

## GDPR Jargon Buster

If you need help navigating your way through technical data protection terms, look no further. We have created a list of commonly used terms and acronyms with a simple explanation about what each one means. Happy reading!

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. This is an agreement entered into between a controller and a processor which sets out the obligations with which the processor must comply when processing the controller's personal data.
DPA 2018 (sometimes also confusingly just called the DPA)	UK Data Protection Act 2018. This is the UK legislation which sets out UK specific rules relating to the implementation of GDPR in the UK.
DPIA (sometimes referred to as a PIA or Privacy Impact Assessment)	Data protection impact assessment, which is 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.
DPO	Data Protection Officer. Under GDPR certain organisations must appoint a DPO who must fulfil the statutory tasks set out in GDPR.
EDPB	European Data Protection Board. This is the group of all EU data protection regulators 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.

ICO	Information Commissioner's Office. This is the UK's data protection regulator.
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 or, or access to, personal data.
PII	Personally identifiable information. This is broadly 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. This is 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 (sometimes referred to as a DSAR or data subject access request)	Subject access request. This is one of the rights which individuals have under GDPR. Under the subject access right, 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. These include 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. These are 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.
EU	European Union.

If you need support with data protection compliance matters please [contact us](#) . You might also be interested in our training courses – find out more [here](#).

