GUIDE

A quick guide to data protection in the Cayman Islands

Last reviewed: March 2023

Data Protection Act (2021 Revision)

The Data Protection Act (2021 Revision) (**DPA**) came into force on 30 September 2019 in order to protect individuals' rights in relation to their personal data. The DPA is based upon, and aims to provide equivalent protection to, the EU General Data Protection Regulation (**GDPR**), which came into force on 25 May 2018.

Who does it apply to?

- Data subjects – the individual whose data is being processed.
- Data controllers – the person who determines the means and purposes of processing data.
- Data processors – the person processing the data on behalf of the data controller.

What data does it apply to?

- Personal data – this includes data relating to a living individual who can be identified, such as the individual's name, address, online identifiers, factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity, and any expression of opinion on the individual or any indication of the intentions of a data controller in respect of the individual.
- Sensitive personal data – this includes personal data regarding, among other things, race, political opinions, religious beliefs, trade union memberships, genetic data, medical records, sex life, the commission or alleged commission of any offence and any related proceedings.

When does it apply to a data controller?

The DPA applies to:

1. data controllers established in the Cayman Islands where personal data is processed in the context of the establishment; and
2. data controllers not established in the Cayman Islands where personal data is processed in the Cayman Islands, otherwise than for the purpose of transit of data through the Cayman Islands (in such cases a local representative must be nominated as data controller).

The eight data protection principles

The DPA establishes eight principles of data protection for data controllers and processors, which provide that personal data must be:

1. Fairly processed and lawfully obtained.
2. Obtained for and processed in accordance with a specified lawful purpose.
3. Adequate, relevant and not excessive to the purpose for which it is collected or processed.

4. Accurate and up to date.
5. Kept for no longer than is necessary.
6. Processed in compliance with individuals' rights under the DPA.
7. Kept safe and secure.
8. Only transferred to another jurisdiction where adequate protection is provided.

The lawful conditions for processing

Under the first data protection principle, data controllers may only process personal data if they have a lawful condition for processing.

The lawful conditions for processing are:

- Consent – the data subject has given consent to processing.
- Contract – 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.
- Legal obligation – the processing is necessary for legal (other than contractual) compliance.
- Vital interests – the processing is necessary to protect the vital interests of the data subject.
- Public functions – the processing is necessary for the administration of justice or the exercise of statutory, governmental or public functions.
- Legitimate interests – the processing is necessary for the legitimate interests of the data controllers or a third party to whom the data is disclosed, unless the processing is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Sensitive personal data requires an additional condition to be fulfilled as well as one of the above conditions. These further preconditions relate to:

- Consent.
- Data subject's employment.
- Vital interests of the data subject or another where consent cannot be given or is unreasonably withheld.
- Information already made public by the data subject.
- Legal proceedings, legal advice, or establishing, exercising or defending legal rights.
- Administration of justice or the performance of public functions.
- Medical purposes (for health professionals or persons owing the same duty of confidentiality).

What rights does the DPA give individuals?

- Right to be informed and request access – A data subject has the right to be informed of processing (including by automatic means) and to be given a description of the data and purposes for processing. This must contain details of the recipients and whether it is intended for the data to be transferred overseas.
- Right to stop processing – A data subject can at any item by notice in writing request that a data controller cease processing. A data controller must comply within 21 days unless a lawful condition for processing exists and is notified to the data subject.
- Right to stop processing for direct marketing – A data subject can at any time by notice in writing request that a data controller cease processing for direct marketing purposes within a reasonable period.
- Right to apply for erasure, rectification, blocking or destruction – A data subject has the right to make a complaint to the Ombudsman in relation to inaccurate data. The Ombudsman may then order the data controller to rectify, block, erase or destroy the data.
- Rights in relation to automated decision making – A data subject has the right to request by notice in writing that a data controller ensure that no decision has been made solely by automatic means in relation to work performance, creditworthiness, reliability and conduct. Where no notice has been given, a data controller must notify the data subject that a decision was taken based on automatic means and that the data subject has 21 days to request the data controller to reconsider.

- Right to complain and seek compensation – An individual has the right to complain to the Ombudsman about any perceived violation of the DPA and to seek compensation for damages in the courts.

Exemptions from individual's rights

The main exemptions from an individual's rights under the DPA are as follows:

- Exemptions from all the rights of individuals if the data is required to safeguard national security.
- Exemptions from the right to be informed and request access for:
  - compliance with international tax treaties;
  - monitoring, inspection or regulatory functions exercised by official authorities (including regulation of the financial services industry);
  - legal professional privilege; and
  - trusts and wills.
- Exemptions from the right to be informed, right to stop processing and right to erasure for:
  - disclosure of information for quasi-judicial and legal proceedings; and
  - obtaining legal advice or for establishing, exercising or defending a legal right.

Data subject access requests

- A data subject access request (DSAR) is a request from a data subject for access to their personal data.
- Any DSAR must be received in writing.
- Data controllers have 30 days to respond either providing the data requested or requesting further information from the data subject to confirm their identity or help locate the data. Once further information has been provided, the data controller has 30 days to comply.
- There is no need to comply with a DSAR where:
  - it is not possible to do so;
  - it would require a disproportionate effort;
  - an identical request has recently been complied with; or
  - it would disclose the data of a third party (unless the third party has given consent or it would be considered unreasonable).
- Where there is a valid reason not to comply as above, the data subject must be notified within 30 days and informed of their right to complain to the Ombudsman.

Obligations in the event of a personal data breach

A breach in security leading to accidental or unlawful destruction, loss or disclosure of data must be notified to:

- the data subject; and
- the Ombudsman;

within 5 days of when the breach should have been discovered with reasonable due diligence.

Details must be given of the:

- nature of the breach;
- consequences;
- measures in place to address the breach; and
- recommendations to the data subject to mitigate the adverse effects of the breach.

Failure to comply is an offence with fines of up to US$121,951.

Penalties

Under the DPA, the Cayman Islands Ombudsman will be the supervising authority with the power to make:

- information orders;
- enforcement orders; and
- monetary penalty orders.

Failure to comply is an offence with liability upon conviction to a fine of US$121,951 and/or imprisonment for a term of 5 years. Additionally, a monetary penalty order of up to US$304,878 may be issued if there has been a serious contravention of the DPA which is likely to cause substantial distress or damage. It is a defence to prove due diligence was exercised. The data controller may also seek judicial review within 45 days.

Transfers of data

Under the eighth data protection principle, personal data may only be transferred to jurisdictions with equivalent protection. There are exceptions to this rule where the transfer is:

- made with **consent**;
- made for a **contract** with the data subject or a third party contract in the interest of the data subject;
- necessary for reasons of substantial **public interest**;
- for **legal proceedings**, legal advice or establishing, exercising or defending legal rights;
- to protect the **vital interests** of the data subject;
- part of **public register**;
- **approved by the Ombudsman**; or
- required under **international cooperation arrangements**.

Contacts

A list of contacts specialising in Cayman Islands data protection law can be found here.