DECEMBER 2022

mourant

UPDATE

Cybersecurity and data breaches in the Cayman Islands

Update prepared by Sara Galletly (Cayman) and Morgan Hendrickson (Cayman)

Given the current prevalence of cybersecurity threats, what is the Cayman regulatory position – and are funds and their managers ensuring compliance when a data breach occurs?

Introduction

Cybersecurity threats are on the rise globally, with phishing, ransomware and other cyber-attacks becoming more sophisticated, increasing the risks of loss and leakage of data belonging to or used by individuals, enterprises and organisations. With these heightened risks, we are seeing an increase in regulatory requirements and oversight, such as the cybersecurity disclosure rules to be introduced by the U.S Securities and Exchange Commission.

Against this background, we summarise the Cayman Islands position, including the overlap between cybersecurity and the Cayman Islands data protection regime.

Cayman Islands cybersecurity requirements

Applicable regulatory measures

The Cayman Islands Monetary Authority (CIMA) has issued both a Rule and a Statement of Guidance on Cybersecurity for Regulated Entities.[1] Whilst these regulatory measures do not apply to Cayman Islands mutual funds or private funds, they do apply to apply to licensees or registrants under most other Cayman regulatory laws[2], including investment managers regulated under the Securities Investment Business Act.

The Rule and Statement of Guidance set out CIMA's requirements in relation to the management of cybersecurity risks. Those expectations include the establishment, implementation and maintenance of a documented cybersecurity framework designed to:

- identify, assess, monitor and mitigate cybersecurity risks; and
- respond to, and aid recovery from, cybersecurity breaches that could have a material impact on an entity's operations.

Under the Rule, the governing body[3] of the regulated entity has ultimate responsibility for cybersecurity. Their duties include:

- approving a written cybersecurity risk management strategy and a comprehensive cybersecurity framework (including cybersecurity risk assessments), as well as ensuring appropriate oversight and periodic review of the risk management framework;
- approving a cybersecurity audit plan and ensuring that any findings are addressed appropriately; and

[1] Available here.

[2] Including the Banks and Trust Companies Act, Companies Management Act, Directors Registration and Licensing Act, Insurance Act, Mutual Funds Act (noting that mutual funds are excluded), Private Trust Companies Regulations and the Securities Investment Business Act.

[3] Ie, the board of directors, general partner(s) or other management committee or body.

- ensuring that periodic and formal, independent cybersecurity and cyber resilience reviews/audits of the organisation occur, taking into consideration the size, nature and complexity of the entity.

Notification of cybersecurity incident

An entity which is in-scope of the Rule and Statement of Guidance that becomes aware of a cybersecurity incident deemed to have a material impact on operations, or which has the potential to become a material incident, must report the incident to CIMA in writing within 72 hours following its discovery. Where there is doubt about whether an incident is material, CIMA should be consulted.

Examples of material incidents that should be reported to CIMA include:

- an event resulting in the unauthorised dissemination of personal data;
- loss or exposure of data in violation of any applicable data protection laws or other regulatory requirements, whether foreign or domestic; and
- extended disruptions to critical business systems or internal operations.

In-scope entities must also notify affected persons if a cyberattack has resulted in the breach of non-public information or disrupts a service that is utilised, including the provision of information on actions taken to contain, remedy and recover from the breach.

Overlap with the data protection regime

The data protection regime

The Cayman Islands Data Protection Act (2021 Revision) (the **DPA**) protects 'personal data', which is data relating to a living individual who can be identified. See our GDPR and Data Protection Information Hub for more information on the DPA.

A 'personal data breach' under the DPA occurs when there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A personal data breach under the DPA, therefore, includes a situation where personal data is accessed or obtained via a cybersecurity attack.

The DPA imposes obligations on 'data controllers' which, in summary, are the persons who determine the purposes, conditions and manner in which any personal data are, or are to be, processed. These obligations include notification obligations which are in addition to the notification obligations imposed by the cybersecurity Rule and Statement of Guidance.

Notification obligation - personal data breach

Where a personal data breach occurs, the DPA requires that the data controller must without undue delay and, in any event, within five days after the data controller should have reasonably been aware of that breach, notify the Cayman Islands Ombudsman and the affected data subject(s) of the breach. That notice must provide details of the breach as well as certain other information, including action taken by the data controller and recommended actions to mitigate possible adverse effects.

Cayman Islands funds

Whilst the cybersecurity Rule and Statement of Guidance apply to Cayman Islands managers but not to Cayman Islands funds, the fund vehicles will usually be data controllers for the purposes of the DPA.

Accordingly, if a cybersecurity attack occurs on a fund's onshore service provider (including the administrator, adviser or manager) and results in unlawful access to personal data in respect of which the Cayman Islands fund is the data controller (such as investor information), the Cayman Islands fund will be required to notify the Ombudsman in accordance with the obligation described above. This notification obligation applies regardless of where in the world the cybersecurity attack and its target are located, and regardless of whether the target is the fund itself, its manager or another third party service provider.

Consequences of failure to notify

Failure to comply with this requirement is an offence under the DPA, giving rise to liability on conviction of a fine of US$121,951.

In addition, section 55 of the DPA provides the Ombudsman with the discretion to impose a monetary penalty on a data controller in an amount of up to US$304,878, where the Ombudsman is satisfied on the balance of probabilities that:

- there has been a serious contravention of the DPA by the data controller; and
- the contravention is likely to cause substantial damage or distress to the data subject.

Next steps

For more information, please get in touch with your usual Mourant contact or one of the contacts named below.

Contacts

Sara Galletly
Partner
Mourant Ozannes (Cayman) LLP
+1 345 814 9233
sara.galletly@mourant.com

Alex Last
Partner
Mourant Ozannes (Cayman) LLP
+1 345 814 9243
alex.last@mourant.com

James Broad
Partner
Mourant Ozannes (Hong Kong) LLP
+852 3995 5722
james.broad@mourant.com

Morgan Hendrickson
Associate
Mourant Ozannes (Cayman) LLP
+1 345 814 9193
morgan.hendrickson@mourant.com

[2021934/85250839/1]