Data protection definitions

GDPR

The General Data Protection Regulation (2016/679) is the new EU Regulation on Data Protection, which came into effect on the 25th May 2018.

Personal Data

Information relating to a living individual who is, or can be, identified by that information, including data that can be combined with other information to identify an individual. This can be a very wide definition, depending on the circumstances, and can include data which relates to the identity, characteristics or behaviour of an individual or influences the way in which that individual is treated or evaluated.

Processing

Processing means performing any operation or set of operations on personal data, including:

- obtaining, recording or keeping data;
- organising or altering the data;
- retrieving, consulting or using the data;
- disclosing the data to a third party (including publication); and
- erasing or destroying the data.

Data Controller

A Data Controller is the person (in the case of a sole trader) or organisation who decides the purposes for which, and the means by which, personal data is processed. The purpose of processing data involves ‘why’ the personal data is being processed and the ‘means’ of the processing involves ‘how’ the data is processed.

Read the Office of the Information Commissioners guidance on the Duties of Data Controllers.

Data Processor

A person or organisation that processes personal data on the behalf of a data controller, for example, outsourced activities such as IT provision, cloud providers, human resources. They are not employees of the data controller. They can only act on the written instructions of the controller.

Data Subject

A Data Subject is the individual the personal data relates to.

Data Protection Impact Assessment (DPIA)

A DPIA describes a process designed to identify risks arising out of the processing of personal data and minimisation of these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance, including ongoing compliance, with the DPJL and GDPR. DPIAs should be carried out before any processing of data takes place.

DPJL

The Data Protection (Jersey) Law 2018, which came into force on 25th May 2018. It replaces the Data Protection (Jersey) Law 2005.

Lawful basis for processing personal data

In order to process personal data you must have a lawful (legal) basis to do so. The lawful grounds for processing personal data are set out in Schedule 2 (Part 1) of the DPJL. These are:

- where you have the consent of the individual;
- where it is necessary for performance of a contract;
- for compliance with a legal obligation;
- where it is necessary to protect the vital interests of a person;
- where it is necessary for the performance of a task carried out in the public interest; or in the legitimate interests of company/organisation (except where those interests are overridden by the interests or rights and freedoms of the data subject).

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

Additionally, Schedule 2 (Part 2) of the DPJL sets out the lawful bases for processing of special category (sensitive) personal data. If you want to process special category data, you need to identify the lawful basis in both parts of Schedule 2.

You need to work out the legal basis before you start processing and document your thinking.

Retention Policy

How long will your organisation hold an individual's personal data? This will be influenced by a number of factors. There may be legal requirements on your organisation, depending on your business type (e.g. General Medical Council or JFSC rules). Keep the data for the least amount of time that you can in accordance with the requirements of your business, store it securely while it is in your possession and make sure to delete it fully and safely at the appointed time.

Special Category Data

This is defined in Article 1 of the DPJL as data 'which reveals 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, or data relating to a person's criminal record or alleged criminal activity'. If you want to process Special Category Data you need to be able to also identify one of the lawful bases in Schedule 2 Part 2 of the DPJL.

Consent

Article 11 of the DPJL has increased the conditions needed for consent as a legal basis for data processing to be valid. It is now necessary to consider whether consent was unambiguous, informed and freely given and the data subject must have the opportunity to withdraw consent for

processing at any time.

Consent should not be assumed (no more pre-ticked boxes) and must be obtained before data processing begins (e.g. through Privacy Notices). There must be a positive, affirmative action by the data subject for consent to be valid. It also requires individual ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

If you offer online information services to children (i.e. purchasing of apps), it is necessary to ensure that you can verify their age and the consent of someone having "parental responsibility" must be obtained if the child is under the age of 13.

Relevant Links

- The Data Protection (Jersey) Law 2018
- Jersey Office of the Information Commissioner
- Data Protection for SMEs
- Data Protection Registration
- GDPR - What will it mean for your business?

Keep up-to-date with business information, news and events
sign up for the Jersey Business newsletter.

Subscribe →