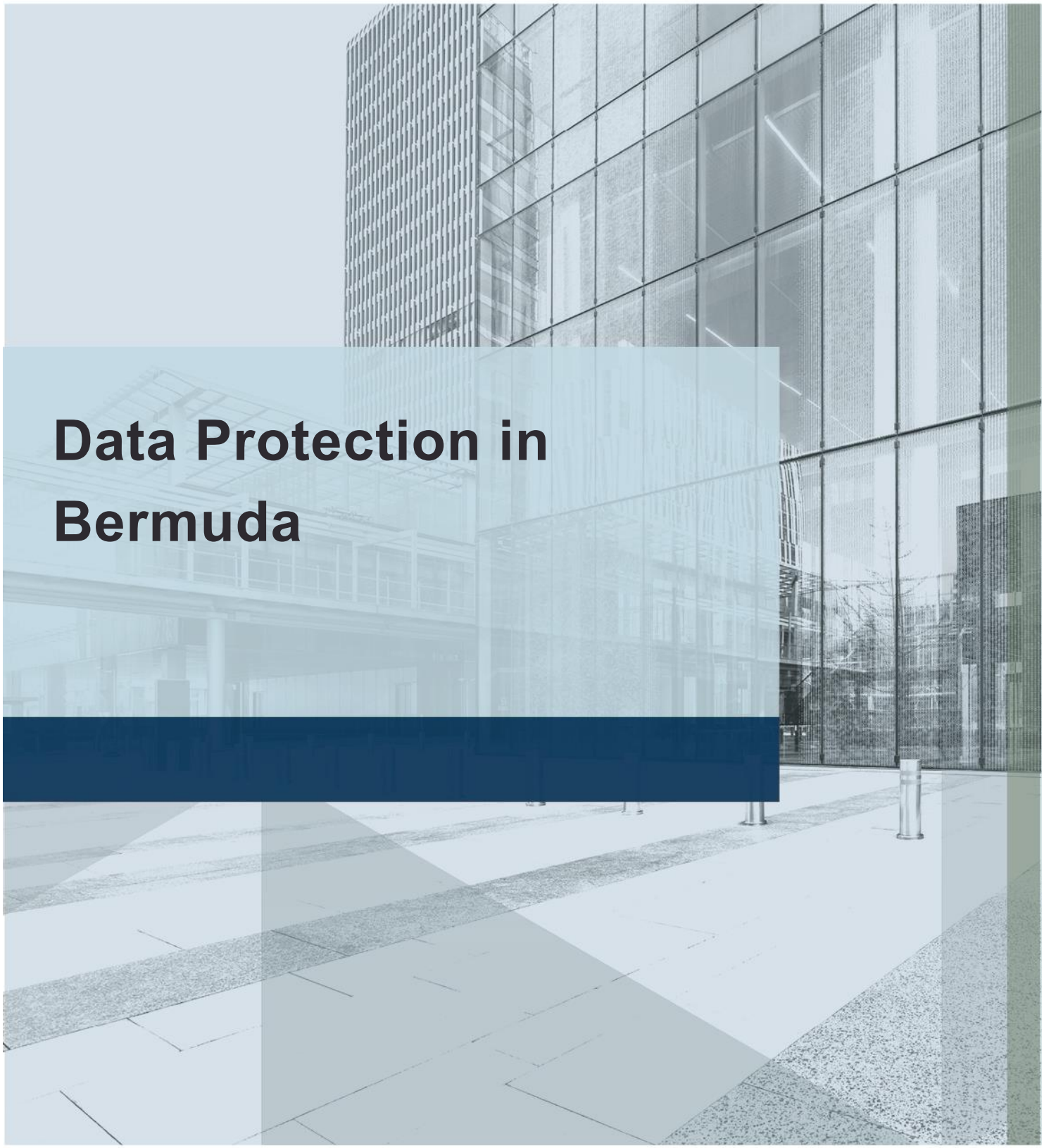
CONYERS



Data Protection in Bermuda

conyers.com

Preface

This publication has been prepared for the assistance of those seeking information regarding the protection and use of personal information in Bermuda. It deals in broad terms with the requirements of Bermuda law. It is not intended to be exhaustive but merely to provide general information to our clients and their professional advisers.

We recommend that our clients seek legal advice in Bermuda on their specific proposals before taking any steps to implement them.

Conyers Dill & Pearman

TABLE OF CONTENTS

1. INTRODUCTION

Bermuda recognises the right to information privacy and has introduced legislation in the form of the Personal Information Protection Act 2016 ("**PIPA**") to regulate and protect the use of personal information under the auspices of a Privacy Commissioner appointed by the Governor (the "**Privacy Commissioner**"). PIPA embodies the eight guiding principles recognised internationally for the collection and use of personal information and is intended to compliment the Public Access to Information Act 2010, which provides for access to information held by public authorities.

PIPA provides that personal information can only be used by an organisation in a lawful and fair manner.

Some sections of PIPA came into force on 2 December 2016. With the appointment of the Privacy Commissioner on 20 January 2020, the remaining sections of PIPA are expected to become operative in the near future.

2. APPLICATION OF PIPA

The legislation targets a very wide range of entities and applies to any individual, entity or public authority collecting, storing and using personal information in Bermuda either electronically, or as part of a structured filing system ("**Organisation**").

3. USE OF PERSONAL INFORMATION BY AN ORGANISATION

An Organisation may use personal information if at least one of the following conditions is met:

(a) **Consent**: the Organisation must be able to reasonably demonstrate that the individual has knowingly consented;

(b) **Reasonableness**: except in relation to sensitive personal information, a reasonable person giving due weight to the sensitivity of the personal information would consider that:

  (i) the individual would not reasonably request that the use of his personal information should not begin or that they would want it to cease; and

  (ii) use does not prejudice the rights of the individual;

(c) **Contractual Necessity**: it is necessary for the:

  (i) performance of a contract to which the individual is a party; or

  (ii) taking of steps at the request of the individual with a view to entering into a contract;

(d) **Legal Requirement**: it is pursuant to a provision of law that authorises or requires such use;

(e) **Public Availability**: it is publicly available and will be used for a purpose consistent with its public availability;

(f) **Emergency**: it is necessary to respond to an emergency that threatens the life, health or security of an individual or the public;

(g) **Public Interest**: it is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the organisation or in a third party to whom the personal information is disclosed; or

(h) **Employment**: it is necessary in the context of an individual's present, past or potential employment relationship with the organisation.

4. TRANSFER OF PERSONAL INFORMATION OUT OF THE JURISDICTION

An Organisation remains responsible for the protection of personal information where it is transferred to an overseas third party. Where the Privacy Commissioner does not designate a particular jurisdiction as providing a comparable level of protection, with few exceptions, the Organisation must employ contractual mechanisms, corporate codes of conduct or other means to ensure the overseas third party provides a comparable level of protection.

5. CATEGORIES OF INFORMATION

5.1. Sensitive Information

As one might expect, the protection of sensitive information is held to higher account and cannot be used to discriminate against any person contrary to the provisions of Part II of the Human Rights Act 1981 without lawful authority. Sensitive information includes personal information relating to an individual's place of origin, race, colour, sex, sexual orientation, national or ethnic origin, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric and genetic information. Sensitive personal information can only be used with lawful authority:

(a) with consent;

(b) by court order/order of the Privacy Commissioner;

(c) in criminal or civil proceedings; and

(d) in an employment or recruitment context if the role justifies it.

5.2. Personal Information regarding Children

Added safeguards apply to the collection of personal information from children (defined as under 14 years) and their immediate family through the provision of a service delivered on-line. Verifiable consent must be obtained from the parent/guardian before the information is collected or otherwise used and privacy notices must be age appropriate.

6. OBLIGATIONS OF AN ORGANISATION

(a) **Privacy Officer**: an Organisation must designate a representative as a privacy officer for compliance purposes.

(b) **Privacy Notices**: an Organisation must provide individuals with a clear and easily accessible privacy notice detailing its practices and policies with respect to personal information either before or at the time of collection of the information (unless all use of the information is within the reasonable expectations of the individual to whom the personal information relates).

(c) **Purpose Limitation**: with certain exceptions, the personal information can only be used for the limited purposes set out in the privacy notice.

(d) **Proportionality**: the information collected must be adequate, relevant and not excessive in relation to the purpose it is used.

(e) **Integrity**: the information must be accurate and kept up to date to the extent necessary for the purpose of use and cannot be kept longer than necessary for that use.

(f) **Security Safeguards**: the personal information an organisation holds must be protected with adequate safeguards against loss, unauthorised access and other misuse. Safeguards must be proportional to the likelihood and severity of the harm threatened by the loss, the sensitivity of the personal information and the context in which it is held.

(g) **Breach of Security**: in case of breach, the Organisation must notify the Privacy Commissioner without delay and all individuals that may be affected.

(h) **Responsibility for Third Parties**: where an Organisation engages the services of a third party in connection with the use of personal information, the Organisation remains responsible for ensuring compliance.

7. RIGHTS OF INDIVIDUALS

7.1. Access

With certain exceptions, Organisations must allow individuals access to their personal information, the purpose for which it is being held, and the names of those and circumstances in which the personal information is being disclosed.

7.2. Rectification, blocking, erasure and destruction

An individual may make a written request to an Organisation that an error or omission in their personal information be corrected. The Organisation is then required to correct the information as soon as reasonably practicable and to advise others to whom the information has been disclosed of the correction. An individual may request that their personal information not be used for advertising, marketing or public relations and may require that personal information be erased or destroyed where it is no longer relevant for the purposes of its use.

An Organisation is required to comply with any reasonable request by an individual for a copy of the personal information held within 45 days (which time may be extended). A fee for provision of the information may be charged.

8. COMPENSATION FOR FINANCIAL LOSS OR DISTRESS

An individual who suffers financial loss or emotional distress through an Organisation's failure to comply with its requirements under PIPA is entitled to compensation from the Organisation.

9. EXCLUSIONS AND EXEMPTIONS

To ensure personal information can be used in appropriate circumstances, PIPA recognises a number of exemptions to the obligations noted, including national security, law enforcement, certain public functions, health care, education, social work, journalism, literature, art, research, history, statistics, information available under enactment, legal proceedings, personal and family or household affairs, corporate finance, negotiations and legal privilege.

A person committing an offence under PIPA, including but not limited to:

(a) wilfully or negligently using or authorising the use of personal information in a manner inconsistent with PIPA and likely to cause harm to an individual;

(b) wilfully attempting to gain or gaining access to personal information in a manner inconsistent with PIPA and likely to cause harm to an individual;

(c) disposing of or altering, falsifying, concealing or destroying personal information, or directing another person to do so, in order to evade a request for access to the personal information;

(d) obstructing the Commissioner or an authorised delegate in the performance of their duties, powers or functions;

(e) knowingly making false statements to the Commissioner or knowingly misleading or attempting to mislead the Commissioner in the course of his duties, powers or function;

(f) failing to notify the Commissioner of a breach of security and failing to notify any individual affected by such breach; or

(g) disobeying an Order of the Commissioner;

may be liable on summary conviction in the case of an individual, to a fine of up to $25,000 and up to two years imprisonment and in the case of conviction of an entity on indictment, to a fine not exceeding $250,000.

For additional information, please contact your usual Conyers Dill & Pearman representative.