

The Cayman Islands' Data Protection Law

Introduction

The Data Protection Law 2017 (“the Law”) was passed by the Cayman Islands’ Legislative Assembly on March 27th 2017 and will come into effect in January 2019.

Generally, the Law imposes strict regulations on entities handling personal data (data controllers), while simultaneously giving greater legal entitlements to persons whose data is being processed (data subjects). Given the considerable changes that the statute imposes, it is vital that businesses familiarise themselves with the Law and adjust their practices if necessary.

The Need for the Law

The Law seeks to comply with the European Commission’s “adequacy standard” as instituted by the Data Protection Directive (1995) and the General Data Protection Regulation. Currently, entities within the European Union are only permitted to transfer personal data to countries outside of the EU/EEA that comply with their established “adequacy standard.” “Personal data” is defined as any data relating to a living individual, including mere opinion of an individual.

The 2017 Law will now allow the Cayman Islands to benefit from greater access into the European market, as the handling of personal data is frequently necessary to facilitate business transactions.

Data Protection Principles

There are eight main data protection principles that a data controller must align their practices with:

1. Personal data must be processed fairly and can only be processed if certain conditions set out in the law are met (e.g. consent is given or there is a legal obligation). ‘Processing’ is defined broadly as to generally mean the obtaining, handling, and destruction of data.
2. Personal data must be obtained for specified lawful purposes.
3. Personal data must be adequate, relevant, and not excessive in relation to the purpose for which it was obtained.
4. Personal data must be up to date and accurate.
5. Personal data must not be kept longer than is necessary in relation to the purpose for which it was obtained.
6. Personal data must be processed in accordance with the rights of the data subjects under the Law.

7. Personal data must be protected by appropriate technical and organizational security measures to ensure against unauthorized or unlawful use, loss, destruction or damage.
8. Personal data must not be transferred abroad unless an adequate level of protection is guaranteed (i.e. a representative data controller is designated or the country adheres to data protection standards equivalent to the Law).

Data Controllers and The Law

“Data controller” means the person who, alone or jointly with others, determines the purposes, conditions and manner in which any personal data are, or are to be, processed and includes any local representatives (i.e. if a data controller is established outside of the Cayman Islands but personal data is still being processed in the Cayman Islands, then a local representative must be established in the Islands, who shall be held to the Law’s standards as if they were the data controller).

The Law imposes a responsibility on all data controllers to adhere to the data protection principles set out above, while also ensuring the compliance by all third party individuals processing data on behalf of the data controller. Businesses must now ensure that an organised system is in place, which allows data controllers to actively monitor any employees who are processing data on their behalf.

It is worth noting that there are additional, more onerous, requirements in order for a data controller to process sensitive personal data. This relates to personal data consisting of:-

- Racial or ethnic origin;
- Political opinions;
- Religious or other similar beliefs;
- Trade union membership;
- Genetic data;
- Physical or mental health conditions, sexual information and medical data;
- Commission or alleged commission of offences.

Finally, data controllers must inform data subjects and the newly appointed office of the Ombudsman of all personal data breaches. The Ombudsman is responsible for maladministration complaints previously handled by the Information Commissioner and the Complaints Commissioner.

Rights of Data Subjects

“Data subject” means-

- a. An identified living individual; or
- b. A living individual who can be identified directly or indirectly by means reasonably likely to be used by the data controller or by any other person

Under the Law, data subjects are given considerable rights in respect to how their personal data is processed, such as-

- The right to access their own personal data and information regarding its use;
- The right to request a cease to all processing of personal data;
- The right to seek compensation from damages caused by violation of the Law;
- The right to seek destruction or to request rectification of incorrect personal data;
- The right to bring a violation of the Law directly to the Ombudsman.

All requests made by data subjects must be in writing and usually accompanied by a fee. A data controller must respond to all written requests within 30 days. However, should the data controller require further information from a data subject before fulfilling a request, the 30-day time limit will pause; when the appropriate information is provided, the 30-day time limit will resume.

Enforcement

The enforcement of the Law is the responsibility of the Ombudsman. As such, he or she may impose monetary penalties up to CI\$250,000 and certain offences, such as making false statements to the Ombudsman, may be punishable by imprisonment up to 5 years depending on conviction in a court of law. As such, it is of the utmost importance that adherence to the Law is practiced and maintained.

How to Prepare

First and foremost, companies should perform an audit to properly examine how data is currently being processed and update any procedures if necessary. If a person is not already appointed to oversee data management, a data controller should be formally designated and trained, if necessary.

Most importantly, keep an eye on the news. Recently, a “working group” of eight private and public citizens, including the Information Commissioner, have been appointed to review the Law and plan the



process of implementation; their work should be monitored closely in order to stay up to date on announcements of regulations and adherence deadlines.

Further Information

At Broadhurst LLC we have 25 years experience of dealing with corporate and regulatory matter and have a proven track record. We would be pleased to assist with compliance with the Data Protection Law. If you have any queries on the above please contact info@broadhurstllc.com

This publication and the material on this website was prepared for general information purposes only to provide an overview of the subject matter. It is not a substitute for legal advice nor is it legal opinion and should not be taken as such. It deals in broad terms only and is subject to change without notice. If you require legal advice, please contact us and arrange a consultation.