HARNEYS

Data Protection in the Cayman Islands

This legal guide provides an overview of how the Cayman Islands' data protection regime operates and what in scope entities need to have in place to ensure they are compliant.

Overview

The Data Protection Act (2021 Revision) (the ***DP Act***) governs how a "data controller" may process, use and retain personal data.

Anyone who falls within the definition of a "data controller" must comply with eight data protection principles in relation to any personal data processed by the data controller. Where a data controller engages a third party (a "data processor") to process personal data on its behalf, the data controller must also ensure that third party complies with the eight data protection principles.

The DP Act also sets out the rights of individuals to control their personal data and implements a system to protect against the misuse of personal data.

The DP Act is similar to the European Union's General Data Protection Regulation (***GDPR***) with which many clients will be familiar.

What are the eight Data Protection Principles?

The eight data protection principles are:

- fairness and lawfulness
- purpose limitation
- data minimisation
- accuracy
- storage limitations
- accountability and respect of rights of data subject
- integrity and confidentiality (security)
- international transfers

Who must comply with the DP Act?

Any data controller that is a:

- Cayman Islands company or partnership
- foreign company registered in the Cayman Islands, or
- business operating in the Cayman Islands,

that processes personal data in the context of being established in the Cayman Islands must comply with the DP Act.

Any data controller that processes personal data in the Cayman Islands, regardless of where it is established, must also comply with the DP Act and appoint a local representative.

The individual to which the personal data relates does not need to be in the Cayman Islands or a citizen of the Cayman Islands.

Who is a data controller or processor?

A "data controller" is an entity that determines the purposes, conditions and manner in which any personal data are processed or are to be processed. Processing includes obtaining, recording or holding data or carrying out any activity on personal data, such as organising, altering, using or disclosing personal data.

A local representative referred to above is also a data controller.

A "data processor" is any person, entity, public authority, agency or other body which processes personal data on behalf of a data controller (but does not include an employee of the data controller).

A business will be considered a data controller of the data it collects and processes for the purposes of its business.

A service provider which receives personal data from a business and processes that data on behalf of the business is a data processor. Examples of data processors will include fund administrators, cloud or other software platform providers, payroll providers, or marketing firms with access to the business' client lists.

What is personal data?

"Personal data" is any type of data that can be used to identify a living individual, such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

The data protection regime is therefore relevant only to the extent that the data in question can be used to identify a data subject.

Examples of personal data include items such as names, email addresses (business or personal), identity card numbers, or telephone numbers – ie any information which allows the data subject to be identified.

"Sensitive personal data" is defined as any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, medical data, data concerning physical or mental health or condition, or sex life or data relating to commission of an offence (including proceedings). Where sensitive personal data is being processed the data controller must adhere to additional conditions described below.

What must a data controller do to comply with the DP Act?

A data controller must ensure that it complies with the eight data protection principles when it processes any personal data.

In order for personal data to be processed lawfully under the first data protection principle, at least one of the following conditions must be met:

- the data subject gave consent
- processing is necessary for performance of a contract, or for pre-contractual steps taken at the data subject's request
- processing is necessary for compliance with any legal obligation of the data controller
- processing is necessary to protect the data subject's vital interests
- processing is necessary for exercise of public functions
- processing is necessary for the purposes of legitimate interests of the data controller

If a data controller is processing sensitive personal data, at least one of the following conditions must also be met (in addition to the above):

- the data subject gave consent
- the processing is necessary for the data subject's employment

- the processing is necessary to protect the data subject's vital interests
- the information is lawfully processed by a non-profit association
- the information has been made public by the data subject
- the processing is necessary for the purpose of legal proceedings
- the processing is necessary for the exercise of public functions
- the processing is necessary for medical purposes, and undertaken by a health professional or person owing a similar duty of confidentiality
- the processing is permitted by regulations

Considerations around consent

Where a data controller relies on a data subject giving consent to the processing, the data controller needs to ensure that:

- consent is given by a positive action to opt in
- consent is explicitly given
- the consent request is prominent, concise, separate from other terms and conditions, and easy to understand
- it is able to prove that consent was given
- it keeps adequate records of when and how consent was given
- there is an easy procedure to withdraw consent

'Consent' of the data subject is "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 data subject".

Consent is not considered a valid legal ground for the processing of personal data where there is a clear imbalance between the data subject and the controller. This is of particular relevance to the relationship between employer and employees.

Consent may be withdrawn by the data subject at any time.

Issues relating to consent will be most relevant in the context of the business' marketing materials/campaigns.

Transfer of data outside the Cayman Islands

Under the eighth data protection principle, personal data must not be transferred to a country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data, subject to certain exemptions (see below).

Adequate level of protection?

The Cayman Islands supervisory authority for the DP Act, the Office of the Ombudsman, will consider the following countries and territories as ensuring an adequate level of protection:

- the member states of the European Economic Area where GDPR is applicable, and
- any country or territory of which an adequacy decision has been adopted by the European Commission

For jurisdictions which do not fall within the above classification, or for transfers that are not exempt (see below), a data controller must assess the adequacy of the jurisdiction using at least all the criteria set out in the DP Act.

Exemptions from the eighth data protection principle

Under the DP Act the eighth data protection principle doesn't apply where:

- the data subject has consented to the transfer
- the transfer is necessary for the performance of a contract between the data subject and the data controller, or for pre-contractual steps taken at the data subject's request
- the transfer is necessary for the performance or conclusion of a contract between the data controller and a third party at the request of the data subject, or in the interests of the data subject
- the transfer is necessary for reasons of substantial public interest
- the transfer is necessary for legal proceedings, obtaining legal advice, or otherwise necessary to establish, exercise or defend legal rights
- the transfer is necessary to protect the data subject's vital interests
- the transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by a person to whom the data are or may be disclosed after the transfer
- the transfer is made on terms of a kind approved by the Office of the Ombudsman as ensuring adequate safeguards for the rights and freedoms of data subjects
- the transfer has been authorised by the Office of the Ombudsman as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects (such as a transfer made on the EU standard contractual clauses)
- the transfer is required under international cooperation arrangements between intelligence agencies or between regulatory agencies to combat organised crime, terrorism or drug trafficking or to carry out other cooperative functions

Are there any exemptions from the DP Act?

There are exemptions from the requirement to comply with some or all of the data protection principles such as for the purposes of safeguarding national security, investigation of crime and legal professional privilege. Any exemption must be assessed on a case-by-case basis.

What rights do data subjects have?

The sixth principle, being to process in accordance with the rights of data subjects, underscores the importance of all the rights of individuals under the DP Act:

- the right to be informed
- the right of access
- the right to rectification
- the right to stop/restrict processing
- the right to stop direct marketing
- the right in relation to automated decision making, and
- the right to complain and seek compensation

Looking at some of these rights more closely, a data subject must be informed of the following by a data controller:

- description of their personal data
- the purpose for processing the personal data
- the persons or types of persons to whom the personal data may be disclosed
- where the personal data may be transferred to outside of the Cayman Islands

- how the data controller safeguards the integrity and confidentiality of the personal data
- any other information required by the Cayman Islands Office of the Ombudsman

A data subject may request details of the personal data held by a data controller. If it is a valid request the data controller must provide such information within 30 days.

A data subject has the right to request that any inaccuracy or incompleteness in their personal data be corrected and the right to request that no automated decision making be made using their personal data.

At any time a data subject may request a data controller to cease processing their personal data for any reason, including direct marketing. The DP Act sets out various time limits for when such cessation must have happened; however, this right is not absolute and there are some limited exceptions to its scope.

A data subject has the right to lodge a complaint with the Office of the Ombudsman.

What happens if there is misuse of personal data?

Where there is a personal data breach, meaning where personal data is accidentally or unlawfully accessed, disclosed, altered, lost or destroyed, the data controller must notify the data subject and the Office of the Ombudsman of the breach without undue delay and in no longer than five days. A failure to do so is an offence under the DP Act.

Any person may make a complaint to the Office of the Ombudsman that personal data is not processed in accordance with the DP Act and the Office of the Ombudsman must determine whether or not to conduct an investigation.

What powers of enforcement does the Office of the Ombudsman have?

The Office of the Ombudsman has the power under the DP Act to require any person to provide information to it in order to fulfil its functions under the DP Act.

Where the Office of the Ombudsman believes the data controller is, or may be, in contravention of the DP Act, it may order a data controller to take, or refrain from, certain actions. It may also make monetary penalty orders.

The Office of the Ombudsman also has the power to seek an inspection and seizure warrant from the Cayman Islands Court.

Other offences under the DP Act

In addition to failing to notify the data subject and the Office of the Ombudsman of a data breach as described above, it is an offence under the DP Act to:

- fail to comply with an order
- fail to provide, alter or destroy information requested by the Office of the Ombudsman
- make a known or reckless false statement in connection with a request for information by the Office of the Ombudsman
- obstruct execution of an inspection and seizure warrant

Save for specific public interest exceptions, it is also an offence under the DP Act to:

- obtain or disclose personal data without the consent of the data controller
- procure such disclosure to a third party
- sell personal data that was obtained unlawfully
- offer to sell personal data that was, or will be, obtained unlawfully

What are the penalties for breach of the DP Act?

There are material financial penalties for persons that breach the DP Act. The penalties range from CI$10,000, to CI$250,000 and there are also possible terms of imprisonment for up to five years. Unlike the GDPR the penalties under the DP Act are fixed rather than based on turnover.

Where an offence under the DP Act is committed with the consent of any director, manager, secretary or similar officer of an entity then such person may also be liable for the applicable penalty.

Are there any guidance notes?

The Office of the Ombudsman has issued a Guide for Data Controllers to explain how the Office of the Ombudsman will likely interpret various provisions of the DP Act. The guide is largely based on the United Kingdom's Information Commissioner's Office's Guide to the GDPR and is a very useful starting point for information.

What should we do?

If you are within scope of the DP Act then you must:

- prepare a privacy notice to give to individuals to explain how you will process, use and retain their personal data
- review your procedures to ensure the manner in which you process and retain personal data complies with the DP Act and that you are able to retrieve specific personal data if requested to do so by a data subject or a relevant authority
- you may need to adopt a data processing, protection and retention policy
- if you engage a third party to process data on your behalf you will need to ensure there is a written contract for such engagement that addresses your obligations under the DP Act, including any transfer of data outside of the Cayman Islands

For investment funds this means they must:

- send the privacy notice to existing investors
- update subscription documents to include a privacy notice for new investors
- update offering documents to reflect the new requirements under the DP Act,

update agreements with any third parties that process personal data on behalf of the fund to ensure such processing is undertaken in compliance with the DP Act especially where there is transfer of data outside of the Cayman Islands.

For more information and key contacts please visit **harneys.com**

© Harneys, April 2025, 611139375.1

Harneys is a leading international offshore law firm. From locations around the globe, Harneys advises the world's top law firms, financial institutions and corporations on the laws of British Virgin Islands, Cayman Islands, Cyprus, Luxembourg, Bermuda, Anguilla, and Jersey. Jersey legal services are provided through a referral arrangement with Harneys (Jersey) which is an independently owned and controlled Jersey law firm. For more information about Harneys please visit harneys.com or contact us at marketing@harneys.com.

The foregoing is for general information only and not intended to be relied upon for legal advice in any specific or individual situation.