COLLAS CRILL

Cayman Islands Data Protection Law

SEPTEMBER 2019

Overview

The Data Protection Law (2017) (the 'DPL') comes into force in the Cayman Islands on 30 September 2019. The DPL will implement established data protection principles in line with those that are being adopted around the world - most notably the adoption of the General Data Protection Regulation ('GDPR') by countries within the European Union and European Economic Area. The DPL imposes obligations on data controllers and provides and rights protections to identified- or identifiable living individuals ('data subjects') in relation to the processing of their Personal Data.

What is Personal Data?

Broadly, personal data ('Personal Data') is data which relates to a living individual who can be identified from such data. Personal Data includes:

- a living individual's location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the data subject;
- an expression of opinion about a living individual; or
- any indication of the intentions of the data controller or any other person in resect of the living individual.

Sensitive Personal Data

Within the concept of Personal Data, there is a subset of sensitive personal data which qualifies for an additional level of protection under the DPL ('Sensitive Personal Data').

Sensitive Personal Data means, in relation to a data subject, Personal Data consisting of:

- the data subject's racial or ethnic origin;
- the data subject's political opinions;
- the data subject's religious beliefs or other beliefs of a similar nature;
- the data subject's membership of a trade union;
- the data subject's genetic data;
- the data subject's physical or mental health or condition;
- the data subject's medical data;
- the data subject's sex life;

- the commission, or alleged commission, of an offence by the data subject; or
- any proceedings against the data subject for any offence committed, or alleged to have been committed.

Who must comply with the DPL?

Data Controllers

A data controller is person or organisation which exercises control over Personal Data by making decisions about why and how Personal Data is processed.

The DPL requires a data controller to apply the eight data protection principles (the '**Principles**') in relation to any personal data which it processes or which is processed by another person on its behalf.

The DPL will apply to any data controller established within the Cayman Islands and to any data controller which is established outside the Cayman Islands which processes Personal Data within the Cayman Islands.

Most Cayman Islands investment funds will, and some Cayman Islands investment managers may, fall under the definition of data controllers.

Data Processors

A data processor is an entity separate from a data controller which processes data on behalf of a data controller.

Whenever a data controller uses a data processor, the data controller must ensure there are agreed terms and conditions in accordance between the data controller and the data processor which comply with the DPL. These 'data processing' agreements ensure that both parties are complying with the Principles.

What are the Principles?

The eight data protection principles, broadly, are that Personal Data must:

1. be processed fairly and lawfully in compliance with the DPL;
2. only be obtained for one or more specified lawful purposes;
3. be adequate, relevant and not excessive in relation to the purpose(s) for which it was obtained;
4. be accurate and up to date;
5. not be kept longer than is necessary for the purpose for which it was obtained;
6. be processed in accordance with the rights of data subjects as specified under the DPL;
7. be protected by appropriate technical and organizational measures to ensure its safety against unauthorized or unlawful use, accidental loss, destruction or damage; and
8. not be transferred abroad unless the country/territory to which it is being transferred ensures there is an adequate level of protection in relation to such Personal Data.

Processing of Personal Data

The DPL broadly defines processing, as it relates to Personal Data, as obtaining, recording or holding Personal Data, or carrying out any operation or set of operations on Personal Data, including:

- organising, adapting or altering Personal Data;
- retrieving, consulting or using Personal Data;
- disclosing Personal Data by transmission, dissemination or otherwise making it available; or
- aligning, combining, blocking, erasing or destroying Personal Data.

Broadly speaking, most activities that affect Personal Data will be considered processing.

There are requirements for processing Personal Data and at least one of the following must apply whenever you process personal data:

- the data subject has given consent to the processing;
- the processing is necessary for the performance of a contract between the data controller and data subject;
- the processing is necessary for complying with a law or laws;
- the processing is necessary in order to protect the data subject's life;
- the processing is necessary to perform a public function, or a function of a public nature exercised in the public interest; or
- the processing is necessary for the legitimate interests pursued by the data controller or a third party (except where the processing is unwarranted because it prejudices the rights and freedoms or legitimate interests of the data subject).

Processing of Sensitive Personal Data

Sensitive Personal Data is given special protections under the DPL. In addition to the requirements for processing Personal Data, one of the following pre-requirements must be met in order to process Sensitive Personal Data:

- the data subject has given specific consent to the processing;
- the processing is necessary for the purposes of exercising or performing a legal right or obligation in connection with the data subjects employment;
- the processing is necessary to protect (i) the vital interests of the data subject or of another person where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject; or (ii) the vital interests of another person in a case where consent by or on behalf of the data subject has been unreasonably withheld;
- the processing (i) is carried out in the course of legitimate activities carried out by a non-profit body or association; (ii) is carried out with appropriate safeguards for the rights and freedoms of the data subjects;

(iii) relates only to data subjects who are members of the body or organisation or who have regular contact with it in connection with its purposes; and (iv) does not involve the disclosure of personal data to a third party without the consent of the data subject;

- the data has been made public as a result of steps taken by the data subject;
- the processing is (i) necessary for the purpose of, or in connection with, any legal proceedings; (ii) necessary for the purpose of obtaining legal advice; or (iii) otherwise necessary for the purposes of establishing, exercising or defending legal rights;
- the processing is necessary for the administration of justice or the exercise of any statutory, governmental or public functions;
- the processing is necessary for medical purposes and is undertaken by (i) a health professional; or (ii) a person who (in the circumstances) owes a duty of confidentiality equivalent to that which would arise if that person were a health professional.

Rights of Data Subjects

Under the DPL, data subjects have certain rights (subject to limitations in relation to how their personal data is handled), including the rights to:

- be informed about the use of their Personal Data;
- access their Personal Data and inquire about its source;
- require the processing of their Personal Data to cease or not begin;
- require the processing of their Personal Data for the purpose of direct marketing to cease or not begin;
- require that no decision which will significantly affect them be made solely by the processing by automatic means of their Personal Data;
- seek compensation for damages caused as a result of contravention of the DPL; and
- complain to the Ombudsman where a violation has occurred and to seek an order to rectify, block, erase or destroy inaccurate Personal Data and opinions based on such inaccurate information.

Requests made by data subjects to data controllers in relation to their rights must be made in writing and any fees that a data controller may require in relation to responding to such a request must be paid by the data subject at the same time as submitting the request.

Data controllers have up to 30 days to respond to requests, provided no further information is needed from the data subject. If further information is required, the response period will be paused and will resume only when the additional information is provided.

The Ombudsman

The Ombudsman is the supervisory authority for data protection related matters in the Cayman Islands and further information in respect of the Ombudsman can be found on its website.

Enforcement and penalties

The Ombudsman will have the authority, power and duty to enforce the DPL. Its broad powers include (amongst others) the power to investigate, monitor and report on complaints and data controllers.

Penalties for failing to comply with provisions of the DPL include fines ranging up to CI$250,000 and/or imprisonment for up to five years.

What do you need to do?

Completing the following actions will help your organization comply with the DPL:

- Determining whether your organisation is a data controller or a data processor under the DPL and understanding how the DPL may apply;
- Conducting an audit to determine what Personal Data is held or being processed by your organization and what policies and procedures (if any) your organisation currently has in place with regards the handling of Personal Data;
- Reviewing and updating where necessary, existing internal and external data handling policies and procedures to ensure compliance with the DPL;
- If necessary, preparing a privacy notice to explain to data subjects how you will process and keep their Personal Data;
- If you use a data processor, ensuring there is a written contract (a 'data processing agreement') in place setting out the details of how Personal Data is handled and processed and so that both parties understand and comply with their responsibilities and liabilities under the DPL.

Please contact your usual Collas Crill contact or a member of our team listed here for additional information or guidance on the Data Protection Law, 2017.