LEGAL ALERT

Cayman Islands' Data Protection Law comes into force on 30 September 2019

The Cayman Islands Data Protection Law, 2017 ("**DPL**") which will regulate the future processing of all personal data in the Cayman Islands or by any entity established in the Cayman Islands will come into effect on 30 September 2019[1]. Cayman Islands' entities that handle any individual's personal information will have certain obligations with respect to that information, including ensuring that any such individual is formally notified as to what any of their personal data is being used for, and by whom. The DPL will have significant implications for investment funds, investment managers and fund administrators, either based in the Cayman Islands or dealing with personal data collected or processed by Cayman Islands entities.

As part of the subscription process in a Cayman Islands investment fund, investors are required to provide a government-issued photo ID, information relating to source of funds and wealth, contact details, payment details, and tax residence information, and sometimes certain additional information about employment, dependents, income and investment objectives (the "**Investor Personal Data**"), which are processed and stored by or on behalf of the investment fund (the "**Fund**") and/or by one or more of the service providers to the Fund. Some of the processing may be done in various jurisdictions.

Generally, the Fund, the administrator of the Fund, any transfer agent or distributor, and the investment manager of a Fund may fall within the definition of a Data Controller or Data Processor under the DPL. For purposes of ensuring compliance, the distinction between a Data Controller and a Data Processor is important, since there is no specific liability under the DPL for Data Processors. Data Controllers will instead be held liable for how the Investor Personal Data is processed.

The Fund's Board of Directors should review the contractual arrangements with the Data Processors and update them as needed to ensure compliance with the DPL; based on the number of investors in the Fund, a Data Protection Officer may need to be appointed, although this is not a formal requirement under the DPL. The Fund's Board of Directors may also request that the current administrator and investment manager of the Fund, if they are not based in the Cayman Islands, document and confirm compliance with the DPL or a similar data protection legislation.

As a reminder, the Board of Directors of the Fund is required to supervise third party service providers and ensure that there are sufficient measures in place to protect Investor Personal Data. Privacy Notices in the Fund's offering documents and in the subscription application should be updated to ensure that investors are fully aware of where their Personal Data is being processed, by whom, and for what purpose.

Main Provisions of the Data Protection Law[2]

Personal Data Any information relating to an individual who can be identified, directly

	or indirectly, from that data (including online identifiers such as IP addresses and cookies may qualify as personal data if they are capable of being linked back to the individual).
Data Controller	A Data Controller is 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. The DPL applies to any Data Controller if (a) the Data Controller is established in the Cayman Islands[3] and the personal data are processed in the context of that establishment; or (b) the Data Controller is not established in the Cayman Islands but the personal data are processed in the Cayman Islands otherwise than for the purposes of transit[4]. In this case, Art. 6(2) of the DPL requires the appointment of a local representative which shall be considered a Data Controller.
Privacy Notice	At the time of collection of the data, individuals must be informed of the purposes and details behind the processing, the details of transfers of data and any security and technical safeguards in place. This information is generally provided in a separate privacy notice.
Right to Access	Individuals have the right to obtain confirmation that their Personal Data is processed and to have access to it. Data Controllers must respond within a month of the access request. The DPL permits a reasonable fee to be charged in certain cases.
Retention Period	If there is no compelling reason for a Data Controller to retain Personal Data, a data subject can request its secure deletion.
Right to Erase	Should the individual subsequently wish to have his/her data removed and the Personal Data is no longer required for the reasons for which it was collected, then it must be erased. Data Controllers must notify third party processors or sub-contractors of such requests.
Transfers	International transfers of Personal Data are permitted to third party processors or between members of the same group.
Data Security	Appropriate technical and organisational measures must be taken to prevent unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data[5].
Data Processors	A Data Processor is any person who processes Personal Data on behalf of a Data Controller (but does not include the employees of the Data Controller). There is no liability for processors under the DPL. However, they may be held liable based on contract or tort law.
Data Breach	In the event of a Personal Data breach, the Data Controller must, "without undue delay" but no longer than five (5) days after the Data Controller should have been aware of that breach, notify the Cayman Ombudsman and any affected individuals[6].

Breach Notice	The notification should describe the nature of the breach, its consequences, the measures proposed or taken by the Data Controller to address the breach, and the measures recommended by the Data Controller to the individual concerned to mitigate the possible adverse effects of the breach.
Right to be Forgotten	The DPL contains a similar right, although this is expressed as a general right of "erasure". Under the UK's Data Protection Act, the right is limited to processing that causes unwarranted and substantial damage or distress. Under the DPL this threshold is not present. If there is no compelling reason for a Data Controller to retain Personal Data, a data subject can request its secure deletion.
Right to Object	An individual has the right at any time to require a Data Controller to stop processing his/her Personal Data for the purposes of direct marketing. There are no exemptions or grounds to refuse. A Data Controller must deal with an objection to processing for direct marketing at any time and free of charge.
Direct Marketing and Consent	Including an unsubscribe facility in each marketing communication is recommended best practice. If an individual continues to accept the services of the Data Controller without objection, consent can be implied.
Data Processors	Best practice would always be to put in place a contract between a controller and processor. Essentially, the contract should require the Data Processor to level-up its policies and procedures for handling personal data to ensure compliance with the DPL. Use of sub-contractors by the service provider should be prohibited without the prior approval of the Data Controller[7].
Data Protection Officer	The DPL does not require the appointment of a Data Protection Officer, although this is recommended best practice.
Penalties	Refusal to comply or failure to comply with an order issued by the Cayman Ombudsman is an offence. Penalties are also included for unlawful obtaining or disclosing Personal Data[8]. Directors may be held liable under certain conditions[9]. The Data Controller is liable on conviction to a fine up to CI$100,000 (circa US$122,000) or imprisonment for a term of 5 years or both. Monetary penalty orders of an amount up to CI$250,000 (circa US$304,878) may also be issued against a Data Controller.

If you would like to discuss the application of the DPL to your particular Cayman Islands entity, please contact your usual Loeb Smith attorney or any of:

E: gary.smith@loebsmith.com
E: ramona.tudorancea@loebsmith.com
E: vivian.huang@loebsmith.com
E: yun.sheng@loebsmith.com
E: elizabeth.kenny@loebsmith.com
E: santiago.carvajal@loebsmith.com

---

1 The Data Protection Law, 2017 (Commencement) Order, 2019
2 This is not a comprehensive analysis of the DPL.
3 Other than residents, fall under this category companies incorporated or registered as a foreign company in the Cayman Islands, partnerships and associations formed in the Cayman Islands, as well as any persons who maintain in the Cayman Islands an office, branch or agency, or a regular practice.
4 See Art. 6 of DPL
5 See Schedule 1 of DPL
6 See Art. 16 of DPL
7 Under DPL, the Data Controller is liable for breaches and non-compliance, whereas processors may not be. It is therefore very important for a Fund's Board of Directors to ensure that adequate contractual protections are in place.
8 See Arts. 53-54 of DPL
9 See Art. 58 of DPL