ORGANISATIONS

JARGON BUSTER / GLOSSARY

digital TOOLKIT

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Data Protection Jargon Buster

Anonymisation: The process of irreversibly turning personal data into a form such that the data subject is no longer identifiable. The Data Protection (Jersey) Law 2018 does not apply to data that has been fully anonymised because it has ceased to be personal data.

Authority: The Jersey Data Protection Authority.

Consent: Any freely given (an individual cannot be forced), specific, informed and unambiguous indication of the data subject's wishes by which he or she signifies agreement to the processing of his or her personal data.

Data Controller: A natural or legal person, public authority, agency or other body that (alone or jointly with others) determines the purposes and means of the processing of personal data.

Data erasure: The right (in certain circumstances) of the data subject to request to have the data controller erase his or her personal data, cease further dissemination of the data, and potentially have third parties cease processing the data. Also known as the 'right to be forgotten'.

Data inventory: A record of processing activities under the responsibility of a data controller.

Data minimisation: The principle that personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Data processor: A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller, but does not include an employee of the controller.

Data portability: The right of the data subject to receive the personal data concerning him or her, which he or she has previously provided to the data controller, in a commonly used and machine-readable format and to transmit that data to another data controller.

Data Protection Authority (Jersey) Law 2018: This Law sets out the Authority's powers in terms of enforcement, investigation, fining etc.

Data Protection (Jersey) Law 2018: This is the main local law which sets out how controllers and processors can deal with personal information. The Data Protection Law 2018 is Jersey's implementation of the European General Data Protection Regulation (GDPR).

Data protection by default: The obligation on controllers and processors to have appropriate technical and organisational measures for ensuring that, by default, only personal data that is necessary for each specific purpose of the processing is processed.

Data protection by design: The obligation on controllers and processors to have appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner.
See also 'privacy by design'.

Data protection impact assessment (DPIA): A term referring to an assessment of the impact of proposed processing operations on the protection of personal data. This should be carried out before any processing starts and where processing is likely to result in a high risk to the rights and freedoms of individuals.

Data Protection Officer (DPO): An individual with expert knowledge of data protection law and practices who must be appointed where the processing in question involves regular and systematic monitoring of data subjects on a large scale, or where the processing is of special categories of data on a large scale. Organisations can also voluntarily appoint a DPO even if they don't legally need one.

Data protection principles: The fundamental principles of data protection which stipulate how controllers and processors must deal with personal data. Personal data should be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and where necessary kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed; and
- Processed in a manner that ensures appropriate security of the personal data.

Data subject: An individual who can be identified, directly or indirectly, from personal data held, for example by reference to a name, social security number or address.

Encrypted data: Personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access.

Jersey Office of the Information Commissioner: The Information Commissioner is the Chief Executive Officer of the Jersey Data Protection Authority, carrying out the day-to-day work.

Joint data controllers: Where two or more controllers jointly determine the purposes and means of processing.

Lawful processing: You must have a legal basis for processing/using personal data. Different legal bases are available depending whether you are processing 'standard' personal data or special category data. You need to know which legal basis you're using before you start processing any data.

For non-special category data, the lawful bases are set out at Schedule 2 (Part 1) of the DPJL, as follows:

(a) consent;

(b) performance of a contract;

(c) protection of the vital interests of an individual;

(d) performance of a task in the public interest; or

(e) legitimate interests of the controller or third party.

(The lawful conditions for processing Special Category data are set out at Schedule 2 (Part 2) of the DPJL.)

Legitimate interest: One of the lawful bases for processing (not applicable to public authorities). This can only be relied on if it doesn't prejudice the rights and freedoms or legitimate interests of a data subject (particularly if the data subject is a child).

Personal data: Any information relating to a living person by which he or she can be identified, directly or indirectly.

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

Privacy by design: A principle that calls for the inclusion of data protection from the designing phase when planning new systems and processes, rather than as an addition.
See 'Data protection by design'.

Privacy policy/ Privacy notice: Controllers must provide data subjects with information about how they are processing that individual's data. This is to ensure fair and transparent processing of his or her personal data. This information is commonly given by way of a privacy policy or notice.

Processing: Any operation or set of operations that is performed on personal data or sets of personal data, whether or not by automated means, including collection, storage, retrieval, use or erasure.

Processor: A natural or legal person, public authority, agency or other body that processes personal data on behalf of the data controller (not an employee of the controller). Processors can only process data in accordance with written instructions given by the controller.

Pseudonymisation: Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information i.e. removing the identifying characteristics of an individual and replacing it with a pseudonym. The additional data must remain separate to ensure that the data subject cannot be identified. This is different from anonymisation because it still allows individuals to be identified using indirect means. It is still personal data.

Right to be forgotten: See 'Data erasure'.

Rights of data subjects: Data subjects have the following rights:
(a) right to be informed;
(b) right of access;
(c) right to rectification;
(d) right to erasure ('right to be forgotten');
(e) right to restriction of processing;
(f) right to data portability;
(g) right to object to processing for public functions, legitimate interests, direct marketing and/or historical or scientific purposes; and
(h) right not to be subject to decisions based solely on automated processing.

Sensitive data: See 'Special categories of personal data'.

Special categories of personal data:	Personal data that is more deemed to be more sensitive such as that revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (Previously known as 'sensitive personal data'.)
Subject Access Request:	A request by a data subject for information about whether or not personal data concerning him or her is being processed, and, where that is the case, the provision of access to the personal data and information, including being told about the purposes of the processing.