1. Background and Overview
The Data Protection Law, 2017 (Law) came into force in the Cayman Islands on 30 September 2019. The Law introduces for the first time in the Cayman Islands a legislative framework on data protection.

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

2. Key Definitions & Concepts
The Law applies to 'personal data' of 'data subject' that is 'processed' by 'data controllers' or 'data processors'.

Data Controller
This is a person, firm or company who, alone or jointly with others, determines the purposes, conditions and manner in which any personal data is, or will be, processed. 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. In an investment fund context, this would be the fund entity and, in some cases, the investment managers.

A data controller is responsible for applying the requirements of the Law and applying the data protection principles to the personal data which it processes (or which are processed by someone else on its behalf).

The Law applies to any data controller in respect of the processing of personal data if the data controller is: (a) established in the Cayman Islands and the personal data is processed in the context of that establishment; or (b) 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. (1)

Data Subject
This is 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.

Processing
This is defined very broadly. It means obtaining, recording or holding data, or carrying out any operation or set of operations involving personal data, including organising, adapting, altering, retrieving, consulting, using or disclosing data by transmission, dissemination or otherwise making it available or aligning, combining, blocking, erasing or destroying personal data.

Sensitive Personal Data
This 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 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; or
- any indication of the intentions of the data controller or any other person in respect of the living individual.

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

- 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;
Cayman Islands Data Protection Law

- the commission or alleged commission of any criminal offences; or
- any criminal proceedings or convictions (including verdict and sentencing).

**Data Protection Principles**

There are eight data protection principles under the Law. It is the duty of a data controller to comply with the principles:

1. Personal data shall be processed fairly.
   - Data must not be processed in a way that is unduly detrimental, unexpected or misleading;
   - Data controllers must be clear, open and honest about why and how personal data is handled; and
   - Data controllers must have valid grounds under the Law for handling personal data.

2. Personal data shall be processed only for one or more specified lawful purposes.
   - Data controllers should:
     - inform the data subject of the reason why they are processing data;
     - document the purpose for the data processing; and
     - only use the data for another purpose if it is compatible with the original purpose, if the data subject consents, or if there is another legal basis for doing so.

3. Personal data shall be adequate, relevant and not excessive.
   - Data controllers must ensure that the personal data they are processing:
     - is sufficient to fulfil the data controller’s stated purpose;
     - has a clear link to that purpose; and
     - is limited to what is necessary for that purpose.

4. Personal data shall be accurate and up to date.
   - Data controllers should:
     - take all reasonable steps to ensure that personal data is not incorrect or misleading;
     - consider whether personal data should be kept updated; and
     - take reasonable steps to correct or erase personal data as soon as possible upon discovering that it is incorrect or misleading.

5. Personal data shall not be kept for longer than is necessary.
   - Data controllers:
     - must not keep personal data for longer than is needed;
     - should consider how long they need to keep personal data; and
     - should erase or anonymize data when it is no longer needed.

6. Personal data shall be processed in accordance with the rights of data subjects.
   - In summary these rights are:
     - the right to be informed;
     - the right of access;
     - the right to rectification, blocking, erasure, destruction;
     - the right to cease processing;
     - the right in relation to automated decision making;
     - the right to stop direct marketing; and
     - the right to complain and seek compensation.

7. Appropriate technical and organisational measures shall be taken in relation to personal data.
   - Security measures taken by a data controller should be ‘appropriate’ to the risks presented by its processing of personal data;
   - Technical measures should include physical security and cyber security; and
   - Appropriate internal processes should be in place for testing and assessing the effectiveness of security measures.

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.
   - Generally, countries or territories that are subject to GDPR, and some non-EU countries including Guernsey, Jersey, New Zealand and Switzerland, are deemed to have an adequate level of protection in place.
   - We note only commercial organisations in Canada and US recipients that are part of the Privacy Shield are deemed to have adequate protection in place.
   - This principle does not apply in all circumstances (for example, where the data subject has consented to the transfer or where the transfer is necessary for performance of a contract between the data subject and the data controller).

3. 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 data protection principles if such third parties are processing personal data on the data controller’s behalf.
Lawful Basis for Processing
In order for a data controller to process personal data fairly (i.e. to comply with the first 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 fulfilled:

- the data subject has given consent to the processing; (2)
- the processing is necessary for the performance of a contract to which the data subject is a party or 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 data subject’s life;
- the processing is necessary for administration of justice or exercise of statutory, governmental or public functions; or
- 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 by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Processing of Sensitive Personal Data
Sensitive personal data is given special protection under the Law. In addition to fulfilling the conditions for processing regular personal data, one of the following preconditions must also be fulfilled:

- 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 to protect the vital interests of the data subject or of another person where consent cannot be given or where the data controller cannot reasonably be expected to obtain consent;
- 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; or
- 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.

4. Rights of Data Subjects
All personal data must be processed in accordance of the rights of data subjects set out below.

Right to be Informed
As discussed above, data controllers generally have the obligation to process information fairly and inform 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:

- identity of the data controller;
- a description of the purposes for which the personal data is being processed.

This information would usually be communicated to the data subject via a privacy notice.

Right of Access
In addition to the initial notification requirements, 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; and
- 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 fee (if applicable) has not been paid. If a request from a data subject is determined to be manifestly unfounded or excessive because the request: (a) is repetitive; (b) is fraudulent in nature; or (c) would divert the resources of the data controller unreasonably, the data controller may charge such fee as covers the cost of providing the requested data and information or may refuse to act on the request and provide the reasons for doing so. Any fee charged by a data controller must be reasonable taking into account the administrative cost of providing the personal data or information requested. Otherwise, information should be provided by the data controller free of charge.

Should a data controller fail to comply with a subject access request, a data subject may apply to the Ombudsman who has broad powers to order compliance and levy fines.
Right to Rectification, Blocking, Erasure, Destruction

The Law does not expressly grant data subjects the right to ask a data controller to correct inaccuracies in their personal data. However, a data subject can apply to the Ombudsman on the basis that personal data held by a data controller is inaccurate. If the Ombudsman is satisfied that personal data is inaccurate, the Ombudsman 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 Ombudsman to be based on the inaccurate data.

In addition, should the data have been accurate but the data controller have contravened the terms of the Law and the Ombudsman is satisfied that there is a material risk of such further contravention, it may make an order to rectify, block, erase or destroy the data.

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

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 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 the performance of a contract to which the data subject is or may become a party;
- the processing is necessary for compliance with any legal obligation (other than a contractual obligation) to which the data controller is subject;
- the processing is necessary to protect the vital interests of the data subject; or
- approval has been obtained from the Ombudsman to not comply with the data subject’s request.

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 of the data subject’s personal data by automatic means. This includes decisions 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 for such purposes are made based solely on automatic processing of the data subject’s personal data, 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 without relying on such automatic process.

Right to Stop Direct Marketing

A data subject is entitled at any time by giving reasonable notice in writing to a data controller to require the data controller 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 material, or marketing material, that is directed to particular data subjects.

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.

5. 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; and
- failing to comply with an enforcement notice or an information notice.

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 Ombudsman also has the right to serve a data controller with a monetary penalty order if the Ombudsman is satisfied on a balance of probabilities that there has been a serious contravention of this 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 ($305,000).

6. Exemptions

It should be noted that the Law contains a number of 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.

7. What Should I Do Now?
In order to ensure compliance with the Law, you should:

• understand your organisation’s treatment under the Law, and, in particular, whether it is a data controller or data processor, 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;
• review, update or create your internal data protection policies and procedures if required (including procedures to validate information held about data subjects);
• consider the extent to which the Law applies to your non-Cayman established clients, if any;
• review, update or create your external privacy notice to inform your clients and employees about the data held on them and the purposes for which such data is processed; and
• 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.

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 then it must nominate a local representative established in the Cayman Islands who will be deemed also to be a data controller.

(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.
Legal services in:
British Virgin Islands
Cayman Islands
Guernsey
Hong Kong
Jersey
London
Luxembourg
Shanghai
Tokyo

Ogier provides practical advice on BVI, Cayman Islands, Guernsey, Jersey and Luxembourg law through its global network of offices. Ours is the only firm to advise on these five laws. We regularly win awards for the quality of our client service, our work and our people.

This client briefing has been prepared for clients and professional associates of Ogier. The information and expressions of opinion which it contains are not intended to be a comprehensive study or to provide legal advice and should not be treated as a substitute for specific advice concerning individual situations.

Regulatory information can be found at www.ogier.com