VOISIN LAW

Guide to data protection in Jersey & the general data protection regulation | 1

The purpose of this guide is to set out a summary of data protection under Jersey law.

Jersey has had data protection legislation since 1987, however in order to comply with current European requirements for the transfer of personal data it became necessary to update Jersey legislation to reflect the current UK position, hence the enactment of the Data Protection (Jersey) Law 2005.

The current legislative framework is set to change next year when the General Data Protection Regulation ("**GDPR**") will replace the Data Protection (Jersey) Law 2005 on 25 May 2018. Below are the key features of the GDPR.

GDPR – the 7 principles

1. Lawfulness, fairness and transparency – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
2. Purpose limitation – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. Data minimization – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accuracy- Personal data shall be accurate and, where necessary, kept up to date
5. Storage Limitation – Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
6. Integrity & Confidentiality – Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
7. Accountability – The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

Consent under the GDPR

- The conditions for consent have been strengthened. The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. It must be as easy to withdraw consent as it is to give it.

Maximum penalties for breaches of the GDPR

- Up to €20 million or 4% of annual global turnover (prior year), whichever is greater, for more serious breaches
- Up to €10 million or 2% of annual global turnover (prior year), whichever is greater, for less serious breaches

Key obligations under the GDPR

- Obligation to maintain records of all processing activities, including the purposes of the processing
  - a description of the categories of data
  - a description of the categories of recipients, including recipients in third countries
  - the time limits for erasure (where possible)
  - a description of the technical and organisational security measures
- Obligation to appoint Data Protection Officer if core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.
- Data Protection Impact Assessment – required in cases where processing likely to result in a high risk to rights and freedoms of individuals.