## Appendix – Glossary of Commonly Used Data Protection Terms

| | |
|---|---|
| **Article 29 Working Party** | a European advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisory and the European Commission. It provides guidelines on the GDPR and data protection matters. |
| **Anonymisation** | where Personal Data is processed in such a way that the data can no longer be attributed to a specific Data Subject. When done properly, anonymisation places data outside the scope of the GDPR. |
| **Automated Decision Making** | these are decisions which are made following Processing of Personal Data solely by automatic means, (i.e. where no humans are involved in the decision-making process). An example would an individual applying for a personal loan online, then being given a yes/no decision based solely on an automated credit search algorithm. |
| **Consent** | defined in the GDPR as "any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her". Silent, implicit indications of consent, such as leaving pre-ticked web form boxes ticked, will not be sufficient for Consent under the GDPR. Note that "informed" Consent requires that the Data Subject has received all the information about the Processing, in a format intelligible to them so they can make an informed decision about their rights (this is a particular challenge for children's consent). Some Processing requires the Data Subject's "explicit Consent". |
| **Data Subject** | means a living person who is the subject of Personal Data. In your business, Data Subjects will likely include your employees, authors, suppliers, website users etc. |
| **Data Subject Rights** | the rights that Data Subjects have under the GDPR including the rights in certain circumstances to access information Data Controllers have about them, stop or restrict Processing about them, to withdraw Consent and complain to a Supervisory Authority. |

| | |
|---|---|
| **Data Controller** | the living person or legal entity which, alone or jointly with others, determines the purposes for which and means of Processing of Personal Data. For example, your business is a Data Controller in respect of the Personal Data it Processes about its employees, customers, authors, suppliers etc (note that the individual employees of the business are not separate Data Controllers). |
| **Data Processor** | the living person or legal entity which processes Personal Data on behalf of a data controller. You might use Data Processors in your business to host your website, send email marketing on your behalf etc. |
| **Data Protection Bill** | the version of the UK's Data Protection Bill first read before Parliament on 13 September 2017, which is set to replace the Data Protection Act 1998, and which is set to implement parts of the GDPR specific to the UK; |
| **DPA (Data Protection Act)** | the Data Protection Act 1998, the UK's existing data protection law; |
| **DPIA (Data Protection Impact Assessment)** | known under the existing data protection laws as a "privacy impact assessment" this tool can help you determine if your Processing will affect the rights of any Data Subjects (and how to mitigate that risk). It is a required process in some instances under the GDPR. |
| **DPO (Data Protection Officer)** | under the GDPR companies must appoint a DPO in certain circumstances (such as when they are Processing on a large scale or undertaking regular or systematic monitoring). |
| **EEA** | European Economic Area. This is the region to which the GDPR primarily applies. Sending or making Personal Data accessible outside of the EEA requires special considerations (see Transfer below). |
| **EU-US Privacy Shield** | the framework for transatlantic exchanges of Personal Data for commercial purposes between the European Union and the United States under which US companies can certify compliance. |
| **GDPR** | the General Data Protection Regulation (EU) 2016/679. There is an online, searchable version of the GDPR text here: https://gdpr-info.eu/. |
| **ICO** | the UK's data protection regulator, the Information Commissioner's Office. The ICO has GDPR guidance and resources here; https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/. |

| | |
|---|---|
| **Lawful Grounds** | Processing may take place only when there is a lawful reason to do so. Commonly referred to as the "six lawful grounds" these are specified in the GDPR as: (i) when the Data Subject has given their Consent for one or more specified purposes; or when the Processing is necessary (ii) for performance of or entering into a contract with or at the request of the Data Subject; (iii) for the Data Controller to comply with a legal obligation; (iv) to protect the vital interests (generally a life-or-death situation) of the Data Subject or another person; (v) for performance of a task in the public interest; (vi) for the purposes of Legitimate Interests (see below). It is important to remember that each Lawful Ground is equally valid. Data Controllers must identify the appropriate Lawful Ground for their Processing and specify these in the Privacy Notice. |
| **Legitimate Interests** | one of the Lawful Grounds for data Processing under the GDPR. Legitimate Interests refers to your interests in conducting and managing your business and your relationship with Data Subjects but it can only apply if you have made an assessment and determined that the rights and freedoms of Data Subjects are not overridden. It can be a tricky concept to apply but it is helpful to consider the nature of your relationship with the Data Subject and whether the kind of Processing you envisage would be within their reasonable expectations. |
| **Model Contract Clauses** | the standard contractual clauses approved by the European Commission as guaranteeing appropriate safeguards under European data protection laws for Personal Data transferred to entities based outside of the EEA. |
| **Personal Data** | any information relating to an identified or identifiable natural person who can be identified, directly, or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; there is no exhaustive list of what constitutes Personal Data so it is important to remember that this broad definition may include digital identifiers (such as social media handles) as well as correspondence about (including opinions of) individuals. |
| **Personal Data Breach** | a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. |

| | |
|---|---|
| **Phishing** | the attempt to obtain confidential or sensitive information such as usernames and passwords, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. Phishing is an increasingly common cause of Personal Data Breaches. |
| **Portability** | the right for an individual to require a Data Controller to give them back a copy of the Personal Data they previously provided or send this data to another organisation so that they can reuse it. The Personal Data has to be provided in a commonly used, machine-readable format and only when the Personal Data has been provided by the Data Subject with their Consent or as part of a contract. This is commonly used in the banking and utilities sectors when individuals switch providers. |
| **Privacy Notice** | a common way for Data Controllers to inform Data Subjects about how, when, where and why their Personal Data is being Processed. This is commonly hosted on businesses' websites. |
| **Profiling** | any form of automated processing of Personal Data intended to evaluate certain personal aspects of an individual. These aspects can include analysing/predicting someone's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement. You may be using Profiling in your business to serve marketing and advertising messages. If so, ensure that you describe this Profiling in your Privacy Notice. |
| **Process(ing)** | obtaining, recording or holding Personal Data or carrying out any operation or set of operations in relation to it and includes the organisation, retrieval, use of the Personal Data, disclosure, erasure or destruction of the Personal Data. This is a very broad definition and it is important to remember that simply storing Personal Data in any accessible/ordered/structured way will be a form of Processing. |
| **Pseudonymisation** | similar to anonymisation, but reversible. This is where Personal Data is processed in such a way that the data can no longer be attributed to a specific Data Subject without the use of 'additional information'. The additional information must be kept separately and be subject to certain measures which ensure that it isn't unduly used to reverse the process. Pseudonymisation is a way to minimise the risk of a Personal Data Breach. |

| | |
|---|---|
| **Special Categories of Data / Sensitive Personal Data** | Personal Data revealing racial or ethnic origin, political opinions, revealing religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purposes of uniquely identifying a natural person, or concerning health, concerning sexual orientation. Special standards apply to the Processing of Special Categories of Data including: you may only Process this when you have the Data Subject's explicit Consent or it is necessary for employment obligations or where the vital interests of the Data Subject or others are at risk (and the Data Subject cannot give Consent). |
| **Supervisory Authority** | a supervisory authority of a European Member State responsible for monitoring the application of data protection laws, which for the UK is the ICO. |
| **Transfer** | a transfer of Personal Data will occur when Personal Data is sent, shared, stored, accessed or otherwise used by a third party (whether an individual or a company) in another country or jurisdiction. There are no restrictions of transfers of personal data within the EEA; however safeguards (or "transfer solutions") must be put in place where Personal Data is transferred outside of the EEA to ensure a level of protection for that Personal Data equivalent to the GDPR. Safeguards that may be applicable include the EU-US Privacy Shield and the Model Contract Clauses. |