APRIL 2025
EDITION

BERMUDA LAW OVERVIEW

DATA PROTECTION – PART 1

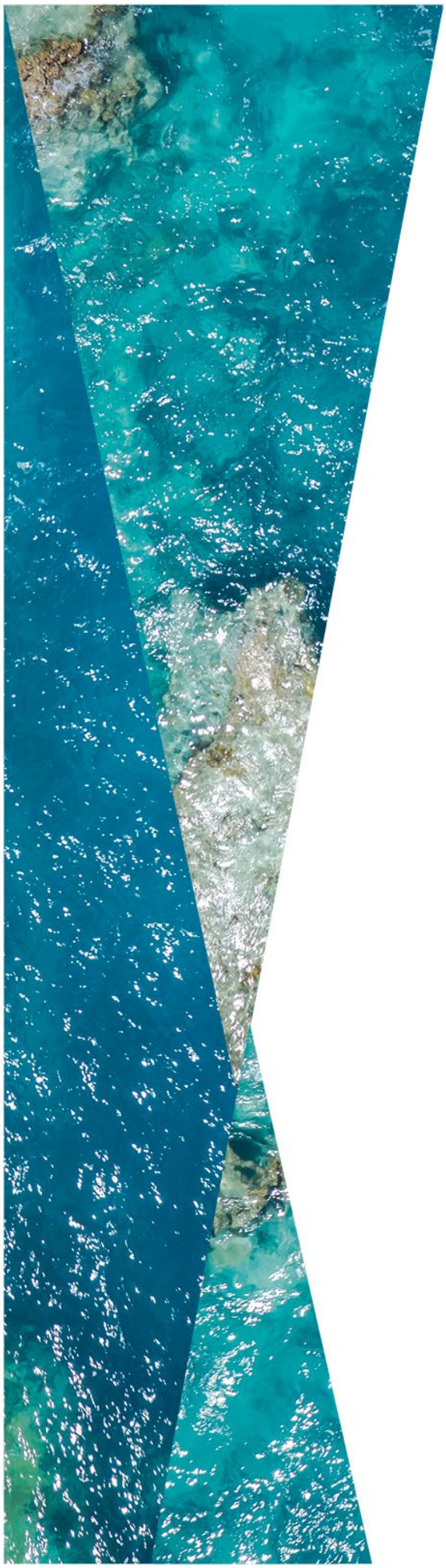
UNDERSTAND THE BASICS

DIVING TO NEW **DEPTHS**

A NEW **OCEAN OF PRIVACY REGULATION**

INSIDE THIS ISSUE

BeesMont Law Limited



ATTORNEY CONTRIBUTOR

Gretchen Tucker is a Bermuda and UK qualified barrister.

She provides advice and representation in connection with regulatory and statutory compliance, administrative decision making and processes, statutory interpretation, policy development and legal reform. She also advises clients on their interactions with Bermuda government watchdogs and regulators.

Gretchen works closely with our Corporate attorneys to advise commercial organisations on transactional employment and privacy issues arising from mergers & acquisitions, business re-organisations and strategic planning as well as compliance with the Personal Information Protection Act 2016.

Industry Activity

In January 2019, in the absence of the appointment of the first Privacy Commissioner for Bermuda, she established a new standing sub-committee of the Bermuda Bar Council advocating for the advancement of privacy law and the appropriate regulation of the legal industry. She served as Chair and Co Chair from 2019-2024.

Gretchen has further served as a Co-Chair of the Bermuda IAPP KnowledgeNet Chapter since 2020.

2022 IAPP Trust Bursary Recipient

2024 Bermuda Privacy Ambassador

2025 WISP Scholar Privacy + Security Forum

GRETCHEN TUCKER

Counsel, Head of Regulatory & Governance

Practice Groups

- Privacy, Security & Information Law
- Regulatory & Compliance
- Employment & Talent Management

Main Practices

- IT Law & Contract Negotiation
- Public Relations and Media Management
- Public Law
- Privacy by Design
- Workplace Privacy
- Employment , Human Rights & Immigration Law

WOMEN DEFINING THE FUTURE 50 FOR THE NEXT 50

The following content was originally published as part of the April 2025 Bermuda – Privacy Overview Guidance Note on the OneTrust DataGuidance platform for regulatory research pursuant to a contributor agreement between OneTrust DataGuidance and attorney contributor, Gretchen Tucker.

LAWS

1.1. Laws and regulations

1.1.1. What laws and/or regulations apply to personal data protection?

Statutory data protection in Bermuda by primarily governed by the Personal Information Protection Act 2016 (**PIPA**), which came fully into force within the jurisdiction on January 1, 2025. Prior to January 1, 2025, the administrative provisions of the statute had been in force since December 2, 2016.

PIPA is subject to the Bermuda Constitution Order 1968 (**Constitution**) which overrides both domestic legislation, common law principles, and the Bermuda Human Rights Act 1981 (**HRA**). Chapter 1 of the Constitution expressly establishes that every person in Bermuda is entitled to protection for the privacy of their home and other property, subject to respect for the rights and freedoms of others and for the public interest.

PIPA expressly states that if its provisions are inconsistent or in conflict with a provision of another enactment, PIPA will prevail unless it is inconsistent with or in conflict with a provision in the HRA, in which case, the HRA will prevail.

1.2. Supervisory authority

1.2.1. Who is responsible for enforcing the law(s) and issuing guidelines?

The Office of Privacy Commissioner for Bermuda (**PrivCom**).

1.2.2. How can the supervisory authority be contacted?

Name: PrivCom

Address: Maxwell Roberts Building, 4th Floor,1 Church Street, Hamilton, HM 11, Bermuda

Email/Online contact form: privcom@privacy.bm (General), investigations@privacy.bm (Reporting Privacy Concern)

Phone: 1-441-543-7748

Website: https://www.privacy.bm/

1.2.3. What are the powers of the supervisory authority?

PrivCom is responsible for monitoring how PIPA is administered and is empowered with extensive statutory powers to meet its statutory mandate, as follows:

Investigation and resolution of complaints:

- conduct investigations or inquiries concerning compliance with PIPA; and
- attempt to resolve complaints by negotiation, conciliation, mediation, or otherwise.

Education and industry guidance:

- comment on the implications for the protection of personal information in relation to an organization's existing or proposed programs;
- approve Binding Corporate Rules (**BCRs**) for transfers of personal information to an overseas third party;
- give guidance and recommendations of general application to an organization on matters relating to its rights or obligations under PIPA; and
- establish or assist with the establishment of certification mechanisms and associated rules for the purpose of demonstrating compliance with PIPA (and may, without prejudice to their tasks and powers, delegate the operation of a certification mechanism to an independent certification body with the appropriate level of expertise in relation to the protection of personal information).

*BCRs are defined by PIPA as personal information protection policies approved by the Privacy Commissioner which are adhered to by an organization for transfers or sets of transfers of personal information

Orders and enforcement activity:

- issue formal warnings, admonish an organization, and bring to its attention any failure by the organization to comply with PIPA;
- agree on a course of action with an organization;
- issue orders in connection with inquiries and permit an organization to transfer personal information to an overseas third party (for use either on behalf of the organization or for that overseas third party's own business practices) where the organization has reasonably demonstrated that it is unable to comply with PIPA's statutory procedure for organizations to assess the level of protection provided by an overseas third party for personal information (provided the transfer does not undermine the rights of the individual); and
- authorize an organization to disregard one or more requests for access to personal information, medical records, or rectification, blocking, erasure, or destruction of personal information if the requests would unreasonably interfere with the operations of the organization or amount to an abuse of the right to make those requests, because of their repetitious or systematic nature or are otherwise frivolous or vexatious.

Sanctioning powers

On completing an inquiry, PrivCom must dispose of the matters by making an order or issuing a formal warning or public admonishment. If the inquiry relates to an organization's decision to give or refuse to give access to all or part of an individual's personal information, the Privacy Commissioner may, by order:

- direct the organization to give the individual access to all or part of their personal information that is under the control of the organization;
- confirm the decision of the organization;
- require the organization to reconsider its decision concerning access; or
- direct the organization to refuse the individual access to all or part of their personal information.

If the inquiry relates to any other matter, the Privacy Commissioner may, by order, do one or more of the following:

- confirm that a PIPA obligation imposed on an organization has been performed;
- require that a PIPA obligation imposed on an organization be performed (including requiring an organization to take specific steps to remedy a breach of the legislation);
- confirm that a right set out in PIPA has been observed;
- require that a right set out in PIPA be observed;
- confirm an organization's decision not to correct, erase, delete, or destroy personal information;
- specify that personal information is to be corrected, erased, deleted, or destroyed by an organization and:
    - how such personal information is to be corrected, erased, deleted, or destroyed; and
    - may, if reasonably practicable, require the organization to notify third parties to whom the personal information has been disclosed of the correction, erasure, deletion, or destruction;
- require an organization to stop using personal information in contravention of PIPA;
- confirm a decision of an organization to use personal information;
- require an organization to destroy personal information used contrary to PIPA; and
- require an organization to provide specific information to persons in the event of a breach of security.

The Privacy Commissioner may, alternatively, make an order as they consider appropriate or may issue a formal warning or public admonishment if the above-mentioned orders would not be applicable.

A copy of the above-mentioned order may be filed with the Registrar of the Supreme Court of Bermuda and, after filing, the order is enforceable as a judgment or order of that court.

1.2.4. Has the supervisory authority released an annual report?

The Privacy Commissioner, not PrivCom, is subject to a statutory requirement to prepare an annual report. This must occur within six months after the end of each calendar year and focus on the work of PrivCom and any other matters relating to the protection of personal information which the Privacy Commissioner considers appropriate. The Privacy Commissioner is further responsible for ensuring that copies of that annual report are laid before each House of the Legislature.

From time to time, the Privacy Commissioner may also lay copies of a report before House of the Legislature with respect to their functions as the Privacy Commissioner as they see fit.

As PIPA only came fully into force on January 1, 2025, it is anticipated that the first annual report will be issued by the Privacy Commissioner in the second half of this year.).

1.3. Guidelines

1.3.1. Have any guidelines been issued on personal data protection?

Several guidelines, tools, templates and codes of conduct pertaining to the use and safeguarding of personal information have been issued by a number of regulators in Bermuda.

Mostly recently (March 7, 2025), the Privacy Commissioner issued its Final Report on the Financial Service Provider's Guidance Notes (the Financial Services Guidance).

PrivCom has also issued non-sector specific guidance and tools, such as:

- Privacy in the Workplace Guidance (August 2024);
- Guidance on vendors, third parties, and overseas data transfers (March 2021) (the **Data Transfers Guidance**); and
- Guide to PIPA (October 2024)

There are a number of regulatory authorities and postholders in Bermuda that have statutory authority to issue guidance/have issued guidance pertaining to cyber and data protection, inclusive but not limited to:

- Privacy Commissioner: The Privacy Commissioner is statutorily empowered to give guidance and recommendations of general application to an organisation on matters relating to its rights or obligations under PIPA. The post is further empowered to issue guidance about compliance with PIPA relating to good and bad practice by organisations.
- ICT Policy Minister: PIPA establishes that the ICT Policy Minister may, in consultation with the Privacy Commissioner, prescribe fees to be charged by organisations for the administration of data rights requests for access to personal information and access to medical records. As of the date of the drafting of this guidance, the ICT Policy Minister has not prescribed any such fees. The ICT Policy Minister will be required to issue codes of practice, after consultation with PrivCom, with best practice advice for organizations generally, or for specific types of organizations, to comply with PIPA. PrivCom may also be consulted by the ICT Policy Minister in connection with the Minister's passing of general regulations for the carrying out of, or giving effect to the purposes of, PIPA. As of the date of the drafting of this guidance, the ICT Policy Minister has not issued any such guidance.
- Bermuda Monetary Authority: The Bermuda Monetary Authority (BMA) has various codes of conduct applicable to specific licensees (inclusive of Insurance, Corporate Service Providers, Trust Companies, Money Service Businesses, Investment Businesses, Fund Administration Providers, Banks, and Deposit Companies) pertaining to data protection and cyber security. Most recently, the BMA have issued a consultation paper 'Operational Resilience and Outsourcing Code' which is supported by guidance notes.

SCOPE & APPLICABILITY

2.1. Personal scope

2.1.1. Who does the law(s) apply to?

PIPA applies to every organization 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 (Section 3 of PIPA).

An 'organization' is defined by the statute as any individual, entity, or public authority that uses personal information, and an 'individual' is defined as a natural person (PIPA, Section 2 of PIPA). 'Use' or 'using', in relation to personal information, is defined by the statute as carrying out any operation on personal information, including collecting, obtaining, recording, holding, storing, organising, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or otherwise making available, combining, blocking, erasing or destroying it.

2.1.2. What sector(s) does the law(s) apply to?

PIPA applies to the private sector, public, sector, third sector as well as any individual 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.

2.1.3. Who is afforded protections under the law(s)?

Individuals (i.e. natural persons) are afforded protections and rights under PIPA.

2.1.4. Does the law(s) apply to deceased persons?

PIPA does not apply to personal information about an individual who has been deceased for at least 20 years.

2.1.5. Does the law(s) apply to residents?

PIPA applies to residents of Bermuda.

2.1.6. Are there any exemptions?

PIPA establishes a series of statutory 'exclusions' and 'exemptions'.

Certain uses of personal information are excluded from the regulatory scope of PIPA, inclusive of:

- the use of personal information for personal or domestic purposes;
- the use of personal information 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;
- the use of business contact information for the purpose of contacting an individual in their capacity as an employee or official of an organization;
- personal information about an individual who has been dead for at least 20 years;
- personal information about an individual that has been in existence for at least 150 years;
- personal information transferred to an archival institution where access to the personal information was unrestricted or governed by an agreement between the archival institution and the donor of the personal information before the coming into operation of PIPA.
- personal information contained in a court file and used by a judge of any court in Bermuda or used as part of judicial administration or relating to support services provided to the judges of any court in Bermuda, but only where such personal information is necessary for judicial purposes;
- personal information contained in a personal note, communication or draft decision created by or for an individual who is acting in a judicial, quasi-judicial or adjudicative capacity; and
- personal information used by a member of the

House of Assembly or the Senate where such use relates to the exercise of their political function and the personal information is covered by parliamentary privilege.

In certain circumstances, organizations falling within the scope of certain statutory 'exemptions' are able to rely on the same to reduce the extent to which they are required to comply with PIPA:In PrivCom's Guide to PIPA, the regulator explains the effect of PIPA's exclusions and exemptions as follows:

- National security exemption: Upon successful reliance on this exemption, except for the minimum requirements, Parts 2 and 3 of PIPA will not apply to the use of personal information required for the purpose of safeguarding national security.
- Communication provider exemption: An organization that acts as a communication provider and its directors, officers, or authorized agents are not liable under PIPA for any breach committed while acting as a communication provider. A 'communication provider' is defined by PIPA as an internet service provider, telecommunications, and such other organization that acts as a conduit for personal information transmitted by a third party and who does not determine the purpose of using that personal information.
- Regulatory activity and honours exemption: Upon successful reliance on this exemption, except for the minimum requirements, Parts 2 and 3 of PIPA will not apply to the use of personal information if such use is required for the purposes of discharging functions to which the exemption applies to the extent to which the application of those Parts would be likely to prejudice the proper discharge of those functions.
- General exemption: Upon successful reliance on this exemption, except for the minimum requirements, Parts 2 and 3 of PIPA do not apply to the use of personal information in any case where such use is required for:
    - the prevention or detection of crime and compliance with international obligations regarding the detection, investigation and prevention of crime;
    - the apprehension or prosecution of offenders;
    - the assessment or collection of any tax or duty;
    - the prevention, investigation, detection and prosecution of breaches of ethics for regulated professionals; or
    - the economic or financial interests of Bermuda, including monetary, budgetary and taxation matters, compliance with international tax treaties and any monitoring, inspection or regulatory function exercised by official authorities for monetary, budgetary and taxation purposes in Bermuda, to the extent that the application of those Parts would be likely to prejudice any of those matters.

'Minimum requirements' refers to the requirements in Sections 5, 8, 11, 12, and 13 of PIPA.

In PrivCom's Guide to PIPA, the regulator explains the effect of PIPA's exclusions and exemptions as follows:

"Depending on how an organization uses personal information, there are three basic levels of privacy programme compliance with PIPA:

- *full compliance, meaning PIPA applies fully to how an organization uses personal information;*
- *partial exemption for uses of personal information that are exempt under Sections 22 (National security exemption), 24 (Regulatory activity and honours exemption), and 25 (General exemption).*
- *Uses of personal information are usually only exempt from provisions of PIPA to the extent that PIPA would interfere with the intended purpose. The minimum requirements still apply; and*
- *no compliance is required for uses of personal information that are excluded under Section 4 Exclusions."*

2.2. Territorial scope

2.2.1. What is the territorial scope of the law(s)?

The territorial scope of PIPA is not restricted to only residents of Bermuda. Notably, the statute is not concerned with the residence, domicile, or geographic location of the individual whose personal information is being used.

This approach reflects Bermuda's positioning as both an international centre for business and an attractive tourist destination. Business and vacation travellers to Bermuda will likely provide their personal information to a number of organizations inclusive of accommodation providers, retailers, restaurants, as well as emergency and medical service providers. Moreover, the nature of commercial arrangements often involves the use of personal information in multiple jurisdictions.

In this respect, Section 3.1 of the Financial Services Guidance confirms:

'PIPA does not expressly state that in order for an individual to benefit from the enactment of PIPA that the individual whose personal information is being used in Bermuda must possess Bermudian citizenship, be domiciled in Bermuda, or be a resident of Bermuda. Regardless of the origin of the personal information, or whether the individual to whom the personal information relates is a resident of Bermuda, so long as an organization 'uses' personal information in Bermuda it may be argued that the organization has an obligation to ensure compliance with PIPA.'

The Financial Services Guidance also observes:

- *'For the avoidance of doubt, the application of PIPA is not exclusively tied to the question of whether an organization is domiciled or physically operating in Bermuda. The applicable scope of PIPA does not expressly require an organization to be physically operating from or within Bermuda.'*
- *'Whether a parent company is physically headquartered and/or domiciled in Bermuda, or one of its subsidiaries are, is not the singular factor when considering the application of PIPA. So long as an organization 'uses' or is found to be 'using' personal information in Bermuda, the organization shall fall under the scope of PIPA. Consequently, if an organization is virtually operating in Bermuda and in doing so 'uses' personal information to facilitate commercial and/or administrative activities, it may be argued that the organization is required to ensure compliance with PIPA.'*
- *'While accessing personal information would legally satisfy the definition of 'use' under section 2 of PIPA, merely having the potential to access personal information does not amount to the carrying out of an operation on or the 'use' of the personal information. So long as the potential to access and 'use personal information is not realized, an organization with unrealized 'use' would not fall under the remit of PIPA until the personal information in question is used in accordance with Section 2 of PIPA'*
- *'If an organization establishes its corporate headquarters in Bermuda and subsequently uses personal information in Bermuda, the organization's headquarters would fall within the scope of PIPA. The Economic Substance Regulations 2018 (the ESR) may serve as a useful guide when determining the application of PIPA with respect to complex corporate structures.'*

2.2.3. Does the law(s) apply to citizens living abroad?

PIPA is not concerned with the residence, domicile, or geographic location of the individual whose personal information is being used. It is focused on regulating the use of personal information in Bermuda.

Accordingly, if an organization is using the 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, it is irrelevant whether the personal information pertaining to an individual resident in Bermuda or living abroad. The extent to which PIPA will apply to the respective use of that personal information will be dependent on:

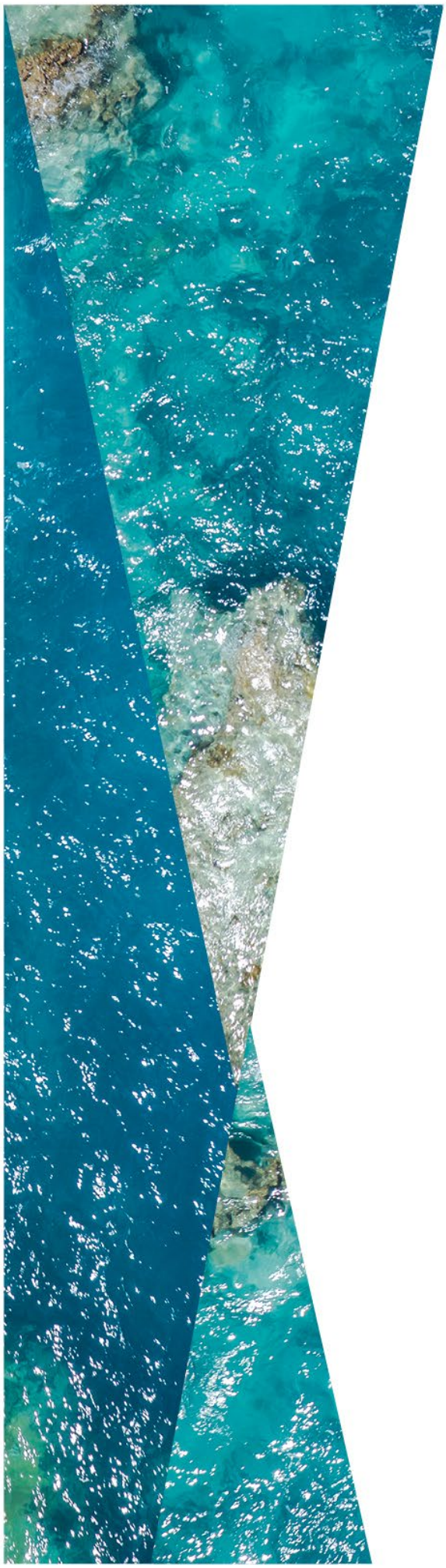
- whether the activity in question is excluded from PIPA's regulatory scope; and
- whether the organization can successfully rely on one or more exemptions in PIPA.

2.3. Material scope

2.3.1. What is the material scope of the law(s)?

PIPA applies:

- to organizations (any individual, entity or public authority)
- that carry out any operation (including collecting, obtaining, recording, holding, storing, organizing, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or other-



-wise making available, combining, blocking, erasing or destroying it);

- on personal information (any information about an identified or identifiable individual);
- on sensitive personal information (any personal information relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information), inclusive of medical records (personal information of a medical or psychiatric nature relating to the individual and personal information kept for the purposes of, or obtained in the course of, the carrying out of social work in relation to the individual); and
- 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 forms, or is intended to form, part of a structured filing system.

2.3.2. Does the law(s) apply to anonymized data?

In connection with the transfer of personal information to an overseas third party, PrivCom has confirmed that if an organization anonymizes personal information so that it is never possible to identify individuals, it is not personal information. On this basis, PrivCom has advised organizations that PIPA transfer restrictions do not apply and they are free to transfer the anonymized information outside of Bermuda.

This guidance would suggest that PIPA does not regulate anonymized information, however, the jurisdiction awaits conclusive guidance on this point from PrivCom.

DEFINITIONS

3.1. Key terms

3.1.1. How is data controller (or equivalent) defined?

There is no statutory term or corresponding definition for 'data controller' in PIPA. Instead, PIPA adopts the statutory term 'organization' which is broadly defined as any individual, entity, or public authority that uses personal information.

3.1.2. How is data processor (or equivalent) defined?

There is no statutory term or corresponding definition for 'data processor' in PIPA. Instead, PIPA adopts the statutory term 'organization' which is broadly defined as any individual, entity, or public authority that uses personal information.

3.1.3. How is data subject (or equivalent) defined?

PIPA adopts the term 'individual' which is defined as a natural personal. The statute further adopts the term 'applicant' which refers to an individual who makes a written request to an organization to exercise a statutory right of an individual established by PIPA (access to, correction, blocking, erasure, and destruction of personal information) in accordance with the statutory procedures established in that statute.

3.1.4. How is processing (or equivalent) defined?

PIPA adopts the terminology of 'use' or 'using' which, in relation to personal information, is defined broadly by PIPA as carrying out any operation on personal information, including collecting, obtaining, recording, holding, storing, organising, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or otherwise making available, combining, blocking, erasing or destroying it.

3.1.5. How is the sale of personal data defined?

There is no definition for the sale of personal information however PIPA expressly does confirm that the statutory procedures which are advantageous for organizations involved in business transactions do not apply to a business transaction where the primary purpose, objective or result of the transaction is the purchase, sale, lease, transfer, disposal or disclosure of personal information.

3.1.6. How is the sharing of personal data defined?

PIPA does not adopt a stand-alone definition for the sharing of personal information. Such activity would fall within the broader PIPA definitions of 'use' or 'using' which, in relation to personal information, are defined as carrying out any operation on personal information, including obtaining, transferring, disclosing, disseminating or otherwise making it available, amongst other activities involving personal information.

3.1.7. How is personal data defined?

PIPA defines 'personal information' as any information about an identified or identifiable individual.

3.1.8. How is sensitive data defined?

PIPA defines ‘sensitive personal information' is any personal information relating to an individual's place of origin, race, color, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information.

3.1.9. How is biometric data defined?

PIPA defines ‘biometric information' as any information relating to the physical, physiological, or behavioral characteristics of an individual which allows their unique identification, such as facial images or fingerprint information.

3.1.10. How is health data defined?

There is no definition for 'health data' in PIPA. The statute, however, does regulate the use of 'genetic information' which is defined by the statute as all personal information relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual resulting, in particular, from an analysis of a biological sample from the individual in question.

PIPA also establishes a separate statutory procedure for medical records in the context of an access request by a data subject (an applicant). Medical records, in this context, are described as 'personal information of a medical or psychiatric nature relating to the individual' or 'personal information kept for the purposes of, or obtained in the course of, the carrying out of social work in relation to the individual.'

3.1.11. How is pseudonymized/de-identified data defined?

There is no definition for 'pseudonymization' in PIPA.

3.1.12. How is anonymized data defined?

PIPA does not adopt a definition for 'anonymization' or 'anonymized data'. However, the Guide to PIPA issued by PrivCom does confirms the regulatory impact of the anonymization of personal information. In the scenario where a Bermuda-based company passes information about its employees to its US parent company in connection with the centralized human resource service in the US, if the Bermuda-based organization anonymizes personal information so that it is never possible to identify individuals, it is not classified as personal information. The outcome, according to the PrivCom guidance, is that the restrictions imposed in PIPA for the transfers of personal information to an overseas third party do not apply and the Bermuda-based organization is free to transfer the anonymized information outside of Bermuda.

The Guide to PIPA, further refers to the process of anonymization in a number of other contexts, such as:

- **purpose limitation**: as a safeguard for the protection of personal information; and
- **proportionality:** in connection with the periodic review which organizations should undertake in respect of the personal information they hold and the organization's decisions to erase or anonymize it when they no longer need it.

3.1.13. How is profiling defined?

In 2022, PrivCom published an article titled 'IWD2022: Empowerment for Women through Privacy Regulations, May 2022' focusing on automated decision-making and profiling within the context of privacy and technology concerns that affect women. This article confirmed that although rights against automated decision-making and profiling are not explicitly mentioned in PIPA, these rights are essentially implied in the wording of the legislation.

PrivCom has confirmed its expectation that organizations must identify the purpose and legal condition under which they use information (such as by requesting an individual's consent, and in order to get that consent, the organization would have to explain its profiling or automated decision-making processes). In addition, PrivCom underscores that PIPA often restricts the use of personal information to when it is "necessary" to accomplish a purpose, and often automated decision-making or profiling may not be strictly necessary.

In the context of its article, PrivCom adopts the following definitions:

- 'automation' is the term used to describe the wide range of technologies that minimise human intervention in processes, such as predetermining decision criteria, subprocess relationships, and self-service checkout machines;
- 'decision algorithms' are mathematic equations designed by developers who use mathematical models to make decisions; and
- 'profiling' refers to the collection and use of data to evaluate specific aspects or characteristics of an individual. The purpose is to predict the individual's behaviour and make decisions to affect it.

DATA PROCESSING PRINCIPLES

4.1. Principles

4.1.1. Does the law(s) provide data processing principles?

Yes, PIPA does establish a series of data protection principles as follows:

- **Fairness** (Section 8 of PIPA): An organization must use personal information in a lawful and fair manner
- **Purpose Limitation** (Section 10 of PIPA): An organization must use personal information
    - only for the specific purposes identified in an organization's privacy notice for which personal information is or might be used: and
    - for purposes that are related to those specific purposes. This requirement, however, will not apply in the following scenarios:
        a) when the use of the personal information is with the consent of the individual whose personal information is used;
        b) when the use of the personal information is necessary to provide a service or product required by the individual;
        c) where the use of personal information is required by any rule of law or by the order of the court;
        d) where the use of the personal information is for the purpose of detecting or monitoring fraud or fraudulent misuse of personal information; or
        e) where the personal information is used for the purposes of scientific, statistical, or historical research, subject to the appropriate safeguards for the rights of the individual.

    Proportionality (Section 11): An organization must ensure that personal information is adequate, relevant, and not excessive in relation to the purposes for which it is used.
- **Integrity of Personal Information** (Section 12): An organization must ensure that any personal information used is accurate and kept up to date to the extent necessary for the purposes of use. An organization must further ensure that personal information for any use is not kept for longer than is necessary for that use.

4.1.2. Does the law(s) require the implementation of Data Protection by Design?

Yes, Section 5 of PIPA requires that every organization must adopt suitable measures and policies to give effect to its obligations and to the rights of individuals set out in the legislation. Those measures and policies must be *designed* to take into account the nature, scope, context, and purposes of the use of personal information and the risk to individuals from the use of personal information. In meeting its responsibilities under PIPA, an organization must act in a reasonable manner.

This data protection concept of 'privacy by design' falls within the statutory 'minimum requirements' established by PIPA (i.e., the requirements of Sections 5, 8,11,12, and 13 of PIPA). Should an organization successfully rely on an exemption set out in PIPA, the minimum requirements of Parts 2 and 3 of PIPA will still apply to regulate the use of personal information.

In providing this response, the author has relied on the definition of the European Commission for 'privacy by design': "*Companies/organizations are encouraged to implement technical and organizational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles right from the start (data protection by design).*"" In this context, the example provided by the European Commission of 'data protection by design' is the use of pseudonymization and encryption.

4.1.3. Does the law(s) require the implementation of Data Protection by Default?

Yes, as stated above, Section 5 of PIPA requires that every organization must adopt suitable measures and policies to give effect to its obligations and to the rights of individuals set out in the legislation. Those measures and policies in must be designed to take into account the nature, scope, context and purposes of the use of personal information and the risk to individuals by the use of the personal information. In meeting its responsibilities under PIPA, an organization must act in a reasonable manner.

Moreover, Section 13 of PIPA requires that organizations must protect personal information that they hold with appropriate safeguards against risk, including:

- loss;
- unauthorized access, destruction, use, modification, or disclosure; or
- any other misuse.

Such safeguards must be proportional to:

- the likelihood and severity of the harm threatened by the loss, access, or misuse of the personal information;
- the sensitivity of the personal information (including, in particular, whether it is sensitive personal information);
- the context in which it is held; and
- must be subject to periodic review and reassessment.

This data protection concept of 'privacy by default' falls within the statutory 'minimum requirements' established by PIPA (i.e., the requirements of Sections 5, 8, 11, 12, and 13 of PIPA). Should an organization successfully rely on an exemption set out in PIPA, the minimum requirements of Parts 2 and 3 will still apply to regulate the use of personal information.

In providing this response, the author has relied on the definition of the European Commission for 'privacy by default': '*Companies/organizations should ensure that personal data is processed with the highest privacy protection (for example, only the data necessary should be processed, short storage period, limited accessibility) so that by default, per-*

-sonal data isn't made accessible to an indefinite number of persons (data protection by default).'

In this context, the example provided by the European Commission of 'data protection by default' is that a social media platform should be encouraged to set users' profile settings in the most privacy-friendly setting by, for example, limiting from the start the accessibility of the users' profile so that it isn't accessible by default to an indefinite number of persons.

4.1.4. Does the law(s) require the implementation of requirements regarding the retention of data?

PIPA does not expressly implement requirements for the retention of personal information (such as the development of retention schedules). However, PIPA does adopt the data protection principle of proportionality (i.e. that an organization must ensure that personal information is adequate, relevant and not excessive in relation to the purposes for which it is used) and, in practice, it may be difficult for organizations to evidence compliance with this section as well as other requirements of PIPA in the absence of adopting retention schedules.

Notably, PrivCom has issued a Data Retention and Destruction Schedule Template and its Guide to PIPA directly considers an organization's adherence to the proportionality requirement and sets out a checklist for organizations to consider.

In connection with determinations as to whether an organization is acting in good faith, PrivCom has confirmed that two principles of its regulatory strategy are constructive engagement with the community and promotion of interoperable best practices across legal jurisdictions.

In this respect, PrivCom has confirmed that, at times, it may make sense for an organization to refer to the guidance from other jurisdictions, and if an organization proactively bases its actions on best practices, even those from beyond our shores, its office will likewise give credit for such good faith efforts.

The Mid-Atlantic Privacy Compass

Proportionality, Guide to PIPA

CCTV Privacy Risks and Best Practices

PrivCom Tool: Retention & Destruction Schedule

LAWFUL BASES

Non-special category personal data

5.1.1. Is a lawful basis required for the processing of non-special category personal data?

Yes, PIPA establishes that (with limited exceptions) an organization may use an individual's personal information only if one or more of the following conditions are met:

- the personal information is used with the consent of the individual where the organization can reasonably demonstrate that the individual has knowingly consented;
- a reasonable person giving due weight to the sensitivity of the personal information, would consider that the individual would not reasonably be expected to request that the use of their personal information should not begin or cease, and that the use does not prejudice the rights of the individual;
- the use of the personal information is necessary for the performance of a contract to which the individual is a party or for the taking of steps at the request of the individual with a view to entering into a contract;
- the use of the personal information is pursuant to a provision of law that authorizes or requires such use;
- the personal information is publicly available information and will be used for a purpose that is consistent with the purpose of its public availability;
- the use of the personal information is necessary to respond to an emergency that threatens the life, health, or security of an individual or the public;
- the use of the personal information is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the organization or in a third party to whom the personal information is disclosed; or
- the use of the personal information is necessary in the context of an individual's present, past, or potential employment relationship with the organization.

Where an organization transfers personal information to an overseas third party, in addition to complying with the above-mentioned requirements, the organization must also meet the specific obligations imposed for such overseas transfers.

5.1.2. Is further processing of personal data allowed?

Yes, if an organization is unable to meet any of the primary conditions of use established in Section 6(1) of PIPA, then the organization may use personal information only if:

- the personal information was collected from, or is disclosed to, a public authority which is authorized or required by a statutory provision to provide the personal information to, or collect it from, the organization;
- the use of personal information is for the purpose of complying with an order made by a court, individual, or body having jurisdiction over the organization;
- the use of the personal information is for the purpose of contacting the next of kin or a friend of an injured, ill or deceased individual;
- the use of the personal information is necessary in order to collect a debt owed to the organization or for the organization to repay to the individual money owed by the organization;
- the use of the personal information is in connection with disclosure to the surviving spouse or a relative of a deceased individual if, in the reasonable opinion of the organization, the disclosure is appropriate; and
- the use of personal information is reasonable to protect or defend the organization in any legal proceeding.

Where an organization transfers personal information to an overseas third party, in addition to complying with the afore-mentioned requirements, the organization must also meet the specific obligations imposed for such overseas transfers.

5.2. Consent

5.2.1. Can personal data be processed on the basis of consent?

Yes, as stated above, PIPA establishes that an organization may use an individual's personal information if the personal information is used with the consent of the individual, where the organization can reasonably demonstrate that the individual has knowingly consented.

5.2.2. How is consent defined?

For the purpose of relying on consent as a condition for the use of personal information, PIPA requires that an organization provide clear, prominent, easily understandable, accessible mechanisms for an individual to give consent in relation to the use of their personal information.

5.2.3. What types of consent are accepted?

The statutory language of PIPA is broad enough to cover scenarios involving express, deemed, and implied consent, and it will be a matter for organizations to decide which form of consent is reasonably for the organization to rely on, and in some circumstances, this may be dependent on the knowledge of the individual concerned.

Notably, PIPA provides for the following scenarios:

- the personal information is used with the consent of the individual where the organization can reasonably demonstrate that the individual has knowingly consented. An organization will typically be required to provide clear, prominent, easily understandable, accessible mechanisms for an individual to give consent in relation to the use of their personal information. However:
- when an individual consents to the disclosure of their personal information by an intermediary for a specified purpose, that individual will be deemed to have consented to the use of that personal information by the receiving organization for the specified purpose; and
- if an individual has an interest in or derives a benefit from coverage or enrolment under an ins-
-urance, trust, benefit or similar plan, the individual will be deemed to have consented to the use of their personal information for the purpose of the plan.

PrivCom has also issued guidance that discusses implied or passive consent and provided the following views:

- Implied, or passive, consent does not require specific action – there is no checkbox to mark or paper to sign;
- Example One: There could be a sign at the entrance to a building stating that surveillance cameras are in use. Entering the premises implies the individual gives consent to be recorded;
- Example Two: A business includes language in a privacy notice stating that it collects personal information as part of a specific service, process, or programme; for example: 'By downloading this program, you consent to the collection of information about you and your activities for the purpose of X';
- For implied consent to be valid, the organization must have notified the individual about the purposes, and the implication must be reasonable; and
- Importantly, implied consent cannot be relied upon for uses of sensitive personal information.

5.2.4. What constitutes valid consent?

This is not a specific subject which is addressed by PIPA however, it is the subject of guidance from PrivCom. In this regard, PrivCom has confirmed that consent should be obvious and require a positive action to opt in.

PrivCom has also recommended:

- keep your consent requests separate from other terms and conditions;
- get separate consent for separate things. vague or blanket consent is not enough; and
- it is good practice to avoid making consent to processing a precondition of a service.

5.2.5. How long is consent valid for?

This is not a specific subject which is addressed by PIPA however it is the subject of guidance from

PrivCom. In this regard, PrivCom has confirmed that there is no set time limit for consent. How long it lasts will depend on the context. Organizations should review and refresh consent as appropriate.

5.3. Performance of a contract with the data subject

5.3.1. Can personal data be processed on the basis of performance of a contract with the data subject?

Yes, PIPA permits personal information being used by an organization in order to effect the performance a contract with the individual concerned.

5.3.2. Which specific conditions must be fulfilled to rely on this lawful basis?

There are a number of conditions of use established by PIPA in this context, as follows:

- the use of the personal information is necessary for:
    - the performance of a contract to which the individual is a party; or
    - for the taking of steps at the request of the individual with a view to entering into a contract;
    - the use of the personal information is necessary in the context of an individual's present, past or potential employment relationship with the organization; and
    - an individual will be deemed to have consented to the use of their personal information for the purpose of coverage or enrolment under an insurance, trust, benefit or similar plan if the individual has an interest in or derives a benefit from that plan.

5.4. Legal obligations

5.4.1. Can personal data be processed on the basis of a legal obligation?

Yes, PIPA permits personal information to be used by an organization on the basis of a legal obligation.

5.4.2. Which specific conditions must be fulfilled to rely on this lawful basis?

The exact language of the conditions of use established by PIPA in this regard are:

- 'the use of the personal information is pursuant to a provision of law that authorises or requires such use; or
- the use of the personal information is for the purpose of complying with an order made by a court, individual, or body having jurisdiction over the organization.

5.5. Interest of the data subject

5.5.1. Can personal data be processed on the basis of the interest of the data subject?

Yes, PIPA permits personal information to be used by an organization on the basis of the interest of the individual.

5.5.2. Which specific conditions must be fulfilled to rely on this lawful basis?

The exact language of the condition of use established by PIPA in this regard is 'except in relation to sensitive personal information, a reasonable person giving due weight to the sensitivity of the personal information would consider that:

- the individual would not reasonably be expected to request that the use of their personal information should not begin or cease; and
- that the use does not prejudice the rights of the individual'.

If an organization is unable to meet this condition of use, it may still be able to lawfully use personal information if

- the use of the personal information is for the purpose of contacting the next of kin or a friend of an injured, ill or deceased individual; or
- the use of the personal information is in connection with disclosure to the surviving spouse or a relative of a deceased individual if, in the reasonable opinion of the organization, the disclosure is appropriate.

5.7. Legitimate interest

5.7.1. Can personal data be processed on the basis of legitimate interest?

PIPA does not expressly provide for the use of personal information on the basis of legitimate interest, however, it is intended that a provision of PIPA operates analogously to the 'legitimate interest provisions' found under Article 6(1)(f) of the GDPR.

Section 6(1)(b) of PIPA

Article 6(1)(f) of the GDPR

Section 5 of the Financial Services Guidance

5.3.2. Which specific conditions must be fulfilled to rely on this lawful basis?

PIPA provides that, except in relation to sensitive personal information, an organization can use personal information where a reasonable person giving due weight to the sensitivity of the personal information would consider:the use of the personal information is necessary for:

- that the individual would not reasonably be expected to request that the use of their personal information should not begin or cease; and
- that the use does not prejudice the rights of the individual.

PrivCom has confirmed that this section of PIPA "operates analogously to the legitimate interest provisions found under Article 6(1)(f) of the GDPR. However, the legal provisions stipulated under PIPA are not identical to those found under the GDPR. Therefore, careful consideration must be paid to account for these technical and administrative nuances."

PrivCom has further confirmed that: *"Upon review of section 6(1)(b) of PIPA, in order for an organization to rely on implied consent as a lawful condition to 'use' personal information, the organization must take into account the reasonable expectations of the individual and whether the organization is reasonable in evaluating that expectation and any potential impact on individual rights under Part III of PIPA."*

"This approach can be contrasted with Article 6(1)(f) of the GDPR, which 'expressly considers the legitimate commercial interests being pursued. Should said legitimate interest direct conflict with an individual's fundamental rights and freedoms, such interests shall be nullified and overridden."

Recognizing this legislative nuance, PrivCom has advised that an organization should be prepared to demonstrate through its administrative processes that it has acted in such a way that accounts for the aforementioned PIPA requirements: *"In summary, the question of whether an individual has consented to the use of personal information and whether consent is required is based on the facts of the matter and shall be determined on a case-by-case basis."*

5.8. Research

5.8.1. Can personal data be processed for research purposes?

Yes, PIPA permits personal information being used by an organization for research purposes.

5.8.2. Which specific conditions must be fulfilled to rely on this lawful basis?

PIPA expressly confirmed that its statutory requirement that an organization limit its use of personal information for the purposes identified to the data subject in its privacy notice and for purposes which are related to those, does not apply 'where the personal information is used for the purposes of scientific, statistical or historical research subject to the appropriate safeguards for the rights of the individual.'

PrivCom has confirmed in its recent guidance that such safeguards should expressly consider the sensitivity of the personal information and the inherent risk associated with 'using' personal information for the purposes of scientific, statistical or historical research. This expectation reflects the general security safeguarding requirements of PIPA.

5.9. Other lawful bases

5.9.1. Are there any additional lawful bases available for data processing?

All Section 6 PIPA conditions of use have been set out in the preceding responses.

Organizations seeking to process data on the basis that 'the personal information is publicly available information and will be used for a purpose that is consistent with the purpose of its public availability',

LAWFUL BASES

Special category personal data

6.1. Sensitive data

6.1.1. Is it permissible to process sensitive data?

Yes, PIPA permits the use of sensitive personal information subject to certain requirements. 'Sensitive personal information' is defined by the Bermuda regulatory framework as any personal information relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information.

6.1.2. Which lawful bases can be relied on for the processing of sensitive data?

Almost all of the conditions of use for personal information established by PIPA (and discussed above) can be relied upon for use of sensitive personal information by organizations. Organizations should, however, note the following:

- PIPA does not permit use of sensitive personal information in reliance on Section 6(1)(b) – i.e. that a reasonable person, giving due weight to the sensitivity of the personal information, would consider that the individual would not reasonably be expected to request that the use of their personal information should not begin or cease and that the use does not prejudice the rights of the individual;
- PIPA prohibits the use of sensitive personal information without lawful authority, if it would discriminate contrary to Part II of the HRA;
    - Part II of the HRA prohibits discrimination and sexual harassment on the basis of a protected characteristic (race, place of origin, colour, ethnic or national origins, sex or sexual orientation, marital status or domestic partnership status, disability, family status, religion or beliefs or political opinions, criminal record (except where there are valid reasons relevant to the nature of the particular offense for which the individual is convicted that would justify the difference in treatment) and age (does not apply in the area of employment)). It further establishes areas of protection. The main areas of protection under the HRA include employment, goods, facilities and services, and accommodation;
    - Sensitive personal information is used with lawful authority if and only to the extent that it is used:
        a) with the consent of any individual to whom the information relates;
        b) in accordance with an order made by either the court or the Privacy Commissioner;
        c) for the purpose of any criminal or civil proceedings; or
        d) in the context of recruitment or employment, where the nature of the role justifies such use.
- Where an organization transfers sensitive personal information to an overseas third party, in addition to complying with the obligations pertaining to general conditions of use, the organization must also meet the specific obligations imposed for such overseas transfers.

Sections 6, 7 and 15 of PIPA

Part II of the HRA

Digital Guidance from the Office of the Human Rights Commission for Bermuda

6.1.3. What constitutes valid consent for the processing of sensitive data?

There are no separate statutory requirements for consent in the context of the provided by PIPA for the use of sensitive personal information and, accordingly, organizations should refer to the general criteria for consent, as discussed in the responses above.

Guide to PIPA (Consent), October 2024

The content of this guide was originally published as part of the April 2025 Bermuda – Privacy Overview Guidance Note on the OneTrust DataGuidance platform for regulatory research pursuant to a contributor agreement between OneTrust DataGuidance and attorney contributor, Gretchen Tucker.

This guide is intended to provide a general overview of primary data protection legislation in Bermuda as of the date of its publication (April 2025) and does not address sectoral or cybersecurity law.

Specific legal advice should be sought for any matters pertaining to its subject matter and this article is not a substitute for the undertaking of legal advice by a Bermuda registered attorney.

BeesMont Law Limited