GDPR Jargon Buster

If you need help navigating technical data protection terms, look no further. We have created a list of commonly used terms and acronyms with simple explanations

BCRs A set of binding corporate rules approved by the regulators that allow multinational companies and organisations to transfer personal data they control from the UK/EU to their affiliates outside the UK/EU (but within the same group).

Biometric data Personal data resulting from specific technical processing which relates to the physical, physiological, or behavioural characteristics of an individual. For example, this can include facial images or fingerprints.

Controller The organisation that decides why and how to use personal data.

Data subject A person whose personal data is processed.

DPA Data processing agreement. An agreement entered into between a controller and a processor setting out obligations the processor must comply with when processing the controller's personal data.

DPA 2018 / DPA Data Protection Act 2018. also sometimes referred to as DPA. This is the UK legislation which sets out UK specific rules relating to the implementation of GDPR in the UK.

DPIA or PIA Data protection impact assessment or Privacy impact assessment , a process which helps organisations to identify, mitigate and document privacy risks associated with proposed data processing activities. For high risk processing activities, DPIAs must be completed under GDPR.

DUA Data (Use and Access) bill. The legislation which is currently going through Parliament, which will amend UK data protection law when it comes into force.

EDPB European Data Protection Board. EU data protection regulator which has certain tasks under GDPR, including issuing guidance and acting as a point of escalation for cross-border matters.

GDPR General Data Protection Regulation EU 2016/679. This is the European Union's data protection law that governs the way in which organisations are permitted to use personal data.

Gen AI Generative Artificial Intelligence. This is artificial intelligence which learns patterns and the structure of the data it is trained on which allows it to produce new data.

ICO Information Commissioner's Office. The UK's data protection regulator.

IDTA International Data Transfer Agreement. This is the template agreement produced by the ICO which can be used for transferring personal data from the UK to other countries in compliance with the requirements of the UK GDPR.

International Data Transfer Addendum (to the SCCs) An addendum which can be used to allow an organisation that has SCCs in place to send personal data from the UK to other countries in compliance with the requirements of the UK GDPR.

LIA Legitimate Interest Assessment. The test you need to carry out when using legitimate interests as a legal basis for processing to ensure that you consider the balance between the interest you have identified and the rights and freedoms of the people who will be affected by the processing.

LLM Large Language Model. Designed to be used for natural language processing (see NLP) tasks. The models are trained on huge amounts of data and can be used for a wide variety of purposes from planning a holiday to answering complex scientific questions. One famous example is ChatGPT.

NLP Natural Language Processing. The use of machine learning to allow computers to recognise, understand and use human language. e.g. when you use an app which recognises speech and turns it into text.

GDPR Jargon Buster

PECR
Privacy and Electronic Communications Regulations 2003. These regulations apply to electronic marketing messages and cookies/tracking technologies amongst other things.

PET
Privacy Enhancing Technology. These are a variety of technologies which can help organisations to implement the data protection principles effectively and incorporate safeguards into processing.

Personal Data
Any information relating to an identifiable individual.

Personal Data Breach
A breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

PII
Personally identifiable information. Similar to personal data and is most commonly used in the US.

Principles
Fundamental principles embedded within the GDPR that set out the main responsibilities for organisations.

Processor
The organisation that processes personal data on behalf of a controller. For example, IT suppliers will often be processors.

ROPA
Record of processing activities. A record of all the personal data that is processed by an organisation. GDPR specifies the records that you need to maintain in your ROPA, which include the purposes for which personal data is being used, recipients of personal data and for how long it is retained.

RTBF
Right to be forgotten. This is one of the rights which individuals have under GDPR where they can request that their personal data is deleted. Also known as the right of erasure.

SAR / DSAR
Subject access request / data subject access request. This is one of the rights which individuals have under GDPR. Individuals can request to obtain a copy of all of their personal data held by an organisation.

SCCs
Standard contractual clauses. These are template contract clauses approved by the European Commission which can be used to ensure there are adequate safeguards in place for personal data that is transferred outside the EU.

Special categories of data
This is a subset of personal data including information about racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data used to uniquely identify an individual, health data, or data concerning an individual's sex life or sexual orientation.

Supervisory Authority
Sometimes referred to as a DPA or Data Protection Authority. An independent public authority established by an EU Member State to oversee GDPR compliance.

TIA or TRA
Transfer impact assessment or transfer risk assessment - risk assessments that must be completed when transferring personal data from the UK or the EU to a third country that does not have the benefit of being recognised as having adequate data protection laws.

TOMs
Technical and Organisational Measures - measures taken by an organisation to ensure the security of personal data, such as cyber security measures, but also risk assessments and access controls amongst many others.

UK BCR addendum
This is an addendum to the EU BCRs which organisations that have approved EU BCRs can use to gain approval for UK BCRs (as an alternative method to apply for UK BCRs).

UK GDPR
This is the UK law equivalent of the EU GDPR. It is very similar to the EU GDPR but some changes were needed mostly to reflect the fact the UK is no longer part of the EU after Brexit.