DATA PROTECTION LAWS OF THE WORLD

Jersey

DLA PIPER

JERSEY

Last modified 27 January 2016

LAW IN JERSEY

The Data Protection (Jersey) Law 2005 ('Law) came into force on 1 December 2005.

Jersey's data protection legislation has been held to be adequate by the European Commission for the purposes of the European Data Protection Directive (Directive 95/46/EC) (see Commission Decision 2008/393/EC).

DEFINITIONS

Definition of personal data

'Personal data' is defined under the Law as data relating to a living individual who can be identified:

- from the data, or
- from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Definition of sensitive personal data

'Sensitive Personal Data' is defined under the Law as personal data relating to:

- the racial or ethnic origin of the data subject
- the political opinions of the data subject
- the data subject's religious beliefs or other beliefs of a similar nature
- whether the data subject is a member of a trade union
- the data subject's physical or mental health or condition
- the data subject's sexual life
- the data subject's commission, or alleged commission, of any offence, and
- any proceedings for any offence committed, or alleged to have been committed, by the data subject, the disposal of any such proceedings or any sentence of a court in any such proceedings.

NATIONAL DATA PROTECTION AUTHORITY

Office of the Information Commissioner
Brunel House
Old Street
St.Helier
Jersey
JE2 3RG

T: +44 (0)1534 716530
E: enquiries@dataci.org

REGISTRATION

Data controllers who process personal data must inform the Information Commissioner (an online portal is available) of the following:

- the name and address of the data controller (including a Jersey resident representative if the data controller is outside Jersey)
- a description of the personal data being, or to be, processed by or on behalf of the data controller and of the category or categories of data subject to which they relate
- a description of the purpose or purposes for which the data are being or are to be processed
- a description of the recipients (if any) to whom the data controller intends or may wish to disclose the data, and
- the names, or a description, of any countries or territories outside Jersey to which (directly or indirectly) the data controller transfers, or intends or may wish to transfer, the data.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer in Jersey.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

- the data subject consents
- the data controller needs to process the data to enter into or carry out a contract to which the data subject is a party
- the processing satisfies the data controller's legal obligation
- the processing protects the data controller's vital interests
- the processing is required by an enactment, the Crown or the government
- the processing is required to perform a public function in the public interest, or to administer justice, or
- the data controller has a legitimate reason for the processing, except if the processing would damage the data subject's rights, freedoms or other legitimate interests.

Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of additional conditions.

The data controller must provide the data subject with "fair processing information". This includes the identity of the data

controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.

TRANSFER

The Law provides that data controllers may transfer personal data out of the European Economic Area if any of the following conditions are met:

- the data subject consents
- the transfer is essential to a contract to which the data subject is party
- the transfer is needed to carry out a contract between the data controller and a third party if the contract serves the data subject's interests
- the transfer is legally required or essential to an important public interest
- the transfer protects the data subject's vital interests, or
- the data is public.

Transfers of personal data to jurisdictions outside of the European Economic Area are allowed if the jurisdiction provides 'adequate protection' for the security of the data, or if the transfer is covered by 'standard contractual clauses' approved by the European Commission. It is likely that Binding Corporate Rules would satisfy the Law.

Following the decision of the Court of Justice of the European Union in Schrems v Data Protection Commissioner (C36214), the US/EU "Safe Harbour" regime is no longer regarded as a valid basis for transferring personal data to the US. Whilst Jersey is not a member of the EU, it can (and does) adopt measures prescribed by the EU in certain areas such as data protection. Jersey uses the EU "adequacy" benchmark to assess whether transfers can be validly made to other jurisdictions.

The Safe Harbour regime had been relied upon as a mechanism for the transfer of data to the US, which did not otherwise have "adequate" measures in place to protect personal data. Now that the regime has been abolished, Jersey businesses are reviewing their procedures. Whilst the Commissioner has not adopted any formal stance in response to the Schrems decision, she is maintaining a close dialogue with the Channel Islands' Brussels office and the UK's Information Commissioner's Office. Whilst awaiting the revised version of the Safe Harbour Privacy Principles, the Commissioner has confirmed that Jersey's existing statutory regime will be adhered to, confirming that she retains the power to investigate complaints made to her, including those founded on transfers reliant upon Safe Harbour as a basis for their validity.

It is anticipated that the Commissioner will likely await the outcome of the US/EU negotiations; however with the prospect of data protection authorities around Europe adopting varying stances, the immediate future remains uncertain. It remains important for businesses to review their procedures and adopt alternative mechanisms if they had previously relied on Safe Harbour.

SECURITY

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data.

BREACH NOTIFICATION

There are no specific duties to inform the Data Protection Commissioner of breaches. However, best practice is likely to be (following the UK) to inform the Data Protection Commissioner of a breach where a significant number of data subjects are affected or where significant harm may (or has already) occurred.

ENFORCEMENT

In Jersey, the Information Commissioner is responsible for the enforcement of the Law. This is a dual role which combines the statutory office of Data Protection Commissioner under the Law with the office of Information Commissioner for the purposes of the Freedom of Information (Jersey) Law 2011.

If the Information Commissioner becomes aware that a data controller is in breach of the Law, an enforcement notice may be issued requiring the data controller to rectify the position.

Failure to comply with an enforcement notice is a criminal offence and can be punished with an unlimited fine.

ELECTRONIC MARKETING

The Law will apply to most electronic marketing.

ONLINE PRIVACY

The 2011 amendments implemented by the UK in relation to cookies have not found their way into Jersey law and there are no immediate plans for this to be done, however the Law will generally apply.

KEY CONTACTS

Carey Olsen
www.careyolsen.com

Huw Thomas
Counsel
T +44 1534 888900
huw.thomas@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our **Data Privacy Scorebox** to assess your organisation's level of data protection maturity.