Key points to consider when handling personal data

April 2023

With news stories of ransomware attacks ever increasing, so too does the potential compromise of personal data held by entities subject to such attacks or other cyber security breaches.

Should such an event occur, it is important to consider your obligations.

An entity is subject to the provisions of the Cayman Islands Data Protection Act (2021 Revision) (**DPA**), pursuant to section 6(1) of the DPA if it is a data controller and:

- the data controller is established in the Cayman Islands; and
- has processed personal data in the Cayman Islands; or
- the data controller is not established in the Cayman Islands but processed personal data in the Cayman Islands otherwise than for the purposes of transit of the personal data through the Cayman Islands.

A data controller is a person/entity who makes decisions about why and how personal data is handled.

In the instance of a ransomware attack or other cyber security breach, a data controller should consider the following key points:

1. What information has been compromised? Is it personal data and/or sensitive personal data?

a. Personal data is data relating to a living individual which can be identified and includes data such as:

i. the individual's location, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the living individual;

ii. an expression of opinion about the living individual; or

iii. any indication of the intentions of the data controller or any other person in respect of the living individual.

b. Sensitive personal data is personal data consisting of:

i. the racial or ethnic origin of the data subject;

ii. the political opinions of the data subject;

iii. the data subject's religious beliefs or other beliefs of a similar nature;

iv. whether the data subject is a member of a trade union;

v. genetic data of the data subject;

vi. the data subject's physical or mental health or condition;

vii. medical data;

viii. the data subject's sex life;

ix. the data subject's commission, or alleged commission, of an offence; or any proceedings for any offence committed, or alleged, to have been committed, by the data subject, the disposal of any such proceedings or any sentence of a court in the Cayman Islands or elsewhere.

2. Is the data controller established in the Cayman Islands?

The data controller would be established in the Cayman Islands if:

a. it is a body incorporated in the Cayman Islands or registered as a foreign company in the Cayman Islands;

b. it has established a partnership or other unincorporated association formed under the law of the Cayman Islands; or

c. it maintains an office, branch, agency or regular practice in the Cayman Islands.

If a data controller is not established in the Cayman Islands but personal data is processed in the Cayman Islands (other than for the purposes of transit of the data through the Cayman Islands), it is required to nominate a local representative established in the Cayman Islands who shall, for all intents and purposes, be the data controller and bear all the obligations under the DPA as if the representative were the data controller.

3. Has the data controller processed personal data in the Cayman Islands other than for the purposes of transit of the personal data through the Cayman Islands?

The definition of processing personal data in the Cayman Islands is very broad under the DPA and includes obtaining, recording or holding data, or carrying out any operation or set of operations on personal data, including:

a. organising, adapting or altering the personal data;

retrieving, consulting or using the personal data;

disclosing the personal data by transmission, dissemination or otherwise making it available; or

aligning, combining, blocking, erasing or destroying the personal data.

It is important to consider where the personal data was collected from the data subjects, was it in the Cayman Islands or elsewhere?

If the personal data was collected elsewhere, the data controller should establish how the personal data was 'processed' in the Cayman Islands in accordance with the definition above.

Examples of processing include: storing IP addresses or MAC addresses; video recording (CCTV); posting or putting a photo of a person on a website or social media; collecting personal data through a website accessed from the Cayman Islands, shredding documents containing personal data; access to or consultation of a database of contacts containing personal data; and staff management and payroll administration.

4. What is a personal data breach?

A personal data breach occurs where there has been a "breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or, access to, personal data transmitted, stored or otherwise processed." Where such breach occurs as a result of a ransomware attack or other cyber security breach, it is likely that there would have been an unauthorised disclosure of personal data regarding the data subjects.

5. What happens if there has been a personal data breach?

If personal data has been compromised and the DPA applies to you as the data controller (i.e. you are established in the Cayman Islands and have processed personal data in the Cayman Islands or you are not established in the Cayman Islands but have processed personal data in the Cayman Islands) then you have an obligation to inform the Ombudsman of the Cayman Islands (**Ombudsman**) and the affected individuals of a data breach without undue delay and no later than 5 days after, with the exercise of due diligence, the data controller became aware of the breach.

6. Report to the Ombudsman

The report to the Ombudsman and data subjects is not required if the breach is unlikely to prejudice the rights and freedoms of the data subjects. The data protection principles contained in Schedule 1 of the DPA should be considered to assess whether the rights and freedoms of the data subjects have been prejudiced. In the instance of a ransomware attack or other cyber security incident the loss of control by the data subjects over their personal data is likely to prejudice the rights and freedoms of the data subjects as they no longer know who has access to their personal data, cannot contact such person or entity and therefore have their personal data deleted in accordance with the right to be forgotten.

Notification of the data breach can be made electronically via this form.

As part of the notification to the Ombudsman, if more information is required regarding the data breach and/or the data subjects to understand the extent of the breach and potential harm to the data subjects, the entity has an ongoing obligation to conduct due diligence. An explanation of the steps taken by the data controller should be disclosed in the notification to the Ombudsman, the reason for any delay in obtaining information and the timescale for providing additional information to the Ombudsman.

7. Failure to Notify

Failure to notify the data breach when required to do is an offence under the DPA and can result in a conviction and fine of $100,000. Failure to notify may also be subject to a monetary penalty imposed by the Ombudsman depending on the severity of the contravention of the DPA and whether substantial damage or distress has been caused to the data subject up to a maximum of $250,000.

If you require any advice regarding a potential data breach or your obligations regarding the DPA, please get in touch with key contacts Natalie Bell or Laura Oseland.

For more information please contact:

Chantelle Day

Partner // Cayman

t:+1 345 914 9623 // *e:*chantelle.day@collascrill.com