GDPR and the Cayman Islands' Data Protection Act, 2021 – a comparison

The EU's General Data Protection Regulation ("**GDPR**") applies to offshore investment funds with European investors. The Cayman Islands Data Protection Act, 2021 ("**DPA**"), regulates the processing of all personal data. Inspired by the UK's Data Protection Act, the DPA includes provisions very similar to GDPR (together "**Data Protection Laws**"), with certain notable differences.

Even though the DPA applies generally to the processing of personal data and not just to investment funds, within this context and as part of the subscription process, investors are required to provide a government-issued photo ID, source of funds and wealth, contact details, payment details, and tax residence information, or even 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 by different parties in various jurisdictions.

Within the context of investment funds, the Administrator, Transfer Agent, Distributor, and the Investment Manager of a Fund may fall within the definition of a Data Controller or Data Processor. To ensure compliance with GDPR and/or DPA, the Fund's Board of Directors should review the contractual arrangements with these parties and may need to appoint a Data Protection Officer. 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 would need to be updated to ensure that investors are fully aware of where their Personal Data is being processed, by whom and for what purpose.

For ease of reference, a brief comparison between GDPR and the DPA is included below[i].

Comparison of the Main Provisions

	GDPR	DPA
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).	Same as GDPR.

	GDPR	DPA
Data Controller	The person who, alone or with others, determines the purposes, conditions and means of the processing of Personal Data.	DPA applies to any Data Controller in respect of Personal Data (a) established and processed in the Cayman Islands; or (b) processed in the Cayman Islands otherwise than for the purposes of transit[ii].
Privacy Notice	At the time of collection of the data, individuals must be informed of the purposes and detail 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.	Same as GDPR.
Right to Access	Individuals have the right to obtain confirmation that their Personal Data is processed and to access it. Data Controllers must respond within a month of the access request. A copy of the information must be provided free of charge.	Same as GDPR, but the DPA permits a reasonable fee to be charged.
Retention Period	Personal data should not be kept for longer than is necessary to fulfil the purpose for which it was originally collected. Controllers must inform data subjects of the period of time (or reasons why) data will be retained on collection.	Not a requirement under DPA. However, as with the GDPR, 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 their 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.	Same as GDPR.
Transfers	International transfers permitted to third party processors or between members of the same group.	Same as GDPR.
Data Security	Minimum security measures are prescribed as pseudonymisation and encryption, ability to restore the availability and access to data, regularly testing, assessing and evaluating security measures.	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[iii].
Data Processors	Security requirements are extended to data processors as well as Data Controllers.	There is no liability for processors under the DPA. However, they may

	GDPR	DPA
		be held liable based on contract or tort law.
Data Breach	Data Controllers must notify the regulatory authority of Personal Data breaches without undue delay and, where feasible, not later than 72 hours after having become aware of a 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 Ombudsman and any affected individuals[iv].
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.	Same as GDPR.
Right to be Forgotten	An individual may request the deletion or removal of Personal Data where there is no compelling reason for its continued processing.	The DPA 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 DPA this threshold is not present. As with the GDPR, 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 their 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.	Same as GDPR.
Direct Marketing and Consent	The Data Controller must inform individuals of their right to object "at the point of first communication" and in a privacy notice. For any consent to be valid it needs to be obvious what the data is going to be used for at the point of data collection and the Data Controller needs to be able to show clearly how consent was gained and when it was obtained.	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.

	GDPR	DPA
Data Processors	The GDPR sets out more detailed statutory requirements to apply to the controller/processor relationship, and to processors in general. Data Processors are now directly subject to regulation and are prohibited from processing Personal Data except on instructions from the Data Controller.	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 DPA. Use of sub-contractors by the service provider should be prohibited without the prior approval of the Data Controller[v].
Data Protection Officer	Mandatory if the core activities of the Data Controller consist of processing operations which require large scale regular and systematic monitoring of individuals or large scale processing of sensitive Personal Data.	Does not require the appointment, although this is recommended best practice.
Penalties	Two tiers of sanctions, with maximum fines of up to €20 million or 4% of annual worldwide turnover, whichever is greater.	Refusal to comply or failure to comply with an order issued by the Ombudsman is an offence. Penalties are also included for unlawful obtaining or disclosing Personal Data[vi]. Directors may be held liable under certain conditions[vii]. The Data Controller is liable on conviction to a fine up to CI$100,000 (approx.. US$122,000) or imprisonment for a term of 5 years or both. Monetary penalty orders of an amount up to CI$250,000 (US$304,878.05) may also be issued against a Data Controller.

Further Assistance

This publication is not intended to be a substitute for specific legal advice or a legal opinion. If you require further advice relating to the matters discussed in this Briefing, please contact us. We would be delighted to assist.

E: gary.smith@loebsmith.com
E: robert.farrell@loebsmith.com
E: ivy.wong@loebsmith.com
E. elizabeth.kenny@loebsmith.com
E: cesare.bandini@loebsmith.com
E: vivian.huang@loebsmith.com
E: faye.huang@loebsmith.com
E: max.lee@loebsmith.com

About Loeb Smith Attorneys

Loeb Smith is an offshore corporate law firm, with offices in the British Virgin Islands, the Cayman Islands, and Hong Kong, whose Attorneys have an outstanding record of advising on the Cayman Islands' law aspects and BVI law aspects of international corporate, investment, and finance transactions. Our team delivers high quality Partner-led professional legal services at competitive rates and has an excellent track record of advising investment fund managers, in-house counsels, financial institutions, onshore counsels, banks, companies, and private clients to find successful outcomes and solutions to their day-to-day issues and complex, strategic matters.

Investment Funds

Banking & Finance

Insolvency/Restructuring

Mergers & Acquisitions

Capital Markets

Corporate

Private Equity

Corporate & Liquidation

Commercial Litigation

[i] The comp ... may be relevant t ... d is therefore not a comprehen
[ii] See Se
[iii] See Sc
[iv] See Sect
[v] Under DPA ... nes and non-compl ... not be. It is therefore very importan ... nsure that adequate c ... e.
[vi] See Sections
[vii] See Sections 5