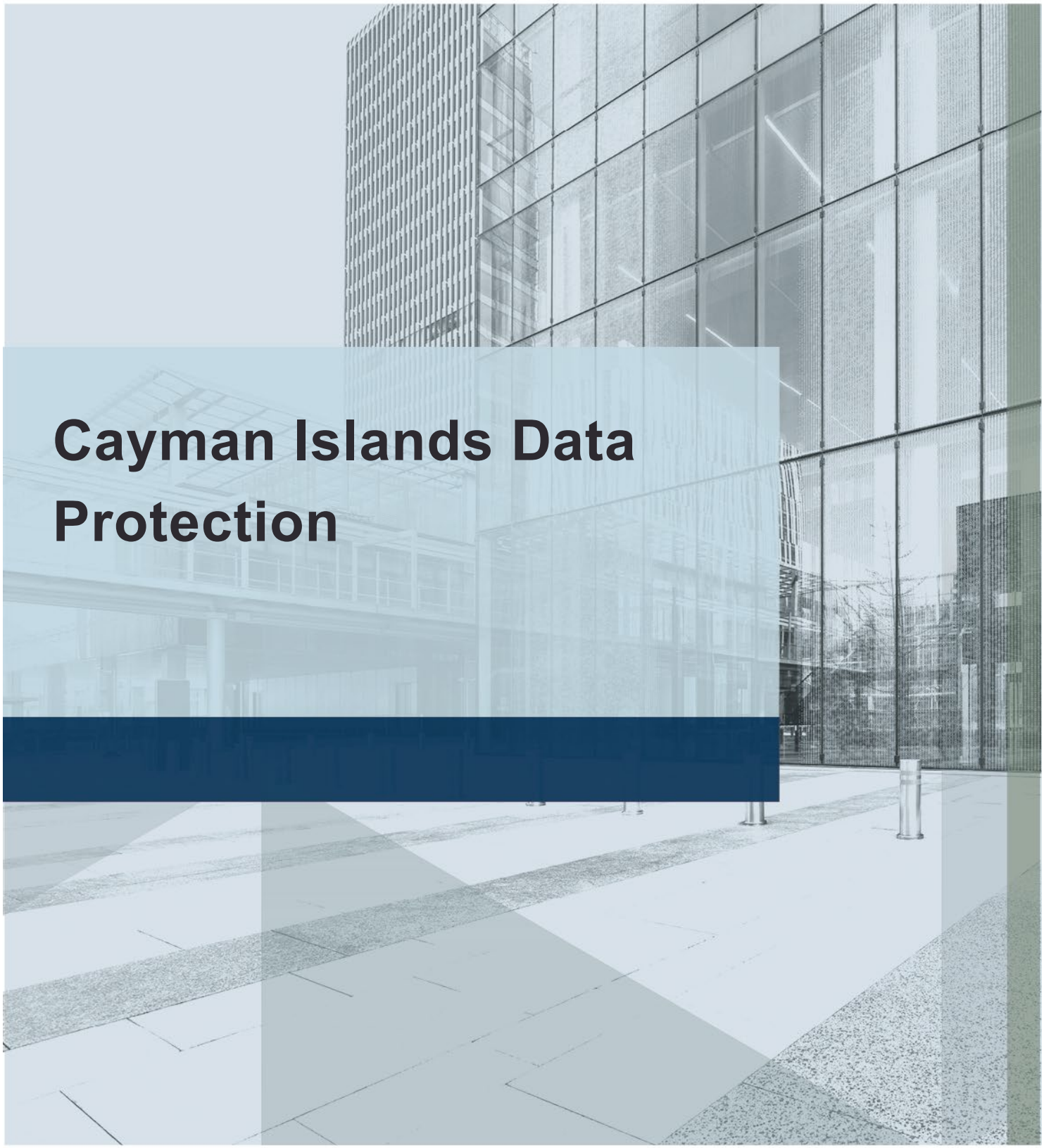
CONYERS



Cayman Islands Data Protection

conyers.com

Preface

This publication has been prepared for the assistance of those who may be in control of or processing personal data in the Cayman Islands. It deals in broad terms with the requirements of the Cayman Data Protection Act (2021 Revision). It is not intended to be a comprehensive guide but deals only with the key concepts and obligations which arise from the same which we hope will be of use to our clients. We recommend that our clients and prospective clients seek legal advice in Cayman on their specific situations.

Conyers

TABLE OF CONTENTS

1. BACKGROUND AND OVERVIEW

The Cayman Islands Data Protection Act (2021 Revision) ("**DPA**") and The Data Protection Regulations, 2018 (the "**Regulations**") came into force on 30 September 2019. The Office of the Ombudsman, the Cayman Islands' supervisory authority for data protection, has also issued a Guide for Data Controllers (the "**Guide**"[1]), a Guide for Data Subjects[2] and Guidance for Small Business and Organizations[3] which indicate how the Ombudsman will interpret the DPA.

The DPA, which is modelled on European data protection legislation, regulates the processing of all Personal Data (defined below) in the Cayman Islands and introduces globally recognized principles regarding the use of Personal Data in the Cayman Islands. The DPA applies to Personal Data processed by "Data Controllers" and "Data Processors" established within the Cayman Islands and to Data Controllers established outside the Cayman Islands that process Personal Data within the Cayman Islands otherwise than for the purposes of transit of the data through the Cayman Islands. Where a Data Controller established outside the Cayman Islands processes data in the Cayman Islands it will be required to nominate a local representative located in the Islands who shall be the Data Controller for the purposes of compliance with the DPA.

2. KEY DEFINITIONS AND CONCEPTS

2.1. Definitions

"consent"	in relation to a Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which the Data Subject, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to the said Data Subject; The burden of proving that consent was given lies with the Data Controller. Consent may be withdrawn at any time; such withdrawal will not affect the lawfulness of processing based on consent before its withdrawal.
"Data Controller"	a person who, alone or jointly with others determines the purposes, conditions and manner in which any Personal Data are, or are to be processed and includes a local representative (who is required to be appointed where the Data Controller is not established in Cayman but the Personal Data are processed in Cayman);

[1] v1.05 May 2023

[2] V02 25 August 2023

[3] Last updated 19 April 2021

"Data Processor"	any person who processes Personal Data on behalf of a Data Controller but does not include an employee of the Data Controller;
"Data Subject"	any identified living individual or any living individual who can be identified directly or indirectly by means reasonably likely to be used by the Data Controller or by any other person;
"Personal Data"	data relating to a living individual who can be identified such as: (a) the living individual's location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the living individual; (b) any expression of opinion about the living individual; or (c) any indication of the intentions of the Data Controller or any other person in respect of the living individual;
"processing"	in relation to data, means obtaining, recording or holding data, or carrying out any operation or set of operations on Personal Data including: (a) organizing, adapting or altering the Personal Data; (b) retrieving, consulting or using the Personal Data; (c) disclosing the Personal Data by transmission, dissemination or otherwise making it available; or (d) aligning, combining, blocking, erasing or destroying the Personal Data.
"Sensitive Personal Data"	in relation to a Data Subject means: (a) the racial or ethnic origin of the Data Subject; (b) the political opinions of the Data Subject; (c) the Data Subject's religious beliefs or other beliefs of a similar nature; (d) whether the Data Subject is a member of a trade union; (e) genetic data of the Data Subject; (f) the Data Subject's physical or mental health or condition; (g) medical data; (h) the Data Subject's sex life; (i) the Data Subject's commission, or alleged commission, of an offence; or (j) 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 Islands or elsewhere.

3. DATA PROTECTION PRINCIPLES

The DPA imposes specific obligations on Data Controllers including the duty to apply the eight Data Protection Principles ("**DPPs**"), the duty to respond in a timely fashion to requests from Data Subjects in relation to their Personal Data and the duty to notify Data Subjects and the Ombudsman of any Personal Data breaches.

3.1. First Data Protection Principle - fair and lawful processing

The first DPP requires that Personal Data be processed fairly. To be processed fairly, there must be a legal basis for handling the Personal Data (at least one of the conditions in paragraphs 1 - 6 of Schedule 2 to the DPA):

(a) consent;

(b) necessary for contract;

(c) legal obligation;

(d) to protect vital interests;

(e) necessary for the exercise of public functions;

(f) legitimate interests.

In the case of Sensitive Personal Data, at least one of the conditions in Schedule 3 to the DPA must be met:

(a) consent;

(b) employment;

(c) vital interests;

(d) non-profit associations;

(e) information made public by Data Subject;

(f) legal proceedings;

(g) public functions;

(h) medical purposes;

(i) circumstances prescribed by regulations.

In determining whether Personal Data are processed fairly, regard will be given to the method by which they are obtained and whether the Data Subject has been deceived or misled as to the purpose for which the data is to be processed. In addition, Personal Data will not be considered to have been processed

fairly unless the Data Subject has been provided with the identity of the Data Controller and the purpose for which the data are to be processed.

3.2. Second Data Protection Principle - processing for one or more specified lawful purposes and not further processed in any incompatible manner

In order to comply with the second DPP, a Data Controller should be clear about why they are collecting Personal Data and what they intend to do with it and ensure that any additional use or disclosure of the Personal Data is also fair, lawful and transparent. A Data Controller that is in compliance with the fairness and transparency obligations required by the first DPP is likely to be in compliance with the second DPP.

3.3. Third Data Protection Principle - Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected or processed

The DPA does not prescribe what is meant by adequate, relevant and not excessive. It is necessary for Data Controllers to identify the minimum amount of Personal Data required to fulfil their specified purposes. If a Data Controller is holding more data than is necessary for its purpose, this is likely to be unlawful (as most of the lawful bases for holding Personal Data have a necessity element). Data Subjects will also have the right to demand that processing cease.

Data may also be inadequate for the stated purpose. A Data Subject may ask a Data Controller to supplement incomplete data under the right to rectification.

3.4. Fourth Data Protection Principle - Personal Data shall be accurate and kept up to date

Data Subjects have the right to have inaccurate Personal Data corrected. "Inaccurate" means, in relation to Personal Data, data that are misleading, incomplete or out of date.

Opinions are subjective and a record of an opinion will not necessarily be inaccurate Personal Data because the Data Subject disagrees with it, or the opinion proves to be wrong. To be "accurate" records should make clear that it is an opinion. Where appropriate, the Ombudsman may order the rectification, blockage, erasure or destruction of expressions of opinion based on inaccurate Personal Data.

It is not necessary to update Personal Data if, for example, it is held for statistical, historical or other scientific research reasons. It may also be reasonable to rely on the Data Subject to tell the Data Controller when their Personal Data has changed.

Data Subjects are entitled to require that a Data Controller cease processing their Personal Data in general or for a specified purpose or in a specified manner.

3.5. Fifth Data Protection Principle - Personal Data shall not be kept for longer than is necessary

Data Controllers should have a policy setting out Data retention periods and should periodically review the same and erase or anonymize data when it is no longer needed. The DPA does not prescribe specific time limits for types of data as it will depend upon how long the data is needed for the specified purposes. Personal Data held for too long will be unnecessary and there will not likely be a lawful basis for retention.

In setting retention periods, factors to consider include information needed to defend possible legal claims; any legal or regulatory requirements; industry standards or guidelines.

It is not always possible to delete or erase all traces of data; in such circumstances, the data should be put beyond use. Alternatively data can by anonymized so that it is no longer in a form which permits identification of Data Subjects.

Personal Data may also be processed for historical, statistical or scientific purposes and may, subject to compliance with the relevant conditions, be exempt from the fifth DPP. If indefinite retention is justified on this basis, the data cannot then be used for another purpose.

3.6. Sixth Data Protection Principle - Personal Data shall be processed in accordance with the rights of Data Subjects under the DPA

The rights of Data Subjects under the DPA are summarised below.

(a) **The right to be informed:**

This right follows from the first DPP requiring fair and lawful processing. Processing will only be fair if Personal Data is handled in ways that people would reasonably expect. This includes being informed of the identity of the Data Controller and the purposes for processing. Typically this would be done in the privacy notice which should be provided to the Data Subject as soon as practicable; usually when the data is being gathered.

(b) **The right of access:**

Subject to certain exceptions, individuals have the right to access their own Personal Data and receive information about its use including for example, the purpose of the processing, to whom the Personal Data may be disclosed, countries to which it may be transferred, and measures taken to protect such data. Data Controllers have 30 days to respond to a written subject access request. If the Data Controller needs additional information to comply with the request and informs the Data Subject in writing, the 30 day time period is suspended pending supply of the information.

(c) **The right to rectification:**

Individuals have a right to have inaccurate data rectified, blocked, erased or destroyed. Rather than requesting that inaccuracies be corrected, the right is to complain to the Ombudsman. As a matter of good practice, Data Controllers should attend to reasonable requests for rectification of data rather than waiting for a formal complaint to be made.

(d) **The right to stop/ restrict processing:**

Subject to certain exemptions, individuals may require that a Data Controller cease processing Personal Data; not begin processing Personal Data; cease processing Personal Data for a specified purpose or cease processing Personal Data in a specified manner.

Data Controllers must comply with such requests as soon as practicable (in any case within 21 days of receiving a written notice) unless the processing is done to meet the conditions of a contract; when it is done under a legal obligation or in order to protect the vital interest of the individual.

(e) **The right to stop direct marketing:**

There is an absolute right for a Data Subject to demand by notice in writing to a Data Controller that direct marketing relating to the Data Subject cease or not begin. "Direct marketing" is defined as:

> *The communication, by whatever means, of any advertising, marketing, promotional or similar material, that is directed to particular individuals.*

(f) **The right in relation to automated decision making:**

Data Subjects should be notified when decisions are being made without human involvement and have the right (within 21 days of such notice) to require, by written notice to the Data Controller, that any such decision be reconsidered on a different basis. For example, processing of Personal Data relating to a Data Subject's performance at work, creditworthiness, reliability, conduct of any other matters relating to the Data Subject. The Data Controller then has 21 days to give the Data Subject a written notice specifying the steps the Data Controller intends to take to comply with the Data Subject's notice.

Notification to the Data Subject is not required if two conditions are satisfied: first - if the decision is taken for the purpose of considering whether to enter into a contract with the Data Subject, or in the course of performing such a contract, or if the decision is authorized or required under any enactment and second - the decision is to grant a request of the Data Subject, or the Data Subject's interests are safeguarded by allowing them to make representations.

(g) **The right to complain and seek compensation.**

An individual has the right to complain to the Ombudsman about any perceived violation of the DPA and to seek compensation from the Data Controller for damages in the courts.

3.7. Seventh Data Protection Principle - appropriate technical and organizational measures shall be taken in relation to Personal Data

The seventh DPP encompasses organizational measures such as staff training and policy development, technical measures such as physical data protection, pseudonymisation, and encryption and securing ongoing availability, integrity of data and accessibility to data by ensuring backups.

The DPA does not define the security measures that are required other than that they be "appropriate" to the risks presented by the relevant processing.

In the context of physical security, relevant factors would include the protection of business premises through locks, alarms and security lighting or CCTV; access to business premises and the supervision of visitors; security of IT equipment, in particular mobile devices.

In terms of cybersecurity, the security of systems, data, online services and devices should be considered.

Where a Data Processor processes data on behalf of a Data Controller, appropriate due diligence should be conducted on the Data Processor. In addition, a formal data processing agreement should be in place.

It is vital that any staff of a Data Controller understand the importance of protecting Personal Data and are familiar with security policies and procedures.

3.8. Eighth Data Protection Principal - international transfers require an adequate level of protection for the rights and freedoms of Data Subjects

The transfer of Personal Data is prohibited where the destination is outside the European Union[4] or is otherwise to a county that does not offer an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data.

The Data Controller should assess a number of factors in deciding whether a country or territory would be compliant with the eighth DPP. Where unsure, a Data Controller may request an authorization from the Ombudsman. Factors to consider include the following:

In addition, Schedule 4 of the DPA sets out transfers to which the 8th DPP does not apply including:

(a) Consent - where the Data Subject has consented to the transfer;

(b) Contract - where the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or the taking of steps at the request of the Data Subject with a view to entering into such contract;

(c) Third Party Contract - where the transfer is necessary for the conclusion or performance of a contract and a third party at the request of, or in the in the interests of the Data Subject;

(d) Public Interest - where the transfer is necessary for reasons of substantial public interest.

(e) Legal Proceedings - where the transfer is necessary for, or in connection with legal proceedings, for obtaining legal advice or otherwise establishing, exercising or defending legal rights.

[4] The Ombudsman considers the following countries and territories to have an adequate level of protection: Member States of the European Economic Area where the EU General Data Protection Regulation ("**GDPR**") is applicable; and any country or territory in respect of which an adequacy decision has been adopted by the European Commission pursuant to Article 45(3) GDPR or remains in force pursuant to Article 45(9) of the GDPR.

(f) Vital Interests - the transfer is necessary to protect the vital interests of the Data Subject;

(g) Public Register - the transfer is part of the personal data on a public register and any publication conditions are complied with;

(h) Transfer on terms approved by the Ombudsman;

(i) Ombudsman has authorized transfer;

(j) International cooperation between intelligence agencies or regulatory agencies - the transfer is required to combat crime, terrorism or drug trafficking or to carry out other cooperative functions.

(k) Regulations concerning the public interest - the Cabinet may by regulation specify other circumstances.

4. EXEMPTIONS

There are exemptions to certain obligations in order to ensure that Personal Data can be used in appropriate circumstances, e.g. for national security, law enforcement, certain public functions, health care, education, social work, journalism, literature, art, research, history, statistics, information available under an enactment, legal proceedings, personal family or household affairs, honours, corporate finance, negotiations, legal privilege. Cabinet may also develop further regulations providing for additional exemptions.

5. ENFORCEMENT

Data subjects can report personal data breaches to the Ombudsman either using a fillable PDF notification form or an online personal data breach notification form. The form can be used by Data Processors and Data Controllers to report personal data breaches directly to the Ombudsman via the Ombudsman's website.

The Ombudsman has the power to:

- hear, investigate and rule on complaints;
- monitor, investigate and report on the compliance of Data Controllers;
- intervene and deliver opinions and orders related to the processing operations;
- order the rectification, blocking, erasure or destruction of data;
- impose a temporary or permanent ban on processing;
- make recommendations for reform of both a general nature and directed at specific Data Controllers;
- engage in proceedings where the provisions of the DPA have been violated, or refer these violations to the appropriate authorities;

- cooperate with international data protection supervisory authorities;
- publicize and promote the requirements of the DPA and the rights of Data Subjects under it;
- do anything which appears to be incidental or conducive to the carrying out of his functions under the DPA.

6. OFFENCES AND PENALTIES

Offences under the DPA include:

- failing to make certain particulars available to a Data Subject in response to a request;
- failing to notify a Data Subject and the Ombudsman of a personal data breach;
- withholding, altering, suppressing or destroying information requested by the Ombudsman;
- knowingly or recklessly disclosing information;
- obstructing a warrant or making a false statement;
- unlawfully obtaining, disclosing, selling or procuring personal data;
- failing to comply with an enforcement or monetary enforcement order;
- other offences specified in Regulations.

Breaches of the DPA could result in fines of up to CI$100,000/US$122,000 per breach, imprisonment for a term of up to 5 years or both. Other monetary penalties of up to CI$250,000/US$305,000 are also possible in certain circumstances where there has been a serious contravention of the DPA of a kind likely to cause substantial damage or substantial distress to the Data subject.

7. ACHIEVING COMPLIANCE

The DPA gives individuals the right to, amongst other things, access Personal Data held about them and to request that any inaccurate Personal Data is corrected or deleted. Data Controllers will need to have policies and procedures in place to manage these requests. The DPA also obliges businesses to cease processing Personal Data once the purposes for which that Personal Data has been collected have been exhausted. Prescribed data retention periods are not set out in the DPA but an analysis will need to be undertaken to determine how long Personal Data should be kept for. Similarly, it will be important to evaluate how Personal Data can be securely deleted once the purposes for holding it have been fulfilled.

Implementing a Personal Data protection compliance programme will require the creation of an effective internal training and governance regime for approving, overseeing, implementing and reviewing the various DPA policies. There will need to be written reporting procedures and approved protocols for dealing with subject access requests, data breaches and for seeking legal advice. The appointment of a Data Protection Officer is also recommended. For further information in respect of your obligations under or steps to achieve compliance with the DPA, please contact your usual Conyers contact.