Privacy and Data Protection in Bermuda

CONYERS

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 legislatively recognised the right to personal information privacy with the enactment of the Personal Information Protection Act 2016 (as amended) ("**PIPA**") which became fully effective on 1 January 2025. PIPA regulates and protects the use of personal information under the auspices of the Office of the Privacy Commissioner for Bermuda (the "**Privacy Commissioner**"). PIPA embodies several internationally recognised principles for the collection and use of personal information, and was intended to complement the Public Access to Information Act 2010 which provides for access to information held by public authorities.

2. APPLICATION OF PIPA

PIPA applies to any "organisation" that "uses" "personal information" in Bermuda where that personal information is used wholly or partly by automated means and to the use, other than by automated means, of personal information which form, or are intended to form, part of a structured filing system. In context, "organisation" means an individual, entity or public authority that uses personal information in Bermuda, "personal information" means any information about an identified or identifiable individual (i.e. a natural person) and "use or using" are broadly defined and would generally capture any manipulation of personal information.

Unlike other data protection regimes such as the EU's GDPR, PIPA does not adopt the concepts of "data controllers" and "data processers" – either an organisation is using personal information in Bermuda, and it must therefore comply with PIPA, or it is not. Whether an organisation is in scope of PIPA will be a fact based analysis. For example, a Bermuda exempted company with domestic operations and employees in Bermuda, will almost certainly be using personal information in Bermuda, and be in scope of PIPA.

3. EXCLUSIONS AND EXEMPTIONS

PIPA specifically recognises a number of exclusions, and does not apply to certain personal information, including when: (i) used for personal or domestic purposes; (ii) used for artistic, literary or journalistic purposes with a view to publication in the public interest in so far as is necessary to protect the right to freedom of expression; (iii) used for business contact information for the purpose of contacting an individual in his capacity as an employee or official of an organisation; or (iv) about an individual who has been dead for at least 20 years or an entity that has been in existence for at least 150 years.

To ensure personal information can be used in appropriate circumstances, PIPA also recognises a number of exemptions to the general obligations, including for safeguarding national security, discharging certain public functions, law enforcement and crime prevention as well as for acts by communications providers.

4. LAWFUL CONDITIONS FOR USE OF PERSONAL INFORMATION

Subject to certain exceptions, an organisation may use personal information only if at least one of the following conditions are met:

(a) **Consent**: it is used with the individual's consent where the organisation can reasonably demonstrate that the individual has knowingly consented;

(b) **Reasonable expectation**: 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 be expected to request that the use of their personal information should not begin or cease; and (ii) the use does not prejudice the individual's rights;

(c) **Contractual Necessity**: it is necessary for the: (i) performance of a contract to which the individual is a party; or (ii) taking steps at the individual's request 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 the purpose of 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.

5. SENSITIVE PERSONAL INFORMATION

PIPA specifically distinguishes "sensitive personal information" which means any 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. An organisation shall not without lawful authority use sensitive personal information in order to discriminate against any person contrary to any provision of Part II of the Human Rights Act 1981.

6. GENERAL PRINCIPLES AND RULES

6.1. General Principles

Organisations in scope of PIPA must adopt suitable measures and policies to give effect to its obligations and the rights of individuals under PIPA. These measures and policies must take into account the nature, scope, context and purposes of the personal information use and the risk to individuals by such use. Organisations must adhere to the following principles set out under PIPA:

(a) **Lawfulness and Fairness:** personal information must only be used in a lawful and fair manner.

(b) **Purpose Limitation**: with certain exceptions, personal information can only be used for the specific purposes set out in an organisation's privacy notice, or for purposes that are related to those specific purposes.

(c) **Proportionality**: personal information collected must be adequate, relevant and not excessive in relation to the purposes for which it is used.

(d) **Reasonableness**: an organisation must act in a reasonable manner in meeting its responsibilities under PIPA.

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

(f) **Security Safeguards**: personal information held by an organisation must be protected with appropriate safeguards against risk including loss, unauthorised access, destruction, use, modification or disclosure and any 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) **Responsibility for Third Parties**: where an organisation engages (by contract or otherwise) the services of a third party in connection with the use of personal information, the organisation remains responsible for ensuring compliance with PIPA at all times.

6.2. Privacy Officer

An organisation must designate a representative "privacy officer" who has primary responsibility for communicating with the Privacy Commissioner. A privacy officer may delegate his duties to one or more individuals, and, provided that they are accessible to each organisation, a group of organisations under common control may appoint a single privacy officer. A privacy officer is not required to be located in Bermuda.

6.3. Privacy Notices

Subject to certain exceptions, an organisation must provide individuals with a clear and easily accessible privacy statement, a "privacy notice", about its practices and policies with respect to personal information. The privacy notice must include certain statutorily prescribed details, including the privacy officer's contact details and the purposes for which personal information is or might be used. Where applicable, organisations must take all reasonably practicable steps to ensure that the privacy notice is provided either before or at the time of collection of the personal information or, where that is not possible, as soon as is reasonably practicable thereafter.

6.4. Breach of Security Notifications

In case of a breach of security leading to the loss or unlawful destruction or unauthorised disclosure of or access to personal information which is likely to adversely affect an individual, an organisation responsible for that personal information must without undue delay:

(a) notify the Privacy Commissioner of the breach; and

(b) then notify any individual affected by the breach.

The Privacy Commissioner's notification must describe (i) the nature of the breach; (ii) its likely consequences for that individual; and (iii) the measures taken, and to be taken, by the organisation to address the breach.

7. RIGHTS OF INDIVIDUALS

Subject to certain restrictions, an individual may submit a written request to an organisation to:

(a) **Access** (i) their personal information in the organisation's custody or control; (ii) the purposes for which the organisation has been or is using their personal information; and (iii) the names of persons or types of persons and circumstances for which their personal information has or is being disclosed;

(b) **Correct an error or omission** in any of their personal information which is under the control of the organisation;

(c) **Erase or destroy** personal information about the individual where that personal information is no longer relevant for the purposes of its use; and

(d) **Block** which is to cease, or not to begin, using their personal information for the purposes of advertising, marketing or public relations, or where the use of that personal information is causing or is likely to cause substantial damage or substantial distress to the individual or another individual.

Organisations must promptly acknowledge receipt of an individual's request and respond within 45 days (which time may be extended). Organisations may be able to charge a fee for requests, however, a fee cannot be charged if the request corrects incorrect information.

An organisation may be able to refuse to provide access to personal information, for example, where it is protected by any legal privilege. In some circumstances an organisation must not provide access to personal information, including where disclosure could reasonably be expected to threaten the life or security of an individual.

8. TRANSFERS OF PERSONAL INFORMATION OUT OF BERMUDA

An organisation remains responsible for the protection of personal information where it is transferred to an overseas third party. With few exceptions, before transferring any personal information to an overseas third party an organisation must assess the level of protection provided by the laws applicable to such overseas third party. The Privacy Commissioner can designate particular jurisdictions as having a comparable level of protection to PIPA, however, to date no such designations have been made. If the organisation reasonably believes that the protection provided by the overseas third party is comparable to the level of protection required by PIPA, the organisation may rely on such comparable level of protection while the personal information is being used by the overseas third party. Where such level of protection is not considered adequate, the organisation must employ contractual mechanisms, corporate

codes of conduct (including binding corporate rules) or other means to ensure that the overseas third party provides a comparable level of protection.

9. PERSONAL INFORMATION ABOUT CHILDREN IN THE INFORMATION SOCIETY

Added safeguards apply where an organisation uses personal information about a child (an individual under the age of 14) in the provision of an "information society service" (meaning a service delivered by digital means or electronic communications) that is (a) targeted at children; or (b) if the organisation has actual knowledge that it is using personal information about children. If consent is relied upon, verifiable consent from a parent or guardian must be obtained by the organisation before any personal information is collected or used.

10. DISCLOSURES FOR BUSINESS TRANSACTIONS

Provided that certain requirements are complied with an organisation is permitted to disclose and use personal information for the purposes of a business transaction. A business transaction consists of a purchase, sale, lease, merger or amalgamation, or the taking of a security interest in respect of, an organisation or a portion of an organisation or any organisation's business or activity or business asset including any prospective transaction. Organisations that are party to the business transaction can also use personal information leading up to and including completion without an individual's consent provided the certain conditions are satisfied.

11. COMPENSATION FOR FINANCIAL LOSS OR DISTRESS

An individual who suffers financial loss or emotional distress as a result of an organisation's failure to comply with any of the requirements of PIPA is entitled to compensation from the organisation. In proceedings brought against an organisation for failure to comply with PIPA, it is a defence for the organisation to prove that it had taken such care as in all circumstances was reasonably necessary to comply with the requirement.

12. OFFENCES

A person committing an offence under PIPA 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. Offences under PIPA include, but are 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) 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;

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

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

(e) disobeying an order of the Privacy Commissioner.

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