1. Background and Overview
On 27 March 2017 the Data Protection Law, 2017 (Law) was passed by the Legislative Assembly of the Cayman Islands. Once enacted, the Law will introduce for the first time in the Cayman Islands a legislative framework on data protection. Although the timeframe for the enactment of the Law is not yet known, the Law will come into force on a date set by Cabinet Order, and different dates may be appointed for different provisions of the Law and in relation to different matters.

This note is not a comprehensive guide to the Law and deals only with the key concepts and obligations which arise from it.

2. What should I do now?
In addition to informing yourself about the Law, we recommend that you implement the following proactive measures prior to the commencement of the Law:

- understand your organisation’s treatment under the Law and the extent of any exemptions that may apply to it.
- conduct an audit (whether formal or informal) of your organisation’s current arrangements and understand how personal data is processed.
- create or update your internal data protection policies and procedures (including procedures to validate information held about data subjects).
- create or update your external data protection policies and procedures to inform your clients and employees about the data held on them and the purposes for which such data is processed.
- agree to responsibilities within your organisation to ensure compliance with the Law and to enforce your privacy policies and to deal with information requests from data subjects.

3. Key definitions and concepts

Data Controller
A person, firm or company who, alone or jointly with others, determines the purposes, conditions and manner in which any personal data is, or are to be, processed. In certain instances, a data controller will also include nominees of the data controller. In an employment context, a data controller will normally be an employer. In a commercial context, a data controller will normally be a service provider that processes personal data in the performance of its services.

The Law applies to any data controller in respect of personal data (a) that is established in the Cayman Islands and the personal data is processed in the context of that establishment; or (b) that is not established in the Cayman Islands but the personal data is processed in the Cayman Islands otherwise than for the purposes of transit of the data through the Cayman Islands.

Data Subject
Any identified living individual or any 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, e.g. employees, applicants, contractors, agency workers and other personnel.

Processing
Obtaining, recording or holding data, or carrying out any operation or set of operations on personal data, including organising, adapting, altering, retrieving, consulting, or using personal data or disclosing personal data by transmission, dissemination or otherwise making it available or aligning, combining, blocking, erasing or destroying personal data.

Data Processor
A person, firm or company that processes personal data on behalf of the data controller, but does not include an employee of the data controller.

Personal Data
Data relating to a living individual who can be identified and includes data such as -

- the 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 living individual.
- an expression of opinion about the living individual.
- any indication of the intentions of the data controller or any other person in respect of the living
Sensitive Personal Data
Sensitive personal data is personal data in relation to the data subject (which qualifies for an additional level of protection under the Law) consisting of information as to:

- racial or ethnic origin.
- political opinions.
- religious or other similar beliefs.
- trade union membership.
- medical or genetic data.
- physical or mental health or condition.
- sexual life.
- the commission or alleged commission of any criminal offences.
- any criminal proceedings or convictions (including verdict and sentences).

Data Protection Principles
There are eight data protection principles. It is the duty of a data controller to comply with the principles:

1. personal data shall be processed fairly.
2. personal data shall be processed only for one or more specified lawful purposes.
3. personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are collected/processed.
4. personal data shall be accurate and up to date.
5. personal data shall not be kept for longer than is necessary.
6. personal data shall be processed in accordance with the rights of data subjects under the Law.
7. appropriate technical and organisational measures shall be taken in relation to personal data.
8. personal data shall not be transferred outside the Cayman Islands unless an adequate level of protection for the rights and freedoms of data subjects is ensured.

4. Requirements for lawful Data Processing - the basics

Data Protection Principles
Under the Law, all data controllers are required to comply with the data protection principles that relate to the personal data that the data controller processes. Data controllers are also required to ensure that third parties comply with the protection principles if such third parties are processing personal data on the data controller’s behalf.

Personal Data
In order for a data controller to process personal data fairly (a required data protection principle), the identity of the data controller and the purpose for which the personal data is processed must be disclosed. In addition, one of the following preconditions must also be satisfied:

- the data subject has given consent to the processing.²
- the processing is necessary for (a) the performance of a contract to which the data subject is a party or (b) taking steps at the request of the data subject with a view to entering into a contract.
- the processing is necessary for legal compliance (other than contractual compliance).
- the processing is necessary to protect the vital interests of the data controller.³
- the processing is necessary for the administration of justice or the exercise of statutory, governmental or public functions.
- the processing is necessary for the purposes of legitimate interests pursued by the data controller or the third party to whom the data is disclosed, except if the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Sensitive Personal Data
Sensitive personal data is given special protection under the Law. In order for a data controller to process sensitive personal data fairly, in addition to fulfilling the conditions for processing regular personal data fairly, one of the following preconditions must also be satisfied:

- the data subject has given consent to the processing.
- processing is necessary for exercising or performing any legal right or obligation in connection with the data subject’s employment.
- processing is necessary (a) to protect the vital interests of the data subject or another person where consent cannot be given by the data subject or the data controller cannot reasonably be expected to obtain such consent or (b) to protect the vital interests of another person where consent of the data subject has been unreasonably withheld.
- processing is carried out in the course of legitimate activities by certain non-profit associations and certain conditions are met.
- the data has been made public as a result of steps taken by the data subject.
- processing is necessary for the purposes of legal proceedings, obtaining legal advice or establishing, exercising or defending legal rights.
- processing is necessary for the administration of justice or the exercise of statutory, governmental or public functions.
- processing is necessary for medical purposes and is performed by a health professional or a person who, in the circumstances, owes a duty of confidentiality equivalent to that which would arise if that person were a health professional.
5. Rights of Data Subjects

Right of Notification and Access
As discussed above, data controllers generally have the obligation to process information fairly and notify data subjects if their personal data is being processed. If personal data is being processed, a data subject is entitled to be given the following information by the data controller as soon as reasonably practicable:

- a description of the personal data held in respect of the data subject; and
- a description of the purposes for which the personal data is being processed.

In addition to the initial notification requirements set out above, unless a limited range of exemptions apply, data subjects are also entitled to request from data controllers:

- a description of the personal data held in respect of the data subject.
- a description of the purposes for which the personal data is being processed.
- a description of the recipients to whom the personal data may be disclosed.
- communication in intelligible form of the personal data and the source of the data.

The data controller need not supply any information where the request has not been made in writing and/or the data controller’s fee (within limits to be set out in regulations) has not been paid.

If the data controller has not been supplied with such information as he reasonably requires to satisfy himself as to the identity of the person making the request and/or to locate the information, the data controller need not supply the information provided the data controller has informed the data subject in writing of this requirement.

The time limit for providing the information is 30 days from the day the data controller receives the request and the fee, but where the data controller has requested further information to satisfy himself of the identity of the data subject and/or to locate the information this period shall not resume until the information has been supplied.

If complying with a subject access request cannot be done without disclosing personal data relating to another data subject who can be identified from that personal data, then information may be withheld, unless:

- that other data subject has consented to such disclosure.
- it is reasonable in all the circumstances to comply with the request without the consent of the other data subject.

However, even where the data controller elects not to disclose personal data, such of the personal data as can be disclosed without revealing the identity of the other individual (including by the removal of names or other identifying information) must nevertheless be disclosed.

Should a data controller fail to comply with a subject access request, a data subject may apply to the Information Commissioner (Commissioner) who has broad powers to order compliance and levy fines.

Right to Cease Processing
A data subject is entitled at any time by notice in writing to a data controller to require the data controller to cease processing, or not to begin processing, or to cease processing for a specified purpose or in a specified manner, the data subject’s personal data. The data controller shall as soon as practicable, but within 21 days, comply with the notice, unless:

- the processing is necessary for (a) the performance of a contract to which the data subject is a party or (b) taking steps at the request of the data subject with a view to entering into a contract.
- the processing is necessary for compliance with any legal obligation to which the data controller is subject (other than a contractual obligation).
- the processing is necessary to protect the vital interests of the data subject.

Automated Decision Making
A data subject is entitled at any time, by notice in writing to a data controller, to require the data controller to ensure that no decision taken by or on behalf of the data controller that significantly affects the data subject is based solely on the processing by automatic means of the data subject’s personal data for the purpose of evaluating the data subject’s performance at work, creditworthiness, reliability, conduct or any other matters relating to the data subject.

If decisions are taken automatically that significantly affect a data subject based solely on processing by automatic means of the data subject’s personal data for the purpose of evaluating the data subject’s performance at work, creditworthiness, reliability, conduct or any other matters relating to the data subject, the data controller shall as soon as reasonably practicable notify the data subject that the decision was taken on that basis. The data subject is entitled within 21 days of receiving that notification, to notify the data controller in writing requiring the data controller to reconsider the decision or to take a new decision otherwise than on that basis.
Direct Marketing
A data subject is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing the data subject’s personal data for the purposes of direct marketing.

“Direct marketing” means the communication (by whatever means) of any advertising, marketing, promotional or similar material, that is directed to particular individuals.

Rectification, Blocking, Erasure, Destruction
A data subject can apply to the Commissioner on the basis that personal data held by a data controller is inaccurate. If the Commissioner is satisfied that personal data is inaccurate, the Commissioner may order the data controller to rectify, block, erase or destroy such data, or certain other personal data held by the data controller which contains an expression of opinion which appears to the Commissioner to be based on the inaccurate data.

If data received by the data controller has been accurately recorded then the Commissioner may make an order requiring that the data in question be supplemented by a statement of the true facts.

The Commissioner may require the data controller to notify third parties to whom the data has been disclosed of the rectification, blocking, erasure or destruction.

Compensation
A person who suffers damage by reason of a data controller’s contravention of the Law is entitled to compensation from the data controller for that damage.

6. Offences under the Law – the Consequences
It should be noted that a director, manager, secretary or other company officer may be guilty of an offence in addition to the company if the offence is proved to have been committed with their consent or connivance or attributable to their neglect.

Offences under the Law include:
- unlawfully obtaining or disclosing personal data.
- unlawful sale of personal data.
- failing to comply with an enforcement order or an information order.

Fines under the Law could be as high as CI $100,000 (US $122,000) and certain offences are punishable by imprisonment. Under the Law the Commissioner also has the right to serve a data controller with a monetary penalty order if the Commissioner is satisfied on a balance of probabilities that there has been a serious contravention of the Law by the data controller and the contravention was of a kind likely to cause substantial damage or substantial distress to the data subject. Monetary penalty orders could be as high as CI $250,000 (US $305,000).

7. Exemptions
It should be noted that the Law contains a number of very detailed exemptions and modifications that may apply. Without being exhaustive, exemptions and modifications may apply in situations relating to trusts, corporate finance services, national security, crime, health, education, social work, journalism, historical or scientific research, disclosures required by law or legal proceedings and legal professional privilege.

The existence and scope of exemptions which may be applicable to your business should be considered in detail. We advise anyone seeking to rely on such exemptions to contact our office to conduct an initial exemption analysis and/or a full data protection audit.

We expect that regulations and guidance on the Law will be issued prior to its implementation. We shall provide a further update in due course.

We would be happy to discuss the implications of the Data Protection Law, 2017 for your business or organisation. Please contact your usual Ogier attorney or a member of our team listed here.

---

1. If the data controller is not established in the Cayman Islands but the personal data are processed in the Cayman Islands, (otherwise than for the purposes of transit of the data through the Cayman Islands) the data controller must nominate a local representative established in the Cayman Islands who will be the data controller for the purposes of the Law.

2. “Consent” in relation to a data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the said data subject.

3. In other jurisdictions this condition is generally understood to only apply to matters of life and death.
Contact us

James Heinicke
Partner
T+1 345 815 1768
M+1 345 516 0453
james.heinicke@ogier.com

Cory Macculloch
Associate
T+1 345 815 1773
M+1 345 326 3328
cory.macculloch@ogier.com

89 Nexus Way
Camana Bay
Grand Cayman
Cayman Islands KY1-9009
T +1 345 949 9876
F +1 345 949 9877
E cayman@ogier.com