CONYERS

Article

February 2023 | Cayman Islands

Privacy and Data Breaches in the Cayman Islands

Author: Róisín Liddy-Murphy, Counsel

Since the introduction of the Data Protection Act (the "DPA") in 2019, there has been a steady increase in the number of data protection breaches that have been reported to the Office of the Ombudsman.[1] It is expected that this increase is set to continue considering the number of businesses that record personal information in respect of individuals, particularly those of employees and clients in conjunction with the greater awareness and concern over individual's privacy rights. In this regard, it is important for Cayman Islands entities that process personal data to be aware of their obligations under the DPA and are in a position to recognise and adequately respond to a privacy breach or notifications that occur.

Application of the DPA

The first step in ascertaining as to whether or not the DPA is applicable to a Cayman entity is to establish if the entity is a data controller or a data processor.

- A "*data controller*" is the person who alone or jointly with others determines the purposes, conditions and manner in which any personal data are, or are to be, processed.
- A "*person*" includes any corporation, either aggregate or sole, and any club, society, association, public authority or other body, of one or more persons.
- A "*data processor*" is any person that processes personal data on behalf of a data controller but does not include an employee of the data controller.
- The term "*personal data*" means data relating to an identifiable living individual referred to as a "*data subject*". The data subject does not need to be in the Cayman Islands.
- The term "*processing*", in relation to data, means obtaining, recording or holding data or carrying out any operation or set of operations on personal data.
- The term "*personal data breach*" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to, personal data transmitted, stored or otherwise processed.

The DPA defines "personal data" very widely and it is the data controller that is responsible for ensuring that the eight data protection principles are complied with when processing personal information.

Data Protection Principles

The eight data protection principles set out a framework within which personal data is processed.

- Fair and lawful use processing
- Purpose limitation
- Data minimisation
- Data accuracy
- Storage limitations

[1] The Ombudsman is responsible for ensuring the successful functioning of the DPA.The Ombudsman 2020 Annual Report published 14 July 2021, available at https://ombudsman.ky/images/pdf/Office_of_the_Ombudsman_2020_Annual_Report.pdf

- Respect for individual's rights
- Security, integrity and confidentiality
- International transfers

Personal Data Breaches

A personal data breach can be broadly defined as a security incident that affects the confidentiality, integrity or availability of personal data. Breaches can be the result of both accidental and deliberate causes and are not solely centered on the loss of personal data.

They can include unlawful access of personal data by an unauthorised person, deliberate or accidental action (or inaction) by the data controller or data processor, sending personal data to an incorrect recipient, alteration of personal data without permissions and loss of the availability of personal data. Under the DPA, a data breach arises whenever any personal data is lost, destroyed, corrupted or disclosed, if someone accesses the data or passes it on without proper authorisation, or if the data is made unavailable, for example when it has been encrypted by ransomware or accidently lost or destroyed due to a malfunction of the storage medium.

Notification Requirements

A personal data breach must be reported to the Ombudsman and to the individual(s) concerned without undue delay but not later than 5 days after you should, with the exercise of due diligence, have been aware of the breach.

The Ombudsman expects all data breaches to be reported to the Ombudsman and to the individual(s) whose data was breached, unless the breach is unlikely to prejudice the rights and freedoms of the affected data subjects.

In terms of enforcement orders, a personal data breach may not by itself lead to enforcement action by the Ombudsman. The Ombudsman will examine the circumstances of the breach and will determine whether an investigation will be launched. Failing to notifying the Ombudsman or the individual of any security incident may cause additional damages to the individual whose data has been breached and result in damage to an entity's business reputation if an enforcement order issued. It further gives rise to an offence under the DPA and can result in a conviction or a fine of one hundred thousand dollars. Depending on the facts of the matter, it may also be the subject of a monetary penalty imposed by the Ombudsman under section 55 of the DPA.

Penalties

The DPA allows for the imposition of various fines not exceeding $250,000 and/or imprisonment not exceeding five years for specified contraventions under the DPA.

Cayman Enforcement Orders

There have been a number of published enforcement orders in the Cayman Islands that record the conclusions of investigations by the Ombudsman into DPA breaches.[2]

On 7 August 2020, an enforcement order was published whereby the complainant asserted that the Register of Companies ("Registrar") did not have a legal basis to process certain personal data requested on the Registrar platform relating to non-registrable persons. The Ombudsman upheld that it was unnecessary for the Registrar to request and process this information.[3] It was established that the Registrar had not established a satisfactory legal basis for its blanket approach to gathering and processing of personal data of non-registrable persons. The Registrar was required to take a number of steps to ensure compliance going forward with the DPA as per the terms of the enforcement order.[4]

Two subsequent enforcement orders were released on 18 March 2021, the first one concerned Jacques Scott Group ("JSG") who suffered a ransomware attack that affected various types of personal data of some 150 data subjects, including employees, shareholders and pension account members. The Ombudsman found the JSG had violated the seventh data protection principle which requires data controllers to ensure that adequate technical and organizational measures are taken against unauthorized or unlawful processing. The Ombudsman proceeded to issue an enforcement order against JSG setting out a number of recommendations.[5]

Also on 18 March 2021, an enforcement order resulting in a number of recommendations was issued against St. Ignatius Catholic School on the basis that the school did not have an appropriate legal basis for the processing of certain employee personal data.[6]

---

[2] Each of the five above enforcement orders published arise under section 43 of the DPA, whereby a complaint may be made to the Ombudsman by or on behalf of any person about the processing of personal data that has not been or is not being carried out in compliance with the provision of the DPA. Outside of the published enforcement orders, there has been a number of informal resolutions. See the Ombudsman 2020 Annual Report published 14 July 2021 pages 26-39 for some of the case summaries of the informal resolutions, available at https://ombudsman.ky/images/pdf/Office_of_the_Ombudsman_2020_Annual_Report.pdf

[3] Whether processing personal data is considered necessary will depend on an assessment of the objective pursued and whether it is the less intrusive than other options. See the European Data Protection Supervisor, Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit, 11 April 2017, p.5 available at https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en.

[4] https://ombo.bbandp.com//images/pdf/decisions/dp_decisions/DP_Case_202000507.pdf

[5] https://ombo.bbandp.com//images/pdf/DP_Enforcement_Order_201900212_-_Exec_Summary.pdf

[6] https://ombo.bbandp.com//images/pdf/DP_Enforcement_Order_202000820_-_Exec_Summary_Final.pdf

On 12 July 2021, an enforcement order was published against the Department of Agriculture ("DoA").[7] The complainant claimed that the DoA was unnecessarily collecting personal data from individuals who were purchasing retail goods such as plants and trees. In issuing a number of recommendations the Ombudsman determined that the DoA was processing personal data of retail customers unfairly and without legal basis, in contravention of the first data protection principle.

On 22 September 2021, an enforcement order was published against Foster's Supermarket ("Fosters).[8] The complainant applied for a job at Fosters but was not shortlisted for interview. He was told that this was a result of concerns raised during reference checks. He submitted a subject access request under the DPA seeking copies of all information held in relation to his job application, including correspondence with his previous employers. The information supplied to the applicant contained several redactions, mainly of the names of Fosters' staff and individuals from other companies who had supplied references. The Ombudsman investigated the matter and agreed with the complainant that the redactions were not necessary. The Ombudsman referred to the UK Information Commissioners' Office guidance on the factors to consider when balancing the data subject's right to know the source of the information that is held about them against the right to privacy of the third party who can be identified from the information.[9] The Ombudsman published an enforcement order against Fosters issuing a number of recommendations pursuant to section 45(1) of the DPA, which included the full (without redactions) disclosure of the information sought.

So far, there have been no published enforcement orders resulting in a monetary penalty. Notwithstanding this, the Ombudsman investigations (which can include extensive information orders being issued as part of the investigations) and recommendations can be onerous on a data controller and can result in significant reputational damage.

Section 47 of the DPA provide a person who receives an enforcement order under the DPA with the option to judicial review order to the Grand Court within 45 days of receipt and upon notice to the Ombudsman.

Conclusion

The DPA applies to every Cayman entity that processes and controls personal information. The DPA will affect any individual or organisation established in Cayman which processes personal data, even where the data is being processed outside of Cayman. It is important that organisations identify the personal data that it holds and work towards ensuring that they are operating in compliance with the provisions set out in the DPA.

The measures taken by an organisation to ensure compliance with the DPA before and after a breach or investigation occurs become crucial factors that weigh heavily on the Ombudsman determinations.

Conyers has advised a number of leading managers across a broad spectrum of industries on compliance and DPA related matters in conjunction with advising and representing clients on various privacy and data breaches.

Author:

Róisín Liddy-Murphy
Counsel
roisin.liddy-murphy@conyers.com
+1 345 814 7371

[7] https://ombo.bbandp.com//images/pdf/decisions/dp_decisions/DP_Enforcement_Order_DoA_202000892.pdf
[8] https://ombudsman.ky//images/pdf/decisions/dp_decisions/DP_Case_202100204_Fosters_Decision.pdf
[9] https://ico.org.uk/media/for-organisations/documents/1066/employment_practice_code_supplementary_guidance.pdf