Implications of the Cayman Islands Data Protection Law for Investment Funds

Overview

The Data Protection Law, 2017 (the "**Law**"), currently scheduled to come into force on 30 September 2019, introduces, for the first time in the Cayman Islands, a legislative framework for data protection based on a set of internationally recognised privacy principles. The Law regulates the processing of all personal data in the Cayman Islands and will impact all entities established in the Cayman Islands, including all investment funds whether or not registered with the Cayman Islands Monetary Authority. The Law applies irrespective of where personal data is processed and applies to personal data irrespective of individual citizenship or residency.

This note focuses on the specific effect of the Law on investment funds.

With 30 September on the horizon, Cayman Islands funds should take the necessary steps to ensure that they understand their obligations under the Law and establish policies and procedures to provide adequate protection for all personal data under their control.

Impact on Cayman Islands Funds

Under the Law, any entity established in the Cayman Islands that, as a data controller, processes, either directly or indirectly, any individual's personal data will have certain duties with respect to that data and must ensure that such individuals are notified of their identity and for what purpose any of their personal data is used. An "individual" means a living person and, as such, would include an individual serving as director of a corporate investor in a Cayman Islands fund, but not the corporate investor itself.

For the purposes of the Law, a Cayman Islands fund will generally be regarded as a "**data controller**" which is defined as a "person who, alone or jointly with others determines the purposes, conditions and manner in which any personal data are, or are to be, processed". As a data controller, a fund is not only responsible for ensuring that it processes personal data in accordance with the Law, but is also responsible for ensuring that any entity or service provider which processes data on the fund's behalf (a "**data processor**"), complies with the Law. This is particularly important where a data processor operates under the processing instructions and standards of a fund and a data breach occurs – data security requirements under the Law in this context only extend liability to data controllers.

Data Processors

The fund administrator, or registrar and transfer agent, will, in some circumstances, be a data processor (and in other circumstances, be a data controller where it processes personal data, such as know your client information, for its own purposes) as it receives the subscription agreement and supplemental documents which include know your client, FATCA, and other personal data. An investment manager or advisor who reviews fund information related to individuals will also be a data processor for the purposes of the Law.

Data processors may process personal data which the relevant data controller has entrusted to them only in accordance with the data controller's instructions and the terms of a written agreement (a "**data processing agreement**" or "**DPA**"), which forms the basis of a third party service provider's appointment as a data processor. The DPA may take the form of an amendment to an existing service agreement between the fund and the service provider or a stand-alone agreement. A DPA typically sets out data protection responsibilities (e.g. the fund is a data controller and the investment manager is the data processor), processing limitations (e.g. only on the basis of documented instructions from the fund), and requires the data processor to comply with the data protection principles (e.g. that data is kept secure and not transferred to a jurisdiction that does not ensure an adequate level of protection for the rights of data subjects).

A data processor may have already contractually agreed to comply with data protection requirements of another jurisdiction and, if so, the fund's board may consider whether this provides adequate protection under the Law.

Documenting the Law for Funds

A fund should:

1. Have a privacy notice for investors and subscribers (an outward-facing document).
2. Amend any offering memorandum to reference its obligations under the Law.
3. Amend any documentation with third parties who may be handling personal data provided to them by the fund to ensure that they, as data processors, will process personal data in accordance with the Law (e.g. the investment management agreement and administration agreement).
4. Document and put in place the necessary internal procedures to ensure that it will comply with the Law going forward.
5. Pass any corporate resolutions necessary in connection with 1-4 above.

These are each considered in more detail below.

Privacy Notice

A privacy notice enables a fund to comply with the requirement that data subjects (investors) are entitled to be informed of the identity of the data controller and the purposes for which their personal data are processed. Best practice is to provide additional information such as the legal bases on which data is processed, categories of data obtained, source of the data, the recipients or categories of recipients of the data, details of any international

transfers (i.e. transfers outside the Cayman Islands), the retention period of the data, the rights available to individuals (including the right to make a complaint to the Ombudsman), and (if applicable) the details of any automated decision making. This would be inserted in a fund's subscription agreement, but should also be available as a standalone document to existing investors. At a minimum, a privacy notice should be put in place in advance of 1 October 2019.

Offering Memorandum

The offering memorandum should be amended to include a brief description of the Law, investor personal data rights, and lawful purposes for processing. If the fund is not actively offering interests, this step may be undertaken at a later date to include provisions related to data protection.

Third Party Service Providers Handling Personal Data Provided by the Fund

Data processing agreements with third party service providers (data processors), such as the administrator and investment manager, should be amended to explicitly provide for respective obligations under the Law as well as liability for breach of these obligations. Funds should check their administration agreements and investment management agreements to determine whether such agreements contain adequate obligations to comply with the Law or similar measures. In the event that a DPA is absent, this should be added as a matter of course.

Internal Procedures

A fund's internal cornerstone data protection procedures should include: a data protection policy which mirrors its privacy notice and details regarding how personal data is obtained, stored, protected, and processed; a data retention policy and data retention schedule to outline storage and destruction protocols; a data subject access request procedure for appropriate and compliant responses to data subject queries and complaints; and a data incident response plan which includes responsibilities, measures, and reporting obligations in the event of a data breach.

GDPR

The European Union's General Data Protection Regulation (*(EU) 2016/679*) ("**GDPR**") establishes a regulatory framework for the protection of personal data in European Economic Area (EEA) countries. Compliance with the GDPR equates to compliance with the Law in broad terms but there are additional obligations under the Law (e.g. the requirement to notify the Ombudsman in the event of a reportable breach within 5 days). If the fund or investment manager comply with another adequate national data protection standard such compliance may also suffice for the purposes of the Law, but advice in this regard should be sought.

Timing

Every affected fund and investment manager should have a privacy notice in place as soon as possible; ideally when the Law is currently scheduled to come into force on 30 September 2019. Diligent efforts to put in place additional required data protection documentation and procedures should be made following the Law's inception, recognising that, in practice, requests for information by data subjects are unlikely and other requirements such

as implementing a document retention policy can be developed over a period of time.

Further Information

For further information please reach out to your usual Campbells contact or email us on dataprotection@campbellslegal.com.