Marbury Client and Friend Memo
27 September 2019

Cayman Islands

Data Protection in the Cayman Islands

On 30 September 2019, the Cayman Islands Data Protection Law (**DPL**) comes into force, introducing globally recognised standards regarding the protection, processing, and access to, an individual's personal data.

The DPL applies to 'data controllers' established in the Cayman Islands, regardless of whether they have a physical presence in Cayman. Where a data controller engages a third party 'data processor' to process personal data on its behalf, the data controller must ensure that the third-party service provider also complies with the DPL's eight data protection principles:

1. Fair and lawful processing
2. Purpose limitation
3. Data minimisation
4. Data accuracy
5. Storage limitation
6. Respect for the individual's rights
7. Security – integrity and confidentiality
8. International transfers

The DPL introduces a system to protect against the misuse of personal data and a framework whereby individuals can also control their personal data.

Key terms and definitions under the DPL

The DPL applies if you are a Cayman Islands company or partnership, foreign company registered in the Cayman Islands, or a Cayman Islands business or organisation that processes personal data, either directly as a 'data controller' or through the engagement of a 'data processor':

Marbury
Wilson House 1001-2, 19 Wyndham Street, Central, Hong Kong
t +852 2110 0848 | info@marburys.com | www.marburys.com

- 'data controller' "means the person who, alone or jointly with others, determines the purposes, conditions and manner in which any personal data are, or are to be, processed and includes a local representative" within the Cayman Islands.

- 'data processor' "means any person who processes personal data on behalf of a data controller but, for the avoidance of doubt, does not include an employee of the data controller".

The DPL applies to individuals regardless of their nationality or citizenship if their personal data is being processed on behalf of a Cayman Islands data controller. Personal data is any type of data that can be used to identify an individual (the 'data subject').

Does this affect me? Key definitions in context:

To comply with applicable legal, tax or regulatory obligations, including those that derive from anti-money laundering (AML) and counter-terrorism legislation, a Cayman Islands established entity without a physical presence in Cayman would appoint a third-party service provider.

For example, a data controller such as a Cayman Islands-domiciled fund engages a third party to provide the registered office (RO)/fund administration services to liaise with relevant Cayman Islands authorities from within the Cayman Islands, such as making filings with the Cayman Islands Monetary Authority (CIMA) through their online portal REEFS (which is limited to local Cayman Islands service providers). In this case, the fund and the service provider are joint data controllers, with the RO/fund administrator processing the information within the Cayman Islands, for example filing the personal data information of the fund's AML officers, who are also not based in the Cayman Islands.

Obligations under the DPL

Data controllers

Under the DPL, as a data controller, you must:

- specify in your privacy notice the purpose or purposes for processing personal data of clients and employees.

- consider whether you need a separate data protection policy that includes your stated purposes for processing and retaining any personal data in compliance with DPL requirements, including the validation process for any information held about data subjects.

- if engaging a data processor, perform an audit to ensure they can provide sufficient guarantees about their technical and organisational security measures and put in place a written contract (a 'data processing agreement') that stipulates that the data processor acts only on instructions from yourself (the data controller). Furthermore, they must undertake the same security measures that you would have to take if you were doing the processing yourself, especially where an international transfer of data is involved.

Data processors

A data processor must only act on the documented instructions of the data controller. If a data processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a data controller and will have the same liability as a data controller.

The data processor also has the following direct responsibilities:

- not to use a sub-processor without the prior written authorisation of the data controller

- to co-operate with the Office of the Ombudsman, the Cayman Islands' supervisory authority for data protection
- to ensure the security of its processing
- to document their processing activities
- to notify any personal data breaches to the data controller without delay.

If a data processor fails to meet any of these obligations or acts outside or against the instructions of the data controller, then it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

Offences and penalties under the DPL

Monetary penalties of up to CI$100,000 (USD122,000) may be imposed on the data controller for breaching the DPL or a term of imprisonment of up to four years for a director, manager, secretary or other company officer found guilty of an offence under the DPL. In serious cases where the contravention was likely to cause substantial damage or distress to the data subject(s) the penalty could reach CI$250,000 (USD305,000).

Next steps

With much at stake reputationally, Cayman Islands entities are advised to ensure that their data protection provisions are adequate and up to date.

The Cayman Islands' Office of the Obudsman has issued a comprehensive guide on the practical application of the DPL which is available here. Should you have any queries or require any assistance regarding your position with regards to the DPL, please contact your usual Marbury team member or compliance@marburys.com.

Please also take this opportunity to review Marbury's revised privacy policy.