

Data breaches in the Cayman Islands

This summary outlines the key considerations for data controllers in the Cayman Islands dealing with a personal data breach.

Identifying a data breach

In accordance with the Cayman Islands Data Protection Act (2021 Revision) (**DPA**), a 'personal data breach' 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 transmitted, stored, or otherwise processed.

Importantly, data breaches can occur accidentally or deliberately. This would therefore include inadvertently sending an email to the wrong recipient or leaving a document on public transport, and deliberate security incidents, such as a hacker gaining access to your inbox.

Reporting a data breach

When a breach has occurred, the data controller (i.e. the person/entity who determines the purpose and way in which the data has been processed) **must notify** the [Ombudsman](#) and the **applicable data subject(s) of the breach**. This notification must be made **without undue delay**, but no longer than five days after the data controller should have reasonably known about the breach.

The notification must contain mandatory information, including:

- The nature of the breach
- The consequences of the breach
- The measures proposed or taken by the data controller to address and contain the breach
- The measures recommended to the data subject(s) to mitigate the possible adverse effects

Failing to report a data breach

In addition to potential enforcement orders and monetary penalties imposed by the Ombudsman, and/or potential complaints from data subjects, a failure to report a data breach is an offence and the data controller may be liable on conviction to a \$100,000 fine.

Preventing data breaches

A central principle of the DPA is that data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and accidental loss, destruction, or damage to personal data. The Ombudsman will therefore expect all controllers to have security measures in place (such as encryption, anti-virus software, internal disciplinary rules etc.) to avoid breaches.

Other factors to consider

- Do other regulatory reports need to be made (e.g. to the Cayman Islands Monetary Authority)?
- Should your insurance providers be notified of the breach?
- If the breach involves criminal activity, has a report been made to the relevant police force?

Key contacts



Juan Pablo Urrutia
+1 345 949 8599
juanpablo.urrutia@harneys.com
Cayman Islands



Charlotte Allery
+1 284 852 4374
charlotte.allery@harneys.com
British Virgin Islands