, collected and processed.
PRIVACY SHIELD	The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks impose stronger obligations on US organisations to protect personal data of Data Subjects in the EU. The Privacy Shield requires the US to monitor and enforce protection, and to cooperate with Supervisory Authorities. The Privacy Shield program is administered by the US Department of Commerce and enables US-based companies to join one or both of the Privacy Shield Frameworks in order to benefit from the certification. Joining Privacy Shield is voluntary, but having made the public commitment to comply with the requirements, the commitment will become enforceable under U.S. law.

PSEUDONYMISATION	A process undertaken to ensure that no personal data can be attributed to an individual data subject without the use of additional information. A procedure by which the most identifying fields within a data record/ database are replaced by one or more artificial identifiers, or pseudonyms. GDPR explicitly encourages organisations to consider pseudonymisation as a security measure provided the "key" that enables re-identification is kept separate and secure.
RECIPIENT	Person to whom the personal data are disclosed in the course of processing.
RECTIFICATION	The right for Data Subjects to have inaccurate personal information corrected.
REGULATION	A binding legislative act that must be applied in its entirety across the European Union.
RIGHT TO BE FORGOTTEN	See **Data Erasure**.
RIGHT TO ACCESS	See **Subject Access Right**.
SENSITIVE PERSONAL DATA	Personal Data that is of a private nature and includes racial origin, sexual life, political or religious views and affiliations, and physical or mental health.
SUBJECT ACCESS REQUEST	A written or electronic request by an individual to an organisation asking for access to information about the individual held by the organisation.
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 holds. Application is by a Subject Access Request that is free of charge.
SUPERVISORY AUTHORITY	The lead authority in the EU member state that manages data protection compliance.
THIRD PARTY	Any person other than the Data Subject, Data Controller or Data Processor.
USER-MANAGED ACCESS (UMA)	A standard protocol adopted in 2015 and designed to give an individual data subject, a unified control point for authorising access to their personal data, content, and services, no matter where that data is stored.