Hedge Fund Law Report
An Acuris company

HFLR.com

September 12, 2019

PRIVACY

How Fund Managers Should Prepare for the Cayman Islands Data Protection Law

By Sailaja Alla, Peter Colegate and David Lee, *Appleby*

The Cayman Islands Data Protection Law, 2017 (DPL) comes into force on 30 September 2019 and will regulate the future processing of all personal data in the Cayman Islands. Drafted around a set of internationally recognised privacy principles, the new law provides a framework of rights and duties designed to give individuals greater control over their personal data. The DPL joins the Confidential Information Disclosure Law, 2016 and common law obligations of confidentiality to give the Cayman Islands the most comprehensive data protection regime in the region.

With the implementation date less than a month away, managers of Cayman funds that have not already done so should take steps to ensure that they understand their funds' obligations under the new law. This will include having in place policies and procedures to ensure the proper protection of all personal data under their control, as well as creating an effective governance regime for approving, overseeing, implementing and reviewing those policies. Cayman funds must get it right – reputations and criminal liability will soon be at stake.

This article reviews the key provisions of the DPL and how Cayman funds can achieve compliance with it.

See "How Fund Managers Can Navigate the E.U. General Data Protection Regulation and the Cayman Islands Data Protection Law" (Aug. 9, 2018).

Effect on the Funds Industry

"Personal data" is defined widely under the law to include any data relating to a living individual. Therefore, the average fund potentially generates and retains a large amount of personal data. Fund managers hold proprietary and personal information about markets, companies and individuals, including high-value email and contact lists and net worth information.

Under the DPL, personal data held by a fund must be processed fairly and lawfully and used for a legitimate purpose that has been notified to the data subject in advance. Personal data holdings should not be excessive in relation to the purposes for which they are collected and should be securely purged once those purposes have been fulfilled. If personal data is processed for any new purposes, this processing can only be undertaken if there is a legitimate purpose for doing so and if the data subject has been notified.

While it is unlikely that a fund manager will use personal data other than for the purposes of processing an investment and meeting legitimate reporting and record keeping obligations, funds must set out both the purposes for which personal data is being collected and details regarding with whom that data may be shared. The fund should disclose this information in a separate privacy notice, which can be provided with the fund's offering memorandum and subscription documents.

Transferring Data to Third Parties

Fund managers' operational, trading and back-office functions are now mostly digitised and delegated to external service providers. In an age where highly sensitive information can be exchanged at the touch of a button, data-protection issues must be considered before any transfers of personal data are made to third parties.

Fund managers must, therefore, conduct proper due diligence on the systems, policies and procedures of those third-party service providers to ensure that personal data is handled appropriately and securely. In addition, it is advisable for each manager to conduct regular physical audits and independent testing of a service provider's controls.

Contractual provisions should be put in place between the fund (as the data controller) and the third-party service provider (as the data processor) to ensure that any personal data is processed only for authorised purposes; that all data is stored and transmitted securely; and that disaster-recovery practices are in place in the event of a data breach. Use of subcontractors by the service provider should be prohibited without the prior approval of the fund.

For more on how fund managers can diligence and contract with third parties, see "How Fund Managers Can Mitigate the Risks of Open-Source Software" (Mar. 7, 2019); "What Fund Managers Should Consider When Negotiating SaaS Agreements" (Dec. 20, 2018); and "Key Considerations for Fund Managers When Selecting and Negotiating With a Cloud Service Provider" (Sep. 21, 2017).

Achieving Compliance

The DPL gives individuals the right to access personal data held about them and to request that any inaccurate data be corrected or deleted. Funds will need to implement policies and procedures to manage these requests.

The law also obliges businesses to cease processing personal data once the purposes for which that data has been collected have been exhausted. Prescribed data-retention periods are not set out in the DPL, but an analysis will need to be undertaken to determine how long data should be kept for. Similarly, it will be important to evaluate how personal data can be securely deleted once the purposes for holding it have been fulfilled.

See "Will Inadequate Policies and Procedures Be the Next Major Focus for SEC Enforcement Actions?" (Nov. 30, 2017).

The Office of the Ombudsman will have responsibility for enforcing the new law and has issued a Guide for Data Controllers to assist organisations with the implementation process. Breaches of the DPL could result in fines of up to CI$100,000 per breach,

imprisonment for a term of up to five years or both. Other monetary penalties of up to CI$250,000 are also possible under the law.

In addition to the enforcement powers of the Ombudsman, the DPL provides that any person who suffers damage as a result of a data controller's breach may bring a civil claim for compensation. This means that a DPL breach could be used either as a standalone claim or as part of a litigation strategy to support a wider claim against a fund.

Implementing a new data protection compliance programme to take account of the DPL or incorporating the requirements of the DPL into an existing programme will involve ensuring that there is an effective governance regime for approving, overseeing, implementing and reviewing data-protection policies and procedures. Although the appointment of a Data Protection Officer is not mandatory under the DPL, funds are recommended to do so to ensure a coordinated chain of command and proper compliance.

Protecting personal data is increasingly business-critical for funds. Even if monetary losses are not sustained as a result of personal data being mishandled, the reputational damage to a fund following a breach could be devastating.

Sailaja Alla is a corporate partner in Appleby's Cayman office. She has extensive experience advising clients on all aspects of the formation, operation, restructuring and termination of all types of Cayman Islands investment funds. She also advises on Cayman regulatory and licensing issues in relation to these funds and has experience in a wide range of general corporate matters.

Peter Colegate is counsel and co-head of Appleby's global technology and innovation group, and he is based in the Cayman Islands. His practice is focused on privacy; data protection; and strategic corporate-commercial and regulatory work in the technology and innovation sectors.

David Lee is a litigation partner in Appleby's dispute resolution practice group in the Cayman Islands. Lee is a leading member of Appleby's fund disputes team advising both investors and financial institutions in some of the largest and most complex fund disputes. He joined Appleby from a global law firm where he was a partner in both its London and Hong Kong offices and led its fund disputes practice.