ABI UK GDPR Good Practice Workshop

Glossary

“Accountability”: The responsibility of organisations to comply with data protection laws and demonstrate that they are protecting personal data.

“Consent”: A clear agreement from an individual to allow their personal data to be processed for a specific purpose.

“Controller”: An individual or organisation that determines the purposes and means of processing personal data.

“Data Protection Impact Assessment (DPIA)”: A process to identify and minimise the data protection risks of a project.

“Data Subject”: An individual whose personal data is being processed.

“Data Minimisation”: The principle that personal data collected should be adequate, relevant, and limited to what is necessary for the purpose.

“Legitimate Interest”: A lawful basis for processing personal data where the processing is necessary for the interests of the data controller or a third party, balancing those interests against the rights of the data subject.

“Processor”: An individual or organisation that processes personal data on behalf of a controller.

“Privacy Information”: Information provided to data subjects about how their personal data will be used, including their rights and the purpose of processing.

“Special Category Data”: A type of personal data that is considered sensitive (e.g., health data, racial or ethnic origin) and requires more stringent protection under data protection laws.

“Sub-processor”: A third party engaged by a processor to assist in processing personal data.

“UK GDPR”: The United Kingdom General Data Protection Regulation, which governs the handling of personal data in the UK.

“Legitimate Interest Assessment (LIA)”: A process to evaluate whether the processing of personal data for legitimate interests is justifiable.

“Function Creep”: The expansion of the use of personal data beyond its original purpose without the data subject's consent.

“Invisible Processing”: Processing personal data without the knowledge of the data subject, which can pose high risks to individual rights.

“ICO”: The Information Commission(er)'s Office, the UK authority set up to uphold information rights.

“Data Breach”: A security incident that results in the unauthorised access, loss, or destruction of personal data.

“Retention Policy”: A policy that outlines how long personal data will be kept and the conditions for its removal or destruction.

“Processing”: Any operation performed on personal data, including collection, storage, use, sharing, and deletion.

“Transparency”: The principle that data subjects should be able to understand how their personal data is being used and processed.

“Training Record”: Documentation of training provided to staff regarding data protection and compliance with regulations.

“Risk Assessment”: The process of identifying potential risks to personal data and evaluating the measures to mitigate those risks.

“Data Sharing Agreement”: A formal agreement between parties that outlines how personal data will be shared and the responsibilities of each party.