Privacy Commissioner
Bermuda | Quo Data Ferunt

FINANCIAL SERVICE PROVIDER'S GUIDANCE NOTES – FINAL REPORT

produced by the Office of the Privacy Commissioner for Bermuda (PrivCom)

07 March 2025

Table of Contents

1. Executive Summary

The Office of the Privacy Commissioner ("PrivCom") is responsible for regulating every organisation that uses personal information in Bermuda: (i) wholly or partly by automated means; and (ii) the use of personal information through automated means which form, or are intended to form, part of a structured filing system. In furtherance of this responsibility, PrivCom's regulatory activities are performed in accordance with the Personal Information Protection Act 2016 ("PIPA").

Bermuda's financial services industry is a highly regulated sector, where most licensed sectoral participants have developed highly sophisticated legal and compliance departments and operational risk committees that are accustomed to effectively addressing both legal and regulatory obligations. Prior to the enactment of PIPA on 1st January 2025, PrivCom proactively engaged with industry stakeholders of Bermuda's financial service sector to identify any areas of PIPA which lack clarity or give rise to regulatory overlap, inconsistencies or conflicts with respect to the administrative satisfaction of pre-existing regulatory reporting and performance obligations.

By adopting a proactive regulatory approach, PrivCom was able to: (i) identify industry specific related issues concerning Bermuda's financial service sector; (ii) provide related guidance; and (iii) actively support financial service providers in their implementation of appropriate operational and administrative practices that ensure compliance with PIPA and Bermuda's existing financial services regulatory framework regulated by the Bermuda Monetary Authority ("BMA").

The adoption of a collaborative effort with industry stakeholders is viewed by PrivCom as being an effective method within which it may reduce any perceived friction in the daily operation of financial services and the application and compliance with numerous domestic regulatory frameworks. Through its public consultation process PrivCom was able to:

- Establish constructive dialogue where concerns were communicated and addressed;
- Establish regulatory clarity and understanding of the commercial activities of Bermuda's financial service sector;
- Better understand how industry stakeholders are organizationally structured and the use of third-party affiliates;
- Develop a shared understanding of PrivCom's compliance expectations of PIPA and how industry stakeholders may satisfy these expectations;
- Identify the perceived challenges associated with the implementation of PIPA; and
- Share existing guidance notes and PrivCom's responses to frequently asked questions (FAQs).

By undertaking a public consultation process with Bermuda's financial service providers, PrivCom simultaneously strengthened industry stakeholder relationships while facilitating the creation of mutually beneficial regulatory relationships between PrivCom and various industry stakeholders.

In response to the stakeholder comments received following publication of the "Financial Service Provider's Guidance Notice – Consultation Document on 29th September 2025 (the "Consultation Document"), PrivCom produced the "Financial Service Provider's Guidance Notes - Final Report" (the "Final Report"), and has elected to undertake a fully comprehensive review of all prior PIPA Guidance Notes published by PrivCom (i.e. PIPA Guide and the Individual's Guide to PIPA) to ensure consistency (collectively referred to as the "PIPA Guidance Notes").

It is important to note that the PIPA Guidance Notes are not legally binding documents, that PrivCom is not bound by the PIPA Guidance Notes and nor do the PIPA Guidance Notes necessarily set out PrivCom's final or definitive position on any one particular matter. To the extent that there might be any inconsistency between the contents of the PIPA Guidance Notes and the operations of PrivCom and its due exercise of its regulatory functions, responsibilities and relevant objectives under PIPA, such guidance is without prejudice to the legal position of PrivCom.

2. Introduction

Bermuda's data protection legislative framework came into effect as of 1 January 2025. PrivCom has expressly considered how the enactment, implementation and enforcement of PIPA will impact one of Bermuda's most significant commercial sectors, namely financial services.

Under section 29 of PIPA the Commissioner of PrivCom is responsible for monitoring how PIPA is administered to ensure that its purposes are achieved. In pursuit of PrivCom's regulatory obligations the Commissioner elected to use his powers under PIPA to undertake a public consultation process and published the Consultation Document and this Final Report in accordance with section 29(c), (d), (i) and (o) of PIPA.

To ensure that PrivCom has a fully comprehensive understanding of the commercial impact PIPA may have on Bermuda's financial service providers, PrivCom actively engaged with industry stakeholders in order to identify the necessity for industry specific guidance, assistance, clarifications, or other regulatory measures that may be required to enable financial service providers to effectively adopt administrative practices which enable on-going compliance with PIPA.

Such stakeholder engagement included, but was not limited to, a review of how PIPA interacts with the existing regulatory legislative frameworks which govern the commercial activities of financial service providers operating from or within the islands of Bermuda. In conjunction with its review of Bermuda's financial service regulatory framework, PrivCom expressly considered associated financial services related legislative regulations, Ministerial Directions and Orders, supplementary statutory instruments, and industry specific codes of conduct.

Bermuda is a sophisticated, innovative, and comprehensively regulated jurisdiction for banks, deposit companies, investment firms, trust management firms, corporate service providers and insurance and reinsurance companies registered and domiciled in Bermuda. Due to the regulatory practices adopted by the Bermuda Monetary Authority ("BMA"), Bermuda's financial services industry has grown to become the largest contributor to Bermuda's local economy.

Given the significant role that financial service providers serve towards the continued growth of Bermuda's local economy, a collaborative and coherent regulatory approach between PrivCom, foreign data protection regulators, and domestic and global financial regulators will facilitate a mutually beneficial, symbiotic approach to data regulation. By adopting a collaborative approach with respect to data protection and regulatory enforcement, PrivCom is of the view that it is strategically positioned to effectively mitigate the risk of conflicting, divergent, and/or duplicative regulatory activities.

Examples of effective cross regulatory cooperation can be found in the United Kingdom ("UK"). In the UK, the Data Regulators Cooperation Forum (the "DRCF") has been created, without formal regulatory mandate, with the intention of providing a forum which allows UK's Information Commissioner's Office ("ICO"), the UK's Financial Conduct Authority ("FCA"), the UK's Competition and Markets Authority ("CMA") and the UK's Office of Communications ("OfCom") to come together to discuss, understand, share insights, and collaborate on guidance and enforcement of personal privacy and data related issues.

This arrangement reflects a long-standing co-existence of the different regulators, and an appreciation of the benefits for both the regulators and the regulated to have open communication and cooperation between the regulators. It is the intention of PrivCom to adopt a similar regulatory arrangement with both domestic and international regulatory authorities.

Appreciating the value in adopting a collaborative approach to regulation and data privacy protection, PrivCom recognizes that with the increased reliance on personal data in order for financial service providers to effectively facilitate domestic and global financial service products, data protection is an increasingly important and shared area of focus. Consequently, effective and efficient collaboration makes regulatory sense in order to establish strong lines of cooperation and communication with industry stakeholders.

Although the guidance provided in the Consultation Document and this Final Report is specifically focused on financial service providers and their obligation to comply with PIPA, many of the principles discussed in the Final Report will likely apply to most organisations using personal information. For further guidance please refer to the Guide to PIPA and the Individuals' Guide to PIPA.

2.1 Objective

PrivCom recognizes that Bermuda's financial service providers have historically been early adopters of innovative technology. Through the increased digitisation of their commercial activities, Bermuda's financial service providers have been able to:

- Better analyse, process, and manage industry specific data;
- Promote the continued development of financial products and services;
- Identify, manage and mitigate commercial and operational risk; and
- Comply with regulatory reporting and performance obligations.

Given Bermuda's financial services' heavy reliance on their ability to "use" personal data to provide financial services and drive continued commercial innovation and digitisation, the BMA's existing regulatory practices have consequently been revised in response. With the enactment of PIPA, PrivCom is of the view that it is prudent to identify areas of potential domestic regulatory overlap, inconsistencies, conflicts, or lack of clarity between obligations under PIPA and the regulatory framework enforced by the BMA.

As part of its preparation for the enactment of PIPA, PrivCom undertook a public consultation process by publishing the Consultation Document with the intention of promoting engagement with Bermuda's financial services sector and determining which sections of PIPA, if any, conflicted with the BMA's existing financial services laws, regulations, and codes of conduct.

By undertaking deliberate measures intended to identify areas of regulatory friction, overlap, or ambiguity, PrivCom has positioned itself to address these areas of concern through the creation of industry specific formal Guidance Notes, Memorandums of Understanding (MOUs) with regulators, or any other legal and regulatory mechanisms specifically intended to support an effective and efficient approach to data privacy and financial services regulation in Bermuda.

2.2 Consultation Process and Methodology

On 6th March 2023, PrivCom circulated a Consultation Letter to a number of financial service providers registered and licensed to operate within Bermuda (the "Consultation Letter"). The purpose of the Consultation Letter was to discuss with various members of Bermuda's financial service sector the regulatory obligations and performance requirements stipulated under PIPA and to understand how PIPA would likely impact their daily operations. The Consultation Letter intended to:

- Obtain feedback regarding areas of concern, or information gaps that PrivCom may need to address through the issuance of industry specific guidance notes; and
- Invite industry stakeholders to a meeting on the 25th of March 2024.

Following circulation of the Consultation Letter, financial service providers were invited to comment on the organisational impact of PIPA by the 15th ofMarch 2024. In response to the Consultation Letter, the feedback received paid particular attention to:

(i) The types of complex corporate structures that are adopted by financial service providers registered in Bermuda;
(ii) The types of financial service providers that may "use" personal information in Bermuda but do not physically operate in Bermuda; and
(iii) The transfer of personal information to overseas third parties.

Based on the commentary received, PrivCom recognizes that a number of legislative provisions under PIPA are clearly understood by Bermuda's financial service providers and are not likely to cause administrative difficulties. However, there were a number of legislative provisions under PIPA that

were identified as requiring further clarification to ensure a level of commercial understanding that facilitates compliance with PIPA.

During the meeting held on 25th March 2024, the following matters were discussed:

- The concerns raised by industry stakeholders in response to the Consultation Letter;
- The queries raised by stakeholders in response to PrivCom's existing FAQs and Guidance available on the PrivCom website (www.privacy.bm);
- The intersection of PIPA and the relevant Anti-Money and Anti-Terrorist ("AML-ATF") reporting obligations imposed by the BMA;[1]
- Matters requiring further clarification from PrivCom; and
- The communication of operational and administrative challenges faced by diverse types of industry participants (i.e. the range of services provided, the types of sensitive personal information collected, the intended use of sensitive personal information, and the nature and operational purpose of various types of corporate structures).

The purpose of the meeting held on the 25th of March 2024 was to afford PrivCom the ability to identify and create an action plan to address any areas of concern raised and to aid financial service providers in the development and implementation of administrative processes intended to ensure organisational compliance with PIPA.

While it was expected that the meeting held on the 25th March 2024 would result in the identification of some material areas of conflict, inconsistencies, or matters requiring further clarification, it was determined that due to the fully comprehensive structure of PIPA, PrivCom has avoided many of the challenges experienced by comparable foreign data privacy regulatory bodies at the time in which their respective data privacy legislative frameworks came into effect. Unlike PrivCom, many foreign regulatory privacy regimes operating in comparably complex financial service sectors experienced issues pertaining to the drafting and practical implementation of their respective data privacy legislative frameworks.

To address the matters which required further clarification, PrivCom arranged for the scheduling of additional in-person meetings to explore and discuss these topics in-depth. Some of the financial services providers who were invited by PrivCom to attend the in-person meetings consisted of industry stakeholders who were unable to attend the in-person meeting held on the 25th of March 2024. Following PrivCom's public engagement activities with industry stakeholders, PrivCom determined that the best mechanism to address the issues raised was to undertake a public consultation process and subsequently issue industry specific guidance notes.

To help facilitate the consultation process and prepare the Consultation Document, PrivCom engaged Vivienne Artz OBE, Senior Data Strategy & Privacy Policy Advisor to the Centre for Information Policy Leadership. Ms. Artz is a specialist in privacy and anti-financial crime issues.

[1] https://www.bma.bm/document-centre/policy-and-gui dance- am l- atf .

On 29th September 2024, PrivCom published the Consultation Document. The Consultation Document expressly discussed the feedback provided in response to the Consultation Letter, the meeting held on 25th March 2024, and subsequent informal meetings held with financial service providers unable to attend the in-person meeting on the 25th March 2024. Industry stakeholders were asked to provide formal written comments to the Consultation Document before 5:00pm (Bermuda time) on 5th November 2025.

Respondents to the Consultation Document did not restrict themselves to the questions asked, as many of those received covered a wide range of topics, some of which were specifically geared towards the impact of PIPA on financial service providers and others more generic. Industry specific questions were related to matters such as PIPA's impact on certain corporate structures and whether an organisation can appoint a corporate entity as its privacy officer as opposed to an individual within the organisation.

Following receipt of the formal comments provided in response to the Consultation Document, PrivCom amended the guidance articulated in the Consultation Document and produced the Final Report. The purpose of the Final Report is to: (i) afford PrivCom the opportunity to formally respond to the public comments received in response to the Consultation Document; and (ii) supplement the Consultation Document where appropriate.

2.3 High Level Outcomes

The main outcome of the consultation process and the publication of the Consultation Document was the determination that there are no material administrative or technical issues for the financial services sector in relation to the enactment and enforcement of PIPA. This is a testament to the drafting of PIPA and the Government of Bermuda ensuring that it effectively facilitates a financial service sector that adequately protects the personal privacy rights of individuals.

This positive regulatory outcome is not often the case in many other jurisdictions, including those with mature regulatory regimes and financial services sectors. Jurisdictions which have attempted to enact comparable data privacy legislation have historically experienced material challenges in the following areas with respect to financial service providers:

- The ability to use some types of personal information;
- The purposes for which personal information may be used in relation to the satisfaction of the commercial, legal and regulatory obligations of the financial institution; and
- The sharing of data within organisations, between organisations, domestically, and across jurisdictions.

PrivCom is of the view that these commercial and regulatory issues experienced elsewhere have been mitigated through the introduction of the following legislative provisions under PIPA:

- Section 6: Conditions for Using Personal Information
- Section 7: Sensitive Personal Information
- Section 15: Transfer of Personal Information to an Overseas Third Party; and
- Section 25: General Exemption.

Due to PIPA having effectively mitigated the commercial and regulatory issues experienced in foreign jurisdictions that have attempted to develop and implement data privacy legislative frameworks, PrivCom identified the following as the primary issues for Bermuda's financial service that require further industry specific guidance:

- The applicability of PIPA with respect to certain types of organizational structures;
- Organisational responsibilities, on-going compliance, and privacy notices; and
- Responding to requests for information by individuals.

This Final Report intends to effectively address and provide industry specific guidance regarding the concerns raised by Bermuda's financial service providers in response to the Consultation Letter and Consultation Document. The concerns requiring further clarification haven been, and will continue to be, addressed primarily through the drafting and publication of FAQs and industry specific case studies and guidance notes [see Appendix B].

PrivCom anticipates that the publication of industry specific FAQs, case studies, and guidance notes will be iterative and in direct response to the continuous evolution of Bermuda's financial service sector. The commercial and administrative processes changed or implemented in response to the enactment and enforcement of PIPA will heavily influence the frequency of the type of guidance by PrivCom in the future.

3. Application of PIPA

3.1 Context

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 organisation "uses" personal information in Bermuda it may be argued that the organisation has an obligation to ensure compliance with PIPA.

Section 3 of PIPA expressly states that:

> *" Except as provided by this Act, this Act 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 is intended to be interpreted broadly to protect individuals from undue harm. So long as an organisation "uses" or is "using" personal information in Bermuda, then PIPA would apply. Under section 2 of PIPA the terms "use" or "using" are defined as carrying out any operation on personal information, including collecting, obtaining, recording, holding, storing, organizing, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or otherwise making available, combining, blocking, erasing or destroying personal information.

With respect to the cross-border nature of modern commerce and the use of technology to innovate commercial activities, the application and enforcement of PIPA will continue to present novel use cases which may require further clarification in the future. Consequently, PrivCom commits to ongoing engagement with Bermuda's financial service industry stakeholders and the granting of the benefit of the doubt in circumstances where an industry participant has accidentally failed to operate in compliance with PIPA and has presented evidence indicating that it has operated in "good faith".

Because of the highly complex corporate structures utilized by financial service providers operating in Bermuda, industry participants must consider their organizational structure when seeking to understand the scope and contextual application of PIPA and its impact on their administrative and commercial activities. Appreciating the commercial nuances of each financial service provider, PrivCom recognizes that there is not one singular model which may be applied across the board with respect to the enforcement of regulatory compliance.

For example, captive insurers may engage the services of an insurance manager to perform their day-to-day administrative activities. As part of their suite of services the insurance manager may or may not provide corporate service provider ("CSP") services. It is not unusual for captive insurers to have one CSP provide a legally registered office in Bermuda and another CSP provide corporate secretarial services. PrivCom further recognizes that larger reinsurers domiciled in Bermuda are more likely to have their own employees in Bermuda. However, smaller reinsurers domiciled in Bermuda are more likely to outsource various administrative activities to an overseas third-party.

3.2 Physically Domiciled and Operating from within Bermuda

For the avoidance of doubt, the application of PIPA is not exclusively tied to the question of whether an organisation is domiciled or physically operating in Bermuda. The applicable scope of PIPA does not expressly require an organisation to be physically operating from or within Bermuda. Section 3 of PIPA states that PIPA shall apply to every organisation that "uses" personal information in Bermuda and therefore the application of PIPA is not contingent on whether an organisation is physically operating in 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 organisation "uses" or is found to be "using" personal information in Bermuda, the organisation shall fall under the scope of PIPA. Consequently, if an organisation 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 organisation 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 organisation 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.

One commentator to the Consultation Document provided an example where a company could have its headquarters physically located in Bermuda while having no access to any personal information from within Bermuda (i.e., insurance policy holder personal information held in overseas servers and platforms). In this circumstance, it may be argued that the company physically headquartered in Bermuda would not fall under PIPA.

In summary, an organisation's requirement to comply with PIPA is not contingent on whether the organisation is physically present in Bermuda. The application of PIPA is dependent on whether the organisation is "using" personal information within Bermuda. Potential access and "use" of personal information held overseas will not automatically render an organisation subject to PIPA. However, what is done with the potential to access and "use" personal information in Bermuda (i.e., whether the personal information is used in Bermuda) may do so. With respect to the points raised in response to the Consultation Document, the section of the Final Report regarding Headquarters has been amended accordingly (see section 3.3 below).

3.3 Headquarters in Bermuda

As previously discussed above, an organisation's obligation to operate in compliance with PIPA is not dependent on whether an organisation is physically domiciled in Bermuda. Whether a parent company is headquartered and domiciled in Bermuda, or one of its subsidiaries are, is not the singular factor when considering the application of PIPA. So long as an organisation is reliant on its ability to "use" personal information in Bermuda, in conjunction with providing a good or service, that organisation shall be considered to fall under the remit of PIPA.

If an organisation establishes its corporate headquarters in Bermuda and subsequently uses personal information in Bermuda, the organisation'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.

Under section 2 of the ESR, the Relevant Activity of "headquarters" typically assume responsibility for the overall success of the group, or an important aspect of the group's performance, and will ensure

appropriate corporate governance. For these purposes, the ESR states that a "headquarters" services include, but are not limited to:

(i) The provision of senior management to one or more affiliates;
(ii) Taking responsibility or control of material risks applicable to activities conducted by, or assets owned by, one or more affiliates; and
(iii) The provision of substantive advice in relation to such risks.

An organisation with headquarters in Bermuda would likely be seen as operating "in Bermuda" according to PIPA. However, depending on the facts (i.e. organizational structure, administrative and commercial activities undertaken in Bermuda, technological infrastructure and the adoption of e-commerce) an organisation headquartered in Bermuda may or may not "use" personal information.

Therefore, if an organisation is based in a foreign jurisdiction and is virtually operating from within Bermuda, that organisation may fall under the remit of PIPA so long as the administrative and commercial activities undertaken in Bermuda require the "use" personal information. However, the extent of its regulatory obligations under PIPA will depend on the type of personal information held, the intended purpose and "use" of the personal information, and whether the organisation is a beneficiary of an exclusion or exemption under PIPA.

3.4 Insurance and Reinsurance

In Bermuda there are numerous types of insurance-related entities, including but not limited to: (i) insurance; (ii) re-insurance; (iii) captives; (iv) brokers; (v) agents; and (vi) managers. Over the course of PrivCom's active engagement with Bermuda's insurance industry stakeholders, various corporate structures, commercial relationships, and operating models were discussed; including those in the chart below. The purpose of such stakeholder engagement was to ascertain the circumstances as to when and to what extent PIPA may apply in the event an insurer and/or a reinsurer is "using" personal information in Bermuda.

Insurer	**Reinsurer**
Third country based	Bermuda based
Bermuda based	Bermuda based
Bermuda based	Third country based

Following in-depth conversations with insurance-related commercial enterprises domiciled and licensed to operate from or within Bermuda, it became clear that the nature of the reinsurer is relevant to the manner of how they operate, such as:

- The reinsurer may reinsure on an individual matter or small category basis and in doing so may have access to the underlying data held by an insurer, including sensitive personal information;
- The reinsurer may reinsure a block of policies or risks, or the reinsurer may acquire part of a larger block of policies or risks. While they will have some access to data to assist with pricing the risk, they will not generally have access to an individual's sensitive personal information as this is not generally data considered necessary to complete pricing activities; and
- The sensitivity of some data held by a reinsurer may be relevant depending on the data's geo-location. Depending on the data's geo-location one may be able to identify individuals, but perhaps not an individual person (i.e., data held may afford someone the ability to distinguish one person from another, but not be enough to know who that person is by name, etc.)

Following industry stakeholder engagement, PrivCom determined how organisations participating in Bermuda's insurance industry can and should manage personal information following the enactment of PIPA (i.e., restricting access to and/or anonymising certain sensitive personal information where possible).

Many of the activities of insurance entities undertaken in Bermuda may coincide with the "use" of personal information and arguably fall under the legal remit of PIPA. Organisations such as reinsurers and captives should determine whether the personal information in its possession is needed to accomplish their intended business purpose. Furthermore, organisations should consider the types of personal information that may need to be "used" to directly or indirectly support the commercial activities of the organisation (i.e., human resources and employee related personal information).

For example, reinsurers should expressly consider the necessity to obtain the personal information of underlying policy holders held by insurers in order to provide reinsurance or captive services. PIPA is clear that any organisation that uses personal information is responsible for its own PIPA compliance, even if it is acting upon the instructions of another organization. Organisations may use mechanisms such as contractual agreements to arrange how compliance with PIPA will be coordinated between them and associated third parties. This regulatory opinion is supported under section 5(3) of PIPA:

> "*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 this Act at all times*"

At times, the use of personal information is necessary to conduct the business of insurance. While reinsurers may not seek to use personal information, in some markets the use of personal information is unavoidable and necessary. In such cases, the organisation should plan to comply with PIPA by implementing measures and policies that are appropriate and proportionate to the associated risk.

Some Bermuda based reinsurers may be required by their overseas partners (i.e., parent company, affiliated subsidiaries forming part of a corporate structure, etc.) to comply with foreign privacy or data protection laws, such as Europe's General Data Protection Regulations ("GDPR"). Compliance with

such laws is unlikely to be in direct conflict with PIPA and organisations can use resources such as PrivCom's "PIPA/GDPR Crosswalk" to evaluate specific measures that may be needed to simultaneously ensure compliance domestically and internationally.

A reinsurer or captive insurer that falls under the remit of PIPA, due to its "use" of personal information in Bermuda, must identify and disclose its lawful condition for "use" of personal information. Under section 6(1) of PIPA, an organisation may use an individual's personal information only if one or more lawful conditions for use are met. The specific condition(s) that may be relied upon will depend on the facts of the matter, the commercial activities undertaken by the organisation, and the organisation's intended "use" of personal information.

An organisation does not need to rely on multiple lawful conditions for use to legally "use" personal information. A single lawful condition for "use" of personal information may be relied upon. If an organisation relies on multiple conditions for use, PrivCom does not place an emphasis on one condition over another; all conditions for "use" shall be treated equally. So long as an organisation can reasonably demonstrate that a lawful condition for "use" has been reasonably applied, it is immaterial as to whether multiple conditions for "use" or a singular condition for "use" has been relied upon in conjunction with the provision of a financial service.

In the event an organisation does rely on multiple conditions for "use", the organisation should ensure that: (i) the conditions for "use" do not conflict; and (ii) the organisation describes the conditions for use in its Privacy Notice. Under section 9 of PIPA an organisation is obligated to provide individuals with a clear and easily accessible statement about its practices and policies with respect to the personal information held and used by the organisation. The Privacy Notice must include the purposes for which personal information is or might be used.[2] An organisation's Privacy Notice may also express how the application of certain lawful conditions for "use" may vary depending on the different types of data sets held by the organisation. PrivCom recognizes that a condition for use for one set of personal information may not be applicable with respect to another set of personal information.

PrivCom further advises organisations to be mindful of the pitfalls associated with overreliance on individual consent as a lawful condition for "use" of personal information. Although an individual may consent to an organisation to "use" their personal information at one point in time, it is possible that that same individual may withdraw their consent at later date; resulting in the organisation having to rely on another lawful condition for "use" in order to provide the requested financial service.

If the individual had not been informed by an organisation that it intends on using their personal information for a purpose other than that has been communicated in the organisation's Privacy Notice or was led to believe that withdrawing their consent would cease the organisation's use of their personal information, the organisation's action may be an unfair "bait-and-switch." Failing to comprehensively communicate all lawful conditions for "use" will likely compromise the organisation's ability to provide the financial services agreed to with the individual. If the individual was informed that the lawful condition was consent, and the individual withdraws their consent, the organisation may no longer be able to "use" personal information.

[2] Section 9(1)(b) of the Personal Information Protection Act 2016

3.5 Holding Companies and Captive Insurance Companies

Given the technical and administrative complexity associated with registered holding entities and captive insurance companies operating from within Bermuda, PrivCom appreciates that there may be some confusion regarding the applicability of PIPA. The extent to which personal information is used by a holding entity or captive insurer will vary according to its specific circumstances and its obligation to comply with domestic and foreign regulatory obligations.

In some circumstances a financial service provider may be licensed to operate from or within Bermuda, have no employees in Bermuda, conduct all its business outside of Bermuda (i.e., a holding company), and may still "use" personal information in Bermuda. Such personal information may include, but is not limited to, the organisation's Register of Directors and Officers, Register of Shareholders, and these individual's respective personal information.

These companies, while maintaining a minimal commercial footprint in Bermuda, typically engage the services of Bermuda-based corporate service provider ("CSP"), where it is the responsibility of the CSP to maintain Director and Shareholder Registers and the associated personal information for the purpose of conducting Board and Shareholder meetings and ensuring compliance with domestic and foreign financial service-related regulatory reporting obligations.

In satisfaction of local and international anti-terrorist financing and anti-money laundering legislation ("ATF-AML"), Bermuda based CSPs are required by the BMA and international financial service regulators to periodically collect due diligence documents (i.e. certified copies of birth certificates, passports, etc.) on each director and each beneficial owner who owns or controls 10% or more of the company. Much like the BMA's regulatory legislative framework, PIPA grants organisations the ability to "outsource" their compliance duties to any third party.

However, under section 5(3) of PIPA, an organisation is not able to circumvent their obligation to ensure compliance with PIPA through the procurement of a third party:

> "*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.*"

Therefore, prior to the procurement of the services of a CSP a holding company or a captive insurer must first determine if it satisfies the definition of "use" or "using" personal information under section 2 of PIPA. If so, the holding company or a captive insurer falls under the remit of PIPA and shall comply with PIPA requirements, such as adopting suitable measures and policies to give effect to its obligations and to the rights of individuals. Furthermore, if the holding company or captive insurer procures the services of a CSP, although the CSP may "use" personal information on its behalf, the organisation remains obligated to ensure compliance with PIPA. This ongoing obligation will likely entail ensuring that the appointed CSP "uses" personal information in accordance with PIPA.

If a captive insurer or holding company were considered an "organisation" that "uses" or is "using" personal information under PIPA, section 5(3) of PIPA states that the responsibility for compliance with PIPA is an ongoing regulatory compliance obligation for the captive insurer or holding company, irrespective of any third-party appointment. When a captive or a holding company enters into a "third party" agreement, the captive or holding company retains responsibility to ensure that the organisation operates in compliance with PIPA. The existence of a third-party service agreement does not necessarily displace the captive or holding company from its obligations under PIPA.

With respect to the legal principle called the "but for" test, absent a formal service agreement with a third party to "use" personal information on behalf of the organisation, the activities and "use" of personal information undertaken by the third party would have had to be performed by the organisation. Therefore, an organisation's procurement of a third-party corporate service provider would likely be considered to fall under section 5(3) of PIPA.

To ensure that a third party "uses" personal information on behalf of an organisation in accordance with PIPA, organisations are advised to use legal instruments such as contractual terms and conditions, to define practical roles, expectations, and/or liabilities. In doing so, organisations are encouraged to consider both their own "use" of personal information as well as the services of a third party that are connected to the "use". The third party may also have its own obligations to comply with PIPA, while the organisation that procured the services of the third party retains responsibility to ensure compliance with PIPA. In other words, depending on the facts of the matter both organisations may have independent obligations to comply with PIPA.

If a Bermuda-based CSP is engaged by a holding company or captive insurer to "use" personal information on its behalf, the CSP is obliged to ensure conformity to PIPA. The CSP would be expected to appointed a Privacy Officer and have a Privacy Programme in place and the holding entity or captive insurer would need to ensure that the CSP does not access or otherwise use the personal information for purposes beyond the authorized scope of the CSP.

Often it is the contractual responsibility of CSPs to oversee the commercial activities of a holding company or captive insurer through formal controls (i.e., contractual provisions, internal policies and procedures, etc.). Such formal controls typically stipulate that the CSP must be notified of any personal information that is shared with third parties and for what purpose.

Where the personal information used by a CSP must be shared with third parties (i.e. accountants, banks, or other local service providers), and that personal information shared by the CSP may be further shared with other entities in connection with the provisioning of an agreed service, it is imperative that the CSP remain aware of any further information sharing of personal information.[3]

If an organisation is of the view that it does not fall under the scope of PIPA (i.e. the organisation does not "use" any personal information in Bermuda, including employment-related personal information such as director and shareholder personal information), it may be argued that the organisation is not required to develop and enforce an internal Privacy Programme or appoint a Privacy Officer. Such an

[3] Sections 6 and 15 of the Personal Information Protection Act 2016

occurrence would be unlikely for a CSP given the commercial nature of CSPs, and in practice it may be a rare occurrence for holding companies or captives.

An organisation that considers itself to fall outside the scope of PIPA will need to be able to demonstrate to PrivCom, or an individual seeking to exercise their individual privacy rights under Part III of PIPA, that it does not use personal information and is not subject to PIPA. This burden of proof may be satisfied through means such as but not limited to the passing of a Board of Director's resolution that declares the organisation does not "use" personal information. In passing such a resolution the organisation's directors should expressly consider the internal analysis performed by the organisation to arrive at such a determination. Such internal analysis should account for the entirety of any personal information held and is used by the organisation and its appointed CSP.

With respect to the operational nuances of reinsurance and captive companies (i.e. the personal information that is shared between an individual and their insurer underwriting their insurance policy, and the exchange of personal information between the insurer and the reinsurer and captive) a reinsurer or captive insurer may be considered to fall under the scope of PIPA if the personal information is shared via loss runs and requests for payment. So long as the personal information shared is "used" in accordance with PIPA the organisation will have a requirement to comply with PIPA.

With respect to the operational nuances of each financial service provider operating from or within Bermuda, PrivCom has elected to adopt a flexible approach to ensuring compliance with PIPA. An organisation's obligations to comply with PIPA shall be determined on a case-by-case basis. There may be instances where an organisation may have minimal compliance requirements under PIPA if they use little personal information and/or the potential misuse of personal information is unlikely to cause harm to an individual. Organisations that use personal information more extensively and/or use personal information in a way that is more likely to cause harm if misused (such as hospitals, banks, health insurance companies) are likely to face more extensive compliance requirements under PIPA.

4. Responsibility and Compliance

Pursuant to section 5(1) of PIPA, every organisation that "uses" personal information in Bermuda shall adopt suitable measures and policies to give effect to its obligations and to the rights of the individuals as set out in PIPA. In accordance with section 5(2) of PIPA, the measures and policies adopted by organisations shall 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.[4] With respect to the use of vendors, third parties, or other data transfers, section 5(3) of PIPA states:

> "*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 this Act at all times.*" This requirement should be read along with that of section 5(7) to "*act in a reasonable manner*" and the requirements described in section 13 "Security safeguards."

[4] Section 5(2) of the Personal Information Protection Act 2016

Under section 5(4) of PIPA an organisation is obligated to appoint an organisational representative to serve in the role of "Privacy Officer". The Privacy Officer is primarily responsible for communicating with the Commissioner of PrivCom. The Privacy Officer is a role that an organisation most commonly designates internally (i.e., someone is formally appointed) and is responsible for ensuring that the organisation operates in compliance with PIPA. The formal appointment of an organisation's Privacy Officer shall be expressly stated within the organisation's Privacy Notice, and the Privacy Notice must disclose the contact information of the Privacy Officer.[5]

Following their formal appointment, the Privacy Officer may delegate his duties to one or more individuals, including third parties.[6] However, should the appointed Privacy Officer elect to delegate their responsibilities to an external third party, doing so does not absolve the organisation from ensuring compliance with PIPA.

Appreciating the complexity of the corporate structures adopted by Bermuda's financial service providers, section 5(5) of PIPA expressly accounts for commercial group structures where a parent company and its affiliated subsidiaries fall under common ownership or control. To avoid the unnecessary duplicative administrative efforts being undertaken by multiple Privacy Officers, PIPA allows for the appointment of a single Privacy Officer provided that the Privacy Officer is accessible from each organisation in the corporate group. Corporate groups are advised to ensure that their appointed Privacy Officer is formally authorised to act across the entirety of the organisation, its subsidiaries, and affiliated third parties, where applicable.

An organisation's appointed Privacy Officer may then delegate his or her duties to one or more individuals pursuant to section 5(6) of PIPA. For example, a financial service provider may appoint a single Privacy Officer within their parent company, and the Privacy Officer may then delegate his responsibilities to their designated insurance manager.

However, it is important to note that such delegation does not absolve the appointed Privacy Officer from ensuring that the parent company and its subsidiaries remain compliant with PIPA. The corporate group's appointed Privacy Officer remains obligated to ensure that the company and/or group of companies remain compliant with PIPA on an on-going basis. Therefore, it is important that any designated "privacy officer", whether they have delegated their responsibilities within the organisation or procured the services of a third party to assist in facilitating compliance with PIPA, is responsive and maintains oversight of organisational compliance.

[5] Section 9(1)(e) of the Personal Information Protection Act 2016
[6] Section 5(6) of the Personal Information Protection Act 2016

When considering who to appoint as their designated Privacy Officer, PrivCom advises organisations to:

(i) Consider individuals who hold a senior position within the organisation and are supported by organisational leadership as part of the organisation's promotion of data privacy as an organisational value;
(ii) Conduct an assessment as to how effectively an individual may be able to effectively fulfil the requirements of the role; and
(iii) Document and periodically assess the individual's ability to effectively serve in the role of Privacy Officer.

An organisation's Privacy Officer may be appointed pursuant to a decision enacted by the organisation's senior management team. Restricting the appointment process to a Director's Resolution would be considered unduly burdensome and potentially expose the organisation to undue operational risk until a Directors meeting is held and a formal resolution is passed. The appointment of the organisation's Privacy Officer shall be reflected within the organisation's Privacy Notice and its internal Privacy Programme.

The Privacy Officer need not personally undertake all administrative responsibilities necessary to facilitate compliance with PIPA. A Privacy Officer may delegate his duties either internally within the organisation or by formally contracting a third party that is able to provide assistive services. However, an organisation cannot outsource or delegate it's responsibility to operate in compliance with PIPA.

With respect to the delegatory powers afforded to an organisation's designated Privacy Officer, some third parties may be procured with the intention of providing "privacy officer" services. Such services may include, but are not limited to:

- Providing technical advice on compliance;
- Managing customer service interactions; and
- Responding to individual personal information requests and the information in "use" by the organisation.

Respondents to the Consultation Document asked whether an organisation's appointed Privacy Officer must be an internal employee of the organisation. PIPA does not expressly state that a Privacy Officer, or the recipient of the delegated duties, must be an internal employee of the organisation. Due to the diverse range of possible entities that may be subject to PIPA, requiring an organisation to appoint an employee as its Privacy Officer could be considered unduly burdensome for many organisations.

Requiring an organisation to appoint an employee who may have no experience or skills with data privacy legislation and the development and enforcement of internal Privacy Programmes has the potential to create an unnecessary administrative exercise for the organisation. In such a circumstance, it is likely that the organisation would appoint an internal employee as its Privacy Officer knowing that they are a mere figurehead and will likely have the appointed Privacy Officer delegate their duties to

an external third party in possession of the requisite skills necessary to assist the organisation ensure compliance with PIPA.

An organisation may instead elect to appoint a third party CSP to act as their Privacy Officer. The organisation may appoint the third party CSP to facilitate compliance with PIPA (i.e., receive communications from individuals regarding rights, communicating with PrivCom on behalf of the organisation, etc.) while the organisation remains responsible and liable for non-compliance with PIPA.

As it is likely that larger, more complex financial services providers will appoint their internal legal counsel or compliance officer as their appointed Privacy Officer, smaller organisations may not have the benefit of such an internal resource. If an organisation is unable to obtain the benefit of legal counsel or a corporate service provider, PrivCom advises such organisations to have their appointed Privacy Officer undertake formal training so that the organisation is equipped to adopt commercial practices that are compliant with PIPA. Alternatively, smaller organisations may consider the value in obtaining the services of a CSP capable of acting as their Privacy Officer.

If the personal information shared with the reinsurer or captive is redacted (i.e. all personal information is no longer identifiable in the documentation provided), it is possible that the reinsurer and/or captive may fall outside of the scope of PIPA. However, if a reinsurer or captive uses any employment related personal information in Bermuda, the organisation will fall under PIPA on those grounds; regardless of whether any personal information shared between the reinsurer and its cedent is redacted.

Honouring the intended purpose of PIPA, PrivCom recognizes that PIPA has been intentionally drafted in such a way to provide organisational flexibility so long as the organisation can:

(i) Justify its actions under the circumstances; and
(ii) Demonstrate it acted reasonably.

No matter which type of Privacy Officer is selected, the Privacy Officer must be able to effectively ensure organisational compliance with PIPA. Depending on the intended use of the personal information held by the organisation, it may be situationally appropriate for the appointed Privacy Officer to be present on site or have the ability to facilitate delegation of their on-site responsibilities in an effective and timely manner. In recognition of the fact that some organisations operate completely virtually, from an internal perspective the “privacy officer” could effectively satisfy their regulatory obligations under PIPA even when physically situated outside of the islands of Bermuda.

Appreciating the increased uptake of hybrid work environments, it is imperative that organisations ensure that their appointed Privacy Officer is strategically positioned to effectively respond to public inquiries. The types of personal information inquiries a Privacy Officer may face will vary depending on the circumstances and the type of business undertaken by the organisation.

4.1 Application of Exclusions and Exemptions

During the consultation process, questions were raised regarding a private company's ability to rely on an Exclusion, pursuant to section 4 of PIPA, or an Exemption, pursuant to sections 22-25 of PIPA. Although the legislation does not explicitly restrict an organisation's ability to rely on an Exclusion and/or an Exemption, there is a burden of proof on the organisation to indicate that an Exclusion and/or Exemption relied upon has been correctly applied. Therefore, an organisation's ability to rely on an Exclusion and/or Exemption under PIPA shall be evaluated by PrivCom on a case-by-case basis.

Given the subjective nature of section 4 and sections 22-25, an organisation's ability to rely on an Exclusion and/or Exemption is not limited to the public sector. Private sectors entities, following the satisfaction of said burden of proof, may rely on such legislative provisions and effectively fall outside the remit of PIPA. However, it is important to note that:

(i) Until the burden of proof has been satisfied it is assumed that the organisation, whether it operates in the private or public sector, shall fall under the remit of PIPA;
(ii) Unlike an Exclusion, an organisation relying on an Exemption must nevertheless comply with the "minimum requirements" stipulated under Part 2 of PIPA; and
(iii) Exclusions under section 25 of PIPA apply only to the extent that Parts 2 or 3 would be likely to prejudice the excluded purpose for use of personal information, and the organisation should be prepared to demonstrate that prejudice.

5. Conditions for Using Personal Information

The lawful conditions for using personal information were extensively explored throughout the consultation process, particularly in the context of the diverse corporate structures leveraged by participants in Bermuda's financial services sector. Following completion of the consultation process, PrivCom has concluded that given the diverse range of group structures utilized by financial service providers domiciled and operating from and within Bermuda, there is no single rule or approach regarding the permitted use of personal information in accordance with PIPA. The ability for an organisation to rely on the conditions to use personal information under section 6 of PIPA shall depend on the facts of the matter.

The facilitation of insurance and reinsurance services typically involve many parties in the "supply chain" or "matrix of activity". Each party forms part of the "matrix of activity" and likely will play a different role in providing services in accordance with the service contract agreed to with the consumer. In conjunction with the fulfillment of these differing roles within the "matrix of activity", each party will likely have different interactions with and "uses" for personal information. Subsequently, the way in which personal information is "used" throughout the "matrix of activity" will likely vary. When the "matrix of activity" involves numerous types of "use" of personal information, individuals are exposed to different types of personal risk.

PrivCom recognizes that reinsurers do not typically have a direct contractual relationship with the individual who has obtained the benefit of the originating insurance policy. Therefore, a reinsurer is likely unable to obtain the express consent from the individual to use their personal information in order to facilitate reinsurance services to the insurer. Instead of obtaining express consent for "use", a reinsurer may arguably rely on section 6(2)(c) of PIPA. Section 6(2)(c) states:

> *"For the purpose of relying on consent as a condition for the use of personal information under subsection (1)(a) –*
>
> *(c) when an individual consents to the disclosure of his 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 organisation for the specified purpose."*

In consideration of data privacy legislative frameworks enacted by comparable regulatory bodies, when "the specific purpose" under section 6(2)(c) is insurance coverage, it may be implied that such a purpose may include a variety of ancillary uses of personal information and should therefore be construed broadly. Failure to adopt such an approach runs the risk of unduly restricting a reinsurer or captive insurer from relying on the express consent that an individual may have provided when soliciting the services of an insurer.

It may be reasonably argued that when an individual provides an insurer consent to use their personal information to provide a specified line of insurance, their express consent includes the ancillary activities an insurer may have to undertake to provide such a service; such as the procurement of a reinsurance policy that will mitigate any underwriting or operational risks the insurance company may face in the course of doing business.

However, insurers are advised to ensure that their Privacy Notice articulate the intended purpose and "use" of their information and explicitly state the organisations to whom the insurer may share their personal information in pursuit of this intended purposes. Reinsurers and captive insurers are advised to ensure that their cedent insurers have Privacy Notices that contain such information so that any consent that is communicated by an individual to an insurer is valid.

In the absence of formally expressed consent to use an individual's personal information to facilitate the provisioning of a financial service product (i.e. reinsurance coverage), the facts of the matter will determine whether a reinsurer or captive insurance company may effectively rely on section 6(2)(d) of PIPA as an acceptable condition to "use" personal information. Section 6(2)(d) of PIPA states:

> *"For the purpose of relying on consent as a condition for the use of personal information under subsection (1)(a) –*

> *(d) an individual will be deemed to have consented to the use of his 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.*

PrivCom is of the opinion that section 6(2)(d) of PIPA is intended to be interpreted broadly. For comparison only, data protection rules in other countries have similar language and purposes to legislatively prescribed public interest exemptions for insurance and reinsurance providers. For example, with respect to Bermuda's reinsurance and captive insurer industry this provision could be used in instances where the provisioning of a reinsurance service to an insurer amounts to an indirect financial benefit to the individual that would reasonably be considered to form part of the insurance service provided to the individual (i.e. security of financial tool procured from the insurer).

While the default position for many organisations is to obtain express consent, in accordance with sections 6(1)(a) and 6(2)(a) of PIPA, reliance on express consent may not be commercially feasible since consent must be clear and informed and may be withdrawn at a later date. Depending on the circumstances, the following conditions for the "use" may be relied upon where an organisation's ability to rely on "consent" may not be appropriate:

- Section 6(1)(c): *The use of the personal information is necessary:*
  - *i. For the performance of a contract to which the individual is a party; or*
  - *ii. For the taking of steps at the request of the individual with a view to entering into a contract*
- Section 6(1)(d): *The use of the personal information is pursuant to a provision of law that authorises or requires such use*.
- Section 6(1)(h): *The use of the personal information is necessary in the context of an individual's present, past or potential employment relationship with the organisation*.

Appreciating that sections 6(1)(a) and 6(2)(a) of PIPA expressly account for circumstances where the communication of express consent may serve as formal authorization to "use" personal information, there may be instances where consent for use may be implied so long as the matter does not concern the use of sensitive personal information. Section 6(2)(b) of PIPA states:

> *"An organisation is not obliged to provide such mechanisms* [to communicate consent] *where it can be reasonably implied from the conduct of an individual that he consents to the use of his personal information for all intended purposes that have been notified to him, but this does not apply to sensitive personal information".*

With respect to the fact that an organisation falling under the scope of PIPA are required to implement an internal Privacy Programme, section 6(1)(b) 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.

Section 6(1)(b) of PIPA states that:

> *"(b) except in relation to sensitive information, a reasonable person giving due weight to the sensitivity of the personal information would consider –*
>
> *(i) That the individual would not reasonably be expected to request that the use of his personal information should not begin or cease; and*
> *(ii) That the use does not prejudice the rights of the individual?*

For comparative purposes only, Article 6(1)(f) of the GDPR states:

> "*1. Processing shall be lawful only if and to the extent that at least one of the following applies:*
>
> *(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".*

Upon review of section 6(1)(b) of PIPA, in order for an organisation to rely on implied consent as a lawful condition to "use" personal information, the organisation must take into account the reasonable expectations of the individual and whether the organisation is reasonable in evaluating that expectation and any potential impact on individual rights under Part III of PIPA. In contrast, GDPR Article 6(1)(f) expressly considers the legitimate commercials 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, an organisation 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.

With respect to the above, there may be circumstances where an organisation has legal authorization to use an individual's personal information. Section 6(3) of PIPA states that if an organisation is unable to meet any of the conditions outlined under section 6(1), the organisation may use the personal information only if:

a) *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 organisation;*
b) *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 organisation;*
c) *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;*

d) The use of the personal information is necessary in order to collect a debt owed to the organisation or for the organisation to repay to the individual money owed by the organisation;
e) 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 organisation, the disclosure is appropriate; or
f) The use of the personal information is reasonable to protect or defend the organisation in any legal proceeding.

5.1 Incidental/Accidental/Unintentional Access and Use of Personal Information

Following completion of the consultation process, industry stakeholders requested further clarification regarding instances where an organisation has incidentally, accidentally, or unintentionally "used" personal information. Industry stakeholders proposed that when an organisation receives incidental personal information (i.e., information that was not requested by the financial service provider), it would be reasonable to conclude that the organisation would not fall under the scope of PIPA so long as:

(i) Such occurrences are infrequent and minimal; and
(ii) The "use" of such personal information is limited to its deletion.

Certainly where personal information is received regularly, in a significant volume, and the "use" of the incidentally provided personal information goes beyond deletion, that organisation should be considered to fall within the scope of PIPA; notwithstanding that the organisation did not specifically request the personal information or that the primary business activities of the organisation do not involve the use of the incidentally provided personal information.

In appreciation of the points raised, PrivCom is of the view that if an organisation was incidentally, accidentally, or unintentionally provided with personal information, the organisation shall be considered to fall under the remit of PIPA even if the use of said personal information is limited to deletion. Under section 2 of PIPA, the "use" or "using" of personal information includes activities such as erasure. So long as the deletion of the personal information incidentally, accidentally, or unintentionally provided to an organisation is occurs in Bermuda (i.e. deleted in Bermuda), the organisation shall fall under the scope of PIPA.

Nevertheless, the burden on organisations and the steps to be undertaken by an organisation in response to the receipt of incidental personal information should align with the requirement to act reasonably under section 5 of PIPA. If an organisation does not intentionally, habitually, and/or regularly use or receive personal information, and therefore is not normally subject to PIPA, then it would not be reasonable to expect the organisation to undertake the administrative steps necessary to ensure compliance with PIPA on the chance that it may incidentally, accidentally, or unintentionally receive personal information. However, following actual receipt of incidental personal information, the organisation in receipt shall be considered to fall under the scope of PIPA and would be expected to act reasonably in response.

6. Sensitive Personal Information

Section 7(1) of PIPA defines "sensitive personal information" 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 memberships, biometric information or genetic information.

For the sake of clarity, "genetic information" is defined 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*".[7]

In contrast to the legal definition of "genetic information", "biometric information" is defined as "*any information relating to the physical, physiological or behavioural characteristics of an individual which allows his unique identification, such as facial images or fingerprint information*"[8]

Having clarified the meaning of "sensitive personal information" and the types of information that may be categorized as such, PrivCom now turns its attention to the legal provisions under PIPA that limit how sensitive personal information may be used. Sensitive personal information sits on the spectrum of risk and sensitivity and should be identified and managed accordingly.

With respect to the use of "sensitive personal information", no organisation shall, without lawful authority, use sensitive personal information in order to discriminate against any person contrary to any provision of Part 2 of the Human Rights Act 1981.[9] However, it is important to note that PIPA in theory permits an arguably discriminatory "use" of sensitive personal information in limited circumstances. For example, reading section 7 in accordance with section 6(2)(d), an individual will be deemed to have consented to an insurance plan that has been underwritten using "sensitive personal information" provided that the individual has an interest in or derive a benefit from an insurance policy.

The nature of a financial service provider's use of sensitive personal information may vary. In conjunction with ongoing financial services regulatory obligations that require organisations to undertake periodic ATF-AML and KYC administration, organisations are likely to require the "use" of sensitive personal information specifically intended to identify an individual, track and verify the source of funding, undertake transaction monitoring, and perform sanctions screening. Given these ongoing regulatory obligations imposed by domestic and international financial services regulators, the ability for an organisation to "use" sensitive personal information is necessary.

[7] Section 2 of the Personal Information Protection Act 2016
[8] Section 2 of the Personal Information Protection Act 2016
[9] Section 7(2) of the Personal Information Protection Act 2016

Under section 6(1)(c) of PIPA the use of "sensitive personal information" is permitted where there is a provision of law that authorises or requires such use. Further, section 25(a) of PIPA provides a general exemption for use of "sensitive personal information" with respect to "*the prevention or detection of crime and compliance with international obligations regarding the detection, investigation, and prevention of crime*". This exemption applies in circumstances where the strict application of a specific provision under PIPA would prejudice the detection, investigation, and prevention of crime.

In some instances organisations are required to retain "sensitive personal information" by a law enforcement agency such as the Bermuda Police Service. The organisation could rely on section 6(1)(c) or section 25(a) until they have received formal communication from the law enforcement agency indicating that an investigation has been closed. At that point, the organisation should consider whether it is necessary to continue to retain the "sensitive personal information" in conjunction with the pursuit of another purpose or intended "use".

As it is common practice for a reinsurer to have limited access to "sensitive personal information", PrivCom recognizes that it is standard industry practice for an insurer to provide a reinsurer with contractual reassurances stipulating that the insurer shall conduct the relevant ATF-AML and sanctions checks against the policy holders on the basis that the reinsurer does not have access to the necessary data to satisfy such a regulatory obligation. It is worth noting at this stage that PIPA requires an organisation to ensure that it does not collect any personal information it does not otherwise need.

In consideration of the potential for financial service providers to encounter regulatory conflict, where an organisation finds themselves having to comply with numerous domestic and international regulatory obligations, organisations should take all reasonable efforts to comply with PIPA. Organisational attempts to ensure compliance with PIPA should not interfere with their ability to ensure compliance with any other or additional specific financial services regulatory obligations.

Personal information may at times be used for statistical research.[10] PIPA does not limit organisations which may undertake such research, but it does clearly state that appropriate safeguards to the rights of individuals should be in place. Such safeguards should expressly consider the sensitivity of the personal information and the inherit risk associated with "using" personal information for the purposes of scientific, statistical or historical research. PIPA's "purpose limitation" section states:

> "*10(1) An organisation shall use personal information only for the specific purposes under section 9(1)(b) or for purposes that are related to those specific purposes.*
>
> *(2) Subsection (1) shall not apply –*
>
> *(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.*

[10] Section 10(2)(e) of the Personal Information Protection Act 2016

This section is read in combination with section 9 on regarding organisational Privacy Notices:

> *9(1) An organisation shall provide individuals with a clear and easily accessible statement ("privacy notice") about its practices and policies with respect to personal information – including:*
>
> *(b) the purposes for which personal information is or might be used.*

With respect to the storage of personal information, section 13(1) of PIPA requires organisations to protect personal information with the enactment of appropriate safeguards specifically intended to mitigate the risk of loss or unauthorized access, destruction, use, modification, or disclosure of personal information and any other misuses. Such safeguards must be proportional to: (i) the likelihood and severity of the harm threatened by the loss, access of misuse of the personal information; (ii) the sensitivity of the personal information (including whether it is sensitive personal information); and (iii) the context in which the personal information is held.[11]

Furthermore, an organisation cannot rely on sections 6(1)(b) or 6(2)(b) of PIPA with respect to an organisation's ability to obtain and rely on consent from an individual in order to use their "sensitive personal information". Section 6(1)(b) of PIPA states:

> *"Except in relation to sensitive personal information, a reasonable person giving due weight to the sensitivity of the personal information would consider –*
>
> *(i) That the individual would not reasonably be expected to request that the use of his personal information should not begin or cease; and*
> *(ii) That the use [of his personal information] does not prejudice the rights of the individual*

PrivCom recognizes the necessity for organisations to identify how the "reasonableness" test and the necessity to provide a mechanism to allow for the communication of consent under section 6(2)(b) of PIPA does not apply to matters concerning the use of "sensitive personal information".

> *"6(2) For the purpose of relying on consent as a condition for the use or personal information under section 6(1)(a) -*
>
> *(b) an organisation is not obliged to provide such mechanisms where it can be reasonably implied from the conduct of an individual that he consents to the use of his personal information for all intended purposes that have been notified to him, but this does not apply to sensitive personal information.*

[11] Section 13(2) of the Personal Information Protection Act 2016

6.1 Potential for Personal Titles to Act as Identifiers

During the public consultation process it was brought to the attention of PrivCom that the use of a person's title (i.e. Mr, Mrs., Ms.) arguably satisfies the definition of "sensitive personal information" as it may be a means within which a person's sex and/or marital status may be identified absent formal disclosure from the individual. The question was raised as to whether such personal information, if collected by an organisation, would result in the organisation falling within the scope of PIPA.

PrivCom recognises that it may be argued that the disclosure of one's title may serve as an indicator of one's sex, which is a protected category under the definition of "sensitive personal information". Furthermore, it may be argued that one's personal title may serve an indicator of one's marital status, and therefore further satisfy the definition of "sensitive personal information."

Therefore, if an organisation requires an individual to state their personal title in order to facilitate the provisioning of a financial service, the collection of such "sensitive personal information" would result in the organisation falling under the scope of PIPA and would subsequently be held to higher regulatory compliance standards.

However, unlike laws in other jurisdictions (such as the GDPR), the "use" of "sensitive personal information" merely requires that such personal information is not to be used for discriminatory practices which run contrary to the Human Rights Act 1981. Organisations should protect this personal information with measures and policies appropriate to the nature, scope, context, and purposes of the use and the risk to individuals.

7. Privacy Notices

Pursuant to section 9(1) of PIPA, an organisation must provide individuals with a clear and easily accessible statement ("Privacy Notice") about its practices and policies with respect to personal information. An organisation's Privacy Notice" must include:

(a) The fact that the personal information is being used;
(b) The purposes for which personal information is or might be used;
(c) The identity and types of individuals or organisations to whom personal information might be disclosed;
(d) The identity and location of the organisation, including information on how to contact it about its handling of personal information;
(e) The contact information of the organisation's Privacy Officer;
(f) The choices and means the organisation provides to an individual for limiting the use of, and for accessing, rectifying, blocking, erasing and destroying, his personal information.

Under Part 2 of PIPA, organisations have a minimum requirement to undertake genuine efforts to operate fairly and transparently Appreciating that it may be practically difficult for an organisation to disclose the identity of the individuals and/or organisations with whom personal information may be shared, organisations should make genuine efforts to disclose in their Privacy Notice the types of parties that an individual's personal information may be shared with in accordance with the provisioning of a financial service. Upon receipt of a rights request, organisations should be prepared to inform the individual with whom the personal information was in fact shared.

Organisations that "use" personal information have an obligation to ensure that their Privacy Notice is fully comprehensive and discloses: (i) the intended use of the personal information held; and (ii) the types of entities that may become privy to an individual's personal information. Organisations that "use" personal information have an obligation to notify individuals in the event the organisation's intended "use" of their personal information changes and potentially conflicts with and/or extends the intended "use" previously disclosed in their Privacy Notice.

Furthermore, if the types of organizations with whom the organisation intends to share information is further extended, the organisation would be required to inform the individual, unless such disclosure is legally restricted pursuant to a legally recognized exclusion and/or exemption. In such instances the organisation would be compelled to update their pre-existing Privacy Notice and accurately disclose the full extent to which an individual's personal information may be "used" and with whom their personal information may be shared.

Section 9(2) of PIPA obligates organisations to take reasonably practical steps to ensure that their Privacy Notice is provided either before or at the time of collection of personal information, or, when that is not possible, as soon as is reasonably practicable. PIPA does not specify the medium of delivery of the Privacy Notice. Therefore, communication of the organisation's Privacy Notice shall be left up to the discretion of the organisation, so long as communication is adequately recorded and readily available for future reference.

PrivCom is of the understanding that many of Bermuda's captive insurers that are legally registered to operate from or within Bermuda do not have an official website or other publicly available platform upon which they may publish a Privacy Notice. Given these operational nuances, it would be considered reasonable for organisations to consistently communicate their Privacy Notice through whatever manner they normally communicate to individuals (i.e. appendix to physical and/or electronic copy of a contractual service agreement, published and readily accessible on the organisation's website, etc.).

Section 9(3)(b) of PIPA states that an organisation need not provide a Privacy Notice if the organisation can reasonably determine that all uses made, or to be made, of the personal information are within the reasonable expectations of the individual to whom the personal information relates. For example, a captive or reinsurance company could demonstrate reliance on section 9(3)(b) of PIPA by providing PrivCom evidence indicating:

(i) that the reinsurer has introduced contractual terms and conditions in their service agreements that require their cedents (i.e. the insurer) to inform individual policy holders of the ways in which their personal information may be in "use"; and/or
(ii) the steps taken by the insurer to inform the individual about the uses.

Organisations must be clear about how they "use" personal information in their Privacy Notice. In circumstances where an organisation is compelled to undertake deliberate measures to ensure compliance with financial, AML, or other legislatively imposed regulations, their Privacy Notice should include a statement indicating that one of the organisation's intended "uses" of personal information is to share personal information with specified regulators to ensure regulatory compliance. The Privacy Notice should identify the types of individuals or organisations to whom the information might be disclosed and enumerate the choices available to an individual regarding such "use", including whether they are unable to exercise a choice.

The legislative obligation to provide individuals with a copy of their Privacy Notice, in accordance with section 9, is considered separate from the general obligation for organisations to use personal information fairly.[12] For the purpose of ensuring commercial clarity, the obligation for an organisation to use personal information in a fair manner is intended to be interpreted as an obligation to ensure that an organisation's commercial operations:

(i) Ensure on-going compliance with all applicable law, regulations, codes of conduct, and statutory instruments;
(ii) Facilitate transparency and openness through the disclosure of relevant details; and
(iii) Are neither harmful to, act against, nor conflict with the rights and interests of the individual.

8. Rights of Individuals

During the consultation process extensive discussions were held regarding the practicalities of the right of access to personal information, including: (i) the scope; (ii) costs; (iii) timelines; (iv) the form of responses; and (v) a host of more detailed queries. Following receipt of an individual's request for access to their personal information, section 17(1) of PIPA obligates an organisation to reasonably provide access to the following types of information:

(a) Personal information about the individual in the custody or under the control of the organisation;
(b) The purposes for which the personal information has been and is being used by the organisation; and
(c) The names of the persons or types of persons to whom, and the circumstances in which, the individual's personal information has been and is being disclosed.

[12] Section 8 of the Personal Information Protection Act 2016

In certain circumstances an individual's right to access to their personal information in "use" by an organisation may be limited. Depending on the nature of the personal information and the facts of the matter, an organisation may elect to invoke section 17(2) of PIPA and refuse to provide an individual access to the personal information the organisation uses if:

(a) The personal information is protected by any legal privilege;
(b) The disclosure of the personal information would reveal confidential information of the organisation or of a third party that is of a commercial nature and it is not unreasonable to withhold that information;
(c) The personal information is being used for a current disciplinary or criminal investigation or legal proceedings, and refusal does not prejudice the right of the individual to receive a fair hearing;
(d) The personal information was used by a mediator or arbitrator, or was created in the conduct of a mediation or arbitration for which the mediator or arbitrator was appointed to act under an agreement or by a court; or
(e) The disclosure of the personal information would reveal the intentions of the organisation in relation to any negotiations with the individual to the extent that the provision of access would be likely to prejudice those negotiations.

There may also be instances where an individual's right to access their personal information used by organisation may be entirely restricted due to the applicability of any of the circumstances detailed under section 17(3) of PIPA. An organisation shall not provide an individual access to their personal information if:

(a) The disclosure of the personal information could reasonably be expected to threaten the life or security of an individual;
(b) The personal information would reveal personal information about another individual; or
(c) The personal information would reveal the identity of an individual who has in confidence provided an opinion about another individual and the individual providing the opinion does not consent to disclosure of his identity.

However, PIPA does include a legislative provision which has the potential to restrict an organisation's ability to rely on sections 17(2)(b) and 17(3)(b)-(c) of PIPA. If an organisation is reasonably able to redact the personal information referred to by sections 17(2)(b) and 17(3)(b)-(c), the organisation shall provide the individual with access to his personal information.[13]

Individuals also have a right to compel an organisation to correct informational errors or omissions. Informational inaccuracies run the risk of adversely impacting an individual, (i.e. adversely affecting an organisation's willingness to provide a financial service or the quality of service provided). Under

[13] Section 17(4) of the Personal Information Protection Act 2016

section 19(1) of PIPA an individual may submit a written request to an organisation to correct an error or omission in any of his personal information which is under the control of the organisation.

In the event an organisation receives a request to correct an individual's personal information, the organisation is obligated to: (i) correct the personal information as soon as reasonably practicable; and (ii) where the organisation has disclosed the incorrect information to other organisations, send a notification containing the correct information to each organisation to which the incorrect information is disclosed.[14]

Section 19(6) of PIPA expressly considers circumstances where an individual's personal information is used as part of an organisation's marketing activities. An individual reserves the right to request an organisation to cease, or not begin, "using" his personal information for the purposes of advertising, marketing or public relations.

Additionally, section 19(8) of PIPA empowers an individual to limit or restrict an organisation from using their personal information in circumstances where the individual is of the view that use of their personal information has caused, or is likely to cause, substantial damage or distress to themselves or another individual. Lastly, section 19(10) of PIPA grants an individual the authority to require an organisation to erase or destroy personal information held by an organisation that is no longer relevant for the purposes of its use.

With respect to the individual rights emboldened under sections 17 and 19 of PIPA, it is important to note that section 20 of PIPA imposes administrative requirements that must be satisfied by the individual before the organisation in receipt of the request may formally act in response. For an applicant to submit a valid request, section 20(1) of PIPA stipulates that the request must be in writing and include sufficient information to enable the organisation to identify the personal information.

Upon receipt of a formal individual rights request, the organisation in receipt shall acknowledge the date upon which the request was received and where insufficient information is provided state what further information is required.[15] Following receipt of a complete written request, the organisation shall respond to the applicant no later than: (i) 45 days from the day on which the organisation received the applicant's written request; or (ii) by the end of an extended time period if the time period to respond has been extended pursuant to section 20(6) of PIPA .[16]

Although an organisation is obligated to respond to an individual's request within a reasonable period of time, PIPA does afford organisations the ability to extend the period for responding to an applicant's written request by no more than 30 days, or for a longer period as permitted by the Commissioner.[17]

[14] Section 19(2) of the Personal Information Protection Act 2016
[15] Section 20(3) of the Personal Information Protection Act 2016
[16] Section 20(4) of the Personal Information Protection Act 2016
[17] Section 20(6) of the Personal Information Protection Act 2016

Appreciating the administrative burden associated with individual rights requests, section 20(6) of PIPA states an organisation may extend the period to respond to an individual's request, if:

(a) A large amount of personal information is requested or needs to be searched or corrected;
(b) Meeting the time limit would unreasonably interfere with the operations of the organisation; or
(c) More time is needed to consult with a third party before the organisation is able to determine whether or not to give the applicant access to the requested personal information.

If an organisation extends the period for responding to an individual rights request, the organisation shall inform the applicant of: (i) the reason for the extension; and (ii) the time when a response from the organisation can be expected. Recognizing the administrative burden associated with responding to individual rights requests, organisations are permitted to charge an administrative fee not exceeding the prescribed maximum fee for access.[18] It is important to note that PIPA does not authorize organisations the ability to charge a fee for facilitating the correction of an error or omission of personal information.

To ensure operational clarity, the Minister may, in consultation with the Commissioner, prescribe any applicable fees that may be charged to facilitate an access request.[19] The Commissioner has consulted with the Minister regarding the prescribed maximum fee for facilitating an individual rights access request. However, as of the date of the publication of the Final Report no decision regarding the maximum fee that may be charged for facilitating an access request has been announced by the Minister.

PIPA is technologically neutral and therefore silent as to the format personal information may or must be provided in response to an information request. Therefore, the minimum requirement for organisations to act reasonably shall apply. It would be considered reasonable for organisations that provide an individual access to their personal to provide the requested information in a clear, concise format that is easily accessible.

Appreciating the potential for an individual to abuse their individuals rights through the submission of frivolous or vexatious requests to an organisation, section 20(12) of PIPA grants organisations the ability to refuse an individual rights request should such a request be considered "manifestly unreasonable". Should an organisation refuse an individual rights request, section 20(13) of PIPA requires the organisation to:

(i) Inform the applicant in writing of their reasons for refusal; and
(ii) Inform the applicant of their right to contact PrivCom and submit a formal complaint.

[18] Section 20(8) of the Personal Information Protection Act 2016
[19] Section 20(11) of the Personal Information Protection Act 2016

PrivCom is of the view that refusal of an individual rights request is dependent on ascertaining what would be considered "reasonable" with respect to the facts of the matter (i.e. nature of request, frequency of requests, intended purpose of the request, etc.). Appreciating the nuance associated with an organisation's ability to effectively rely on section 20(13) of PIPA to refuse an individual rights request, PrivCom has elected to grant organisations the benefit of the doubt where genuine efforts to operate in "good faith" have been evidenced by the organisation.

9. Regulatory Bodies and Enforcement

9.1 Domestic Regulators

Every organisation that "uses" personal information in Bermuda is required to ensure compliance with PIPA through the adoption of suitable measures and policies which give effective to the organisation's obligations and the rights of individuals set out in PIPA.[20] PrivCom intends to ensure that the enforcement of PIPA will not interfere with the on-going regulatory activities of domestic regulators such as the BMA.

In the ordinary course of discharging their regulatory functions, regulators may collect, be provided with, and/or use a broad range of personal information. The relevant conditions for "use" under section 6 and general exemptions under section 25 of PIPA permit regulators to lawfully "use" personal information when:

(i) The regulator is authorized or required by a statutory provision to provide personal information to, or collect personal information from, an organisation;
(ii) The regulator seeks to comply with requests from domestic or international law enforcement agencies; or
(iii) The regulator seeks to coordinate with foreign regulatory authorities situated outside of Bermuda on public policy grounds.

Upon the request domestic regulatory bodies, PrivCom shall engage with and provide a Memorandum of Understanding to discuss the conclusions above.

9.2 Overseas Regulators

Appreciating the value in cross-regulatory co-operation, PrivCom is committed to engaging and fostering regulatory relationships with international regulators to ensure that the enforcement of PIPA will not interfere with the regulatory activities of overseas financial services and data privacy regulators. PrivCom intends to enhance Bermuda's reputation as a regulatory leader and ensure that its regulatory actions are reflective of international regulatory methods of best practice.

By making deliberate efforts to draw from the industry experience of comparable international regulatory bodies, PrivCom is of the opinion that individuals whose personal information is used by organisations in Bermuda will directly benefit from this collaborative engagement.

[20] Section 5(1) of the Personal Information Protection Act 2016

When individual data privacy rights are interpreted according to international methods of best practice, PrivCom can better ensure that individuals whose personal information is used in Bermuda are afforded a level of regulatory protection that is reflective of internationally accepted regulatory standards.

Organisations will also benefit from such collaboration through the publication of regulatory guidance that is reflective of internationally agreed methods of best practice (i.e., administrative practices that promote the adoption of operational efficiencies and the reduction of domestic and international compliance costs).

10. Transfer of Personal Information to a Third Party

With respect to an organisation's ongoing requirement to ensure compliance with PIPA, should an organisation in Bermuda seek to contractually engage the services of a third party (i.e. domestically or overseas) section 5(3) of PIPA states that the organisation retains their responsibility for ensuring compliance with PIPA. During the consultation process a number of Bermuda domiciled financial services providers requested further clarification regarding the procurement of, and transfer of personal information to, external third parties.

10.1 Third Parties Domiciled in Bermuda

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.[21] The obligation to ensure ongoing compliance with PIPA means that the organisation should perform due diligence on the third party vendor prior to procuring their services. Should the third-party vendor fail to "use" personal information in compliance with PIPA, the organisation that procured the services of the third party shall be considered liable.

Organisations that choose to transfer personal information to a third party may do so in many different ways and for many different purposes. The personal information that an organisation may transfer to a third party and its sensitivity to risk will likely vary. To ensure that an organisation is meeting its obligations under PIPA, following the transfer of personal information to a third party, PrivCom advises organisations to undertake the following administrative steps:

- Establish internal standards that outsourcing partners or third parties must meet;
- Create an evaluation process as part of its vendor procurement process (such as a survey, questionnaire, or formal audit);
- Conduct due diligence checks in order to validate the data privacy safeguards enacted by potential third party vendors who may be in receipt of personal information held by the organisation;

[21] Section 5(3) of the Personal Information Protection Act 2016

- Execute formal service agreements (i.e. a legally enforceable contract) that contain terms and conditions that explicitly outline the performance responsibilities for the organisation and the third party with respect to the "use" or "using" of personal information; and
- Develop administrative processes that enable the organisation to effectively monitor its relationship with the third party.

The exact nature of these administrative steps will differ for all third-party vendor relationships or third-party data transfers when compared against the administrative processes undertaken by organisations as part of traditional business interactions. The appropriate administrative actions needed to be undertaken by each organisation to ensure continued compliance with PIPA will depend on the sensitivity of the personal information transferred and the risk of harm to individuals.

10.2 Overseas Third Parties

An "overseas third party" in the context of an international business setting could mean, for example, "non-group companies" or subsidiaries of a Bermuda holding company that are domiciled outside of Bermuda. When considering the transfer of information to an overseas third party, the test for determining the application of PIPA is dependent on whether the organisation is: (i) "using" personal information is in Bermuda; (ii) "but for" the fact that the organisation is seeking to procure a third party to "use" personal information on its behalf, would the organisation have to had used the personal information itself in order to provide a financial service.

While many organisations default to the concept of requesting consent of the individual, an organisation's ability to rely on consent as a legal condition to "use" personal information may or may not be appropriate when seeking to transfer personal information to an overseas third party, because:

(i) Communication of consent must be clear and informed; and
(ii) Consent to transfer one's personal information to an overseas third party may be withdrawn.

Appreciating that PIPA requires organisations falling under the scope of PIPA to be transparent regarding its intended "use" of personal information (i.e. publication and communication of a Privacy Notice), if an organisation wishes to rely on individual consent in order to legally transfer personal information to an overseas third party, PrivCom advises Bermuda's financial service providers to ensure that their Privacy Notice expressly explains that the organisation shares an individual personal information with overseas third parties (i.e. transfer of personal information to overseas regulators to ensure ongoing compliance with international regulatory reporting and performance obligations).

PrivCom further advises organisations to ensure that the aforementioned formal declaration in their Privacy Notice enumerate the choices available to an individual regarding the communication of

consent and way in which the organisation may use the individual's personal information.[22] The Privacy Notice must include a statement which outlines the choices and means the organisation provides to an individual for limiting the organisation's use of, and for accessing, rectifying, blocking, erasing and destroying an individual's personal information that is "used" by an organisation.

Given the issues associated with relying on sections 6(1)(a) and 6(2)(b) in order to transfer personal information to an overseas third party, PrivCom recognizes that Bermudian organisations may instead seek to utilise section 6(1)(g) of PIPA as a condition they may rely on when seeking to transfer personal information to an overseas third party. Section 6(1)(g) of PIPA states:

> "*An organisation may use an individual's personal information [if]..*
>
> *(g) 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 organisation or in a third party to whom the personal information is disclosed"*

There are well-established international precedents which expressly account for circumstances concerning the transfer of personal information to an overseas third party and the protection of "public interest". It may be reasonably concluded that there is a genuine public interest in ensuring that financial service providers "using" personal information in Bermuda do not engage in conduct overseas that would constitute a violation of law if performed in Bermuda.

In addition to relying on section 6(1)(g) to support the transfer of personal information to an overseas third party, depending on the facts of the matter an organisation may further rely on sections 6(1)(c),(h) and 6(3) of PIPA. There may be circumstances where individual consent to transfer their personal information to an overseas third party may be implied.

Section 6(1)(c) of PIPA states:

> "(6) *... an organisation may use an individual's personal information only if or more of the following conditions are met -*
>
> *(c) The use of the personal information is necessary -*
>
> *(i) For the performance of a contract to which the individual is a party; or*
> *(ii) For the taking of steps at the request of the individual with a view to entering into a contract.*

Upon review of section 6(1)(h) of PIPA, it is understood that the practical scope of its application is limited to circumstances where the transfer of personal information to an overseas third party is directly related to employment related matters concerning the organisation. Section 6(1)(h) states:

[22] Section 9(1)(f) of the Personal Information Protection Act 2016

> "(6) *... an organisation may use an individual's personal information only if or more of the following conditions are met -*
>
> *(h) The use of the personal information is necessary in the context of an individual's present, past or potential employment relationship within the organisation.*

Where an organisation is unable to rely upon sections 6(1)(c) and 6(1)(h), an organisation may instead be able to rely upon section 6(3) of PIPA to ensure domestic and international regulatory compliance. Where the conditions stipulated under section 6(1) are unable to be met, the organisation may use an individual's personal information only if:

(a) 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 organisation;
(b) The use of the personal information is for the purpose of complying with an order by a court, individual or body having jurisdiction over the organisation;
(c) 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;
(d) The use of the personal information is necessary in order to collect a debt owed to the organisation or for the organisation to repay to the individual money owed by the organisation;
(e) The use of the personal information is in connection with the disclosure to the surviving spouse or a relative of a deceased individual if, in the reasonable opinion of the organisation, the disclosure is appropriate; or
(f) The use of the personal information is reasonable to protect or defend the organisation in any legal proceeding.

PrivCom is of the view that Bermuda's financial service providers are likely to rely on section 6(3)(a),(b),(d) and (f) in the event that the conditions stipulated under sections 6(1)(c) and (h) are unable to be met. In support of the aforementioned conditions for the transfer of personal information to an overseas third party, an organisation must meet the performance obligations stipulated under section 15 if PIPA.[23] Section 15(1) of PIPA states:

> *When an organisation transfers to an overseas third party personal information for use by that overseas third party on behalf of the organisation, or for the overseas third party's own business purposes, the organisation remains responsible for compliance with* [PIPA] *in relation to that personal information"*

During the consultation process an industry stakeholder asked whether PrivCom has considered the interplay between PIPA and sections 29(3) and (5) of the Electronic Transactions Act 1999 and the

[23] Section 6(4) of the Personal Information Protection Act 2016

Safe Harbor Guidelines contained therein. The overlap between PIPA and the ETA has since been updated through the enactment of supplementary regulations.

Like much of PIPA, the provisions of section 15 contain a great deal of flexibility to afford organisations the ability to meet their operational and administrative obligations. Before transferring an individual's personal information to an overseas third party, the organisation must assess the level of protection provided by the overseas third party for that personal information.[24] This means the organisation is obligated to use its judgment and undertake appropriate measures intended to assess and understand how the third party will "use" the information and what safeguards are in place.

Since the transfer of personal information to an overseas third party will likely result in the "use" of personal information outside of Bermuda, it may be argued that the overseas third-party would fall outside the reach of PIPA. However, such a commercial arrangement does not absolve the organisation of their obligation to comply with PIPA.[25] An organisation that procures the services of a third-party to "use" personal information on their behalf is responsible for ensuring that the third party "uses" the personal information provided by the organisation in accordance with PIPA, irrespective as to whether the third-party is domiciled in Bermuda or overseas.

When performing its third-party assessment, the organisation must consider the level of protection afforded by the law applicable to the overseas third party.[26] For example, an organisation's assessment of risk associated with a data transfer to an overseas third-party regulator in the US may include an evaluation of the US Privacy Act of 1974, as amended, the US E-Government Act of 2002, and other Federal privacy laws, regulations, standards, and guidance. Considering these requirements in conjunction with the regulatory provisions outlined in PIPA, an organisation may be able to reasonably conclude that the US's data privacy legislative framework provides comparable levels of protection for personal information.

As part of its determination, an organisation may also consider whether the Minister has designated the jurisdiction within which the overseas third party operates as providing a comparable level of protection as found under PIPA. At this stage the Minister has not designated any jurisdictions as providing a comparable level of protection to that of PIPA. Following such a determination by the Minister, PrivCom shall publish on its website a register of comparable jurisdictions on PrivCom's website for the benefit of industry stakeholders.

For the avoidance of doubt, a formal designation by the Minister declaring that a jurisdiction's law is "comparable" to PIPA (sometimes called "adequacy decisions" by other jurisdictions) would address only one element of section 15: whether the level of protection afforded by the law applicable to an overseas third party is comparable. If such a designation is made by the Minister, then the requirement under section 15(3) to conduct an assessment of the law applicable to a prospective overseas third-party

[24] Section 15(2) of the Personal Information Protection Act 2016
[25] Section 5(3) of the Personal Information Protection Act 2016
[26] Section 15(3) of the Personal Information Protection Act 2016

service provider does not apply. The organisation should proceed to evaluating the business practices of the recipient.

In addition to assessing the law applicable to the overseas third party (i.e. laws, regulations, standards and guidance that are applied by the domestic and/or federal regulator), an organisation may also consider certification mechanisms recognised by PrivCom as evidence of such a level of protection. To date, the only certification mechanism recognized by PrivCom is the Cross Border Privacy Rules System (CBPR) overseen by the Global CBPR Forum. Organisations are invited to refer PrivCom to certification mechanisms whose recognition would be useful.

If an organisation's discretionary assessment concludes that the law applicable to the overseas third party provides a level of protection that is comparable to that of the level of protection afforded by PIPA, the organisation may reasonably conclude that the transfer to and "use" of personal information by the third party would not amount to a violation of PIPA or the data privacy legislative framework to which the overseas third party may be subject to.[27]

However, whether or not an organisation concludes that the jurisdiction of an overseas third party provides a comparable level of data privacy protection, the organisation remains responsible for compliance with PIPA and for ensuring the third party's compliance with PIPA following the procurement of the third-party's services.[28] The organisation must still assess the overseas third party's organisational administrative and technical processes and internal safeguards in order to determine that the overseas third-party's operational practices are secure and effectively provide a level of protection that satisfies the organisation's obligations under PIPA.

If following its assessment an organisation determines that the operational practices undertaken by the overseas third party do not provide an adequate level of protection, the organisation may choose to employ one of the mechanisms outlined under section 15(5) of PIPA. Where an organisation's assessment concludes that the data privacy law applicable to an overseas third party is not consistent with the level of data privacy protection afforded under PIPA, the third party's level of protection may be supplemented through the employment of contractual mechanisms, corporate codes of conduct including binding corporate rules, or other means.

During the consultation process an industry stakeholder responding to the Consultation Document stated that in standard contract clauses approved by foreign regulators there are concepts and requirements that are not included within the PIPA regulations (i.e., data processor/controller). Industry stakeholders further asked whether the inclusion of data protection clauses in their standard operating contracts would be considered a good faith attempt to comply with section 15(5) of PIPA.

PrivCom is of the view that the inclusion of such contractual terms and conditions would satisfy section 15(5). PIPA does not state that data protection contractual clauses adopted by an organisation

[27] Section 15(4) of the Personal Information Protection Act 2016
[28] Section 15(1) of the Personal Information Protection Act 2016

must first be approved by PrivCom before they may be relied upon by an organisation although such an approval process is considered common practice in other jurisdictions to ensure regulatory certainty.

In order to establish regulatory certainty for industry stakeholders, PrivCom has elected to undertake a review of the most commonly used data protection contractual terms and conditions in the United Kingdom and Europe and identify any contractual terms and conditions that would be considered to run contrary of PIPA, while bearing in mind the cost and burden that any change from standard practice may incur on the business community.

The purpose of such a comparative exercise is to develop a set of data protection standard contractual terms and conditions that may be relied upon by organisations that "use" personal information in Bermuda. Until PrivCom's guidance on standard contractual clauses is released, organisations are advised to use standard contractual clauses approved by data protection regulators outside of Bermuda. Doing so would amount to a good faith attempt to comply with section 15(5).

PIPA does state that binding corporate rules, or personal information protection policies adopted by an organisations seeking to transfer personal information to an overseas third party, are to be approved by the Commissioner.[29] PrivCom intends on undertaking a future consultation process with the intention of developing a set of industry specific binding corporate rules and a process for approving organisational information protection policies.

In conjunction with the aforementioned consultation, organisations will be asked to participate in a Pilot Programme on binding corporate rules. Until such a process is finalized, organisations should document their good faith efforts but should not rely solely on the use of corporate binding rules as a means of ensuring compliance with section 15(5) of PIPA.

Recognizing the regulatory performance obligations imposed under sections 15(1)-15(5) of PIPA, it is important for Bermuda's financial service providers to be mindful of the administrative exemptions stipulated under section 15(6) of PIPA. An overseas transfer may circumvent the administrative processes stipulated under section 15(1)-15(5) of PIPA in circumstances where:

(a) The transfer of personal information to an overseas third party is necessary for the establishment, exercise or defense of legal rights; or
(b) The organisation assess all of the circumstances surrounding the transfer of personal information to an overseas third party and has reasonably concluded that the transfer of personal information is:
    (i) Small-scale;
    (ii) Occasional; and
    (iii) Unlikely to prejudice the rights of an individual.

[29] Section 29(g) of the Personal Information Protection Act 2016

However, in order for an organisation to rely upon section 15(6) of PIPA, the organisation must be able to document that the transfer is not large scale, that it is not a systematic transaction expected to occur regularly in conjunction with the organisation's day-to-day operations, and that it can be reasonably concluded that the overseas third-party recipient is a permitted recipient of individual's person information. This exemption may only be considered on a case-by-case basis and that an organisation should not broadly apply this exemption through blanket application. Doing so would be by its very nature systematic and not occasional.

Following completion of the consultation process, PrivCom is of the understanding that Bermuda's financial service providers do not typically engage in transfers of personal information with overseas third parties and that such transactions are generally irregular and unpredictable. To avoid the unintended regulatory consequence of being disproportionately prescriptive, any determination as to whether a data transfer is considered "small scale" will be dependent on the facts of the matter and its contextual circumstances.

What may be considered a "large scale" transfer of individual personal information in Bermuda may be considered a "small scale" transfer for an overseas third party which is domiciled in a foreign jurisdiction whose local population dwarfs Bermuda's local resident population in comparison. Under PIPA this would not be a "small scale" transfer. Likewise, a transfer that consists of information related to every life event from birth for a single individual would not be small scale.

In light of the contextually subjective application of section 15(6) of PIPA, PrivCom advises organisations to assess their circumstances and position themselves to be able to demonstrate that responsible decision-making is undertaken when transferring personal information to an overseas third-party. Transfers that consist of a limited number of specific records for an individual would likely be considered small scale, as would similar transfers for a small, defined group of individuals.

The question of whether a transfer of information to an overseas third-party would likely prejudice the rights of an individual is also a subjective question of fact and circumstance. PrivCom is of the view that the term "rights" should be interpreted to broadly to mean privacy rights, human rights, criminal rights, or other rights as defined under the Human Rights Act 1981. For comparison, in other jurisdictions, similar provisions to section 15(6) prohibit a transfer if doing so would adversely affect an individual's "interest".

Since the use of personal information for the purposes of ensuring compliance with overseas regulations would arguably serve a Bermudian public interest function, it is important to highlight the exemptions outlined under section 24(2)(a) of PIPA.

Except for the "minimum requirements" of PIPA, Parts 2 and 3 of PIPA do not apply so long as compliance with Parts 2 and 3 does not prejudice the proper discharge of any of the following "relevant functions":

> "*(a) To protect members of the public against –*

(i) *Financial loss due to dishonest, malpractice or other seriously improper conduct by, or the unfitness, impropriety or professional incompetence of, individuals concerned in the provision of banking, insurance, investment, trust or other financial services or in the management and ownership of an organisation;*
(ii) *Financial loss due to the conduct of discharged or undischarged bankrupts; or*
(iii) *Dishonesty, malpractice or other seriously improper conduct by, or the unfitness or professional incompetence of, individuals authorized to carry on any profession or other activity;*

Given the intended purpose of section 24(2)(a) of PIPA is to protect public interests, compliance exceptions may be relied upon by an organisation so long as doing so would not prejudice the discharge of such public interests. Furthermore, PrivCom reserves the right to investigate and make orders, as appropriate.

PrivCom has released more extensive guidance on section 15. In short, organisations must consider the law that applies to the overseas third party and must reasonably consider whether the level of data privacy protection provided by the third party is comparable to PIPA. If not, the organisation may proceed but must employ mechanisms to create such protection. These are two separate questions that require an organisation to conduct a fully comprehensive review of the data protection legal framework applicable to the overseas third-party, as well as undertake a due diligence assessment of the third-party and its operational practices (i.e. a privacy risk or impact assessment).

11. Breach of Security Reporting Obligations

Respondents to the Consultation Document expressed the view that PIPA breach notification obligations under PIPA could be aligned with similar obligations imposed by other domestic or overseas regulators.

In the case of a breach of security leading to the loss or unlawful destruction or unauthorized disclosure of or access to personal information which is likely to adversely affect an individual, section 14(1) of PIPA requires the organisation responsible for that personal information to, without undue delay:

(a) Notify the Commissioner of the breach; and
(b) Notify any individual affected by the breach.

In the immediate term, the alignment of breach notification standards with other domestic or overseas regulators presents a challenge because the different laws and regulations that apply will use differing definitions and triggers (i.e. even foreign privacy data legislative frameworks may set different thresholds for notification).

The obligation for organisations to report a breach "without undue delay" has been interpreted by PrivCom in such a way to give companies flexibility in the middle of a crisis event and is not necessarily intended to be more onerous than breach reporting rules in other jurisdictions. However, the question of whether a delay is "undue" may ultimately depend on the facts of the matter and will be determined on a case-by-case basis.

If an organisation is aware of a likely adverse effect to an individual that would have otherwise been mitigated by taking measures sooner, then the organisation should make reasonable efforts to notify the Commissioner and the individual affected. The sensitivity of the personal information and the potential for harm to an individual will affect whether a delay will be considered reasonable.

PrivCom's long-term regulatory strategy is to ease compliance requirements through an interoperability approach that will align PIPA's requirements to those of other domestic regulators and data protection regulators in other jurisdictions to the extent allowed by law.

12. Other Exclusions and Provisions

Under section 4(1)(c) of PIPA, business contact information is excluded if it is used for purpose of contacting an individual in his or her capacity as an employee or official of an organisation. If business contact information is used for any purpose other than to serve as a point of contact, reference, or directory, then PIPA may apply.

Section 4(1)(g) of PIPA states that PIPA does not apply where personal information is contained in a court file and used by a judge of any court in Bermuda or used as part of judicial administration or relating support services provided to the judges of any court of Bermuda, but only where such personal information is necessary for judicial purposes. This exclusion is limited to use by a judge or for judicial purposes.

If personal information is used by another organisation or for another purpose, then PIPA may apply. Section 4(3) of PIPA states that the action shall not apply so as to: (a) affect any legal privilege; (b) limit the information available by law to a party to any legal proceedings; or (c) limit or affect the use of information that is the subject of trust conditions or undertakings to which a lawyer is subject.

Under PIPA section 46, organisations may use personal information for the purposes of a "business transaction," defined broadly to include a purchase, sale, lease, merger or any other type of acquisition or disposal. This section provides for uses without the consent of the individual when personal information is necessary to proceed with the business transaction.

13. Conclusion

It is a testament to the drafting and approach taken to the PIPA that no material issues were identified regarding the application of PIPA, particularly with respect to the commercial and administrative activities of organisations operating within Bermuda's financial services sector. An independent assessment determined that PIPA is fit for purpose for governmental, commercial, and societal purposes with respect to Bermuda's financial service sector.

Potential challenges pertaining to an organisation's ability to process some types of personal information and/or the sharing of the data within organisations, between organisations, and across borders are adequately addressed by PIPA sections 6 (Conditions for using personal information), Section 7 (Sensitive Personal Information), Section 15 (Transfer of personal information to an overseas third party) and Section 25 (General Exemption).

PrivCom has also established a constructive stakeholder engagement mechanism and consultation process with financial service providers in Bermuda and with domestic and overseas regulators. PrivCom is of the view that the establishment of such mechanism for cross-regulatory engagement shall enable PrivCom to:

(i) Facilitate effective future stakeholder engagement;
(ii) Track the progress of PIPA implementation;
(iii) Provide iterative guidance and FAQs as needed; and
(iv) Address evolving issues.

This proactive approach to stimulating stakeholder engagement has created a positive dynamic for cooperation and collaboration in Bermuda between regulators and Bermuda's financial services sector. Proactive engagement with Bermuda's financial services stakeholders has the potential to offer PrivCom the capacity to support further preemptive regulatory action specifically intended to support commercial and regulatory innovation.

Rather than adopt a "wait and see" regulatory approach, PrivCom's attitude towards the enforcement of Bermuda's data protection legislative framework is a "listen, learn, and engage" approach, which has arguably resulted in improved awareness and understanding of PIPA for businesses in Bermuda and a better understanding by PrivCom of business entities.

Through careful drafting of PIPA and proactive guidance, Bermuda appears poised to avoid many of the regulatory obstacles experienced in other jurisdictions when a new horizontal legislation comes into effect which impacts both personal and business lives.

APPENDIX A

Consultation Letter

From: Alexander White <amw@privacy.bm>
Sent: Wednesday, March 6, 2024 9:28 PM
To: The Office of the Privacy Commissioner <PrivCom@privacy.bm>
Subject: Save-the-dates: call for input regarding privacy guidance

CAUTION: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear colleagues in financial services,

I am pleased to reach out to you on the important topic of how data privacy interacts with your work, and I request your assistance with ensuring this messages reaches a variety of stakeholders.

Our office is seeking input from the community regarding areas of concern or gaps that map need to be addressed in the new regime. I have often said that developing guidance on best practices should be a collaborative, multi-stakeholder process, and that the best way we can protect individuals' privacy rights is by ensuring the practices make business sense, too.

You are invited to provide your input by 15th March and to participate in a meeting on 25th March to discuss and explore the intersection of the pending Personal Information Protection Act ("PIPA") ht t ps:/ / www.pri vacy.bm / , due to come into effect on 1st January 2025, and financial obligations under the relevant AML/financial crime legislation, such as https://www.bma.bm/document-centre/policy-and- gui dance- am l- atf . The aim is to identify any areas of potential inconsistency or gaps which may need to be addressed to ensure that both legislative and regulatory requirements complement each other, enabling our businesses to operate efficiently, effectively and with regulatory certainty.

Financial services is an important sector Bermuda, and the largest contributor to the Bermudian economy. With Bermuda's PIPA due to come into effect on 1st January 2025 (joining 2/3 of all other countries with privacy legislation), the countdown is on the ensure not only appropriate operationalisation of the Office of the Privacy Commissioner (PrivCom), but also to review how the PIPA interacts with existing legislation, regulation, and regulators. Our goal is to ensure a collaborative and coherent approach between PrivCom and other regulators to enable a joined up approach to data regulation and help to avoid overlapping or divergent approaches or duplicate enforcement.

The purpose of the meeting scheduled for 25th March 2024 is to reflect on the contributions requested of each of the sectors subject to anti-financial crime obligations by 15th March 2024 to provide their comments on any areas which may require clarification or guidance on the intersection of the PIPA and other requirements.

The meeting on 25th March will be hosted by my office and led by Vivienne Artz OBE, Senior Data Strategy & Privacy Policy Advisor to the Centre for Information Policy Leadership and specialist in the privacy and anti-financial crime issues.

The outcome is to identify and create an action plan to address any areas of concern to ensure a smooth transition of the PIPA into effect on 1st January 2025 for our businesses in Bermuda.

We will shortly be sending out to you a brief paper setting out potential areas for consideration for your feedback to assist you in this process. In the meantime, you may wish to consider the following specific issues in formulating your response:

- Do the conditions for personal data use in section 6 of PIPA meet the needs for data processing under anti-financial crime requirements? Note that consent is not generally regarded as an appropriate basis for processing in the context of anti-financial crime.
- Personal data processed for anti-financial crime purposes includes sensitive personal information (section 7 PIPA). Are the purposes of use of sensitive personal data wide enough and specific enough to include anti-financial crime?
- Are the exemptions in Part 4 of PIPA sufficient, particularly the "General Exemption," to cover both reactive and proactive processing of personal and sensitive personal data for anti-financial crime purposes? See section 25 for details
- Anti-financial crime is a global issue, and regular transfers of significant amounts of data need to be shared both within companies and with their service providers, regulators and others. Do the provisions of section 15 of PIPA support such data sharing outside of Bermuda?

We look forward to hearing from you on this important issue. In the interim, please can you ensure that both dates are in your diary:

Deadline for feedback: 15 March 2024

Meeting: 25 March 2024

Format: Virtual; log-in link to be distributed based on the RSVP

RSVP: By replying to PrivCom@privacy.bm.

Thank you for your willingness to offer your insights so that we may best meet the goals of PIPA while ensuring that, as we say, "Privacy Means Business."

Alex

Alexander McD White (Mr. | he/him)

Privacy Commissioner

Privacy Commissioner
Bermuda | Quo Data Ferunt

APPENDIX B

Submitted Case Study Examples

1. Certain policyholder information contained within reinsurance transaction documents

Context: A Bermuda exempted company licensed as reinsurer ("**BDA Re**") which is operating in Bermuda with physical premises and employees, and carrying out reinsurance/retrocession transactions with third party cedants, for example, a Japanese insurer. BDA Re's approach in such transactions (and ancillary transactions) is generally to not accept, share or exchange any personal information, and their intent is that this approach will be unchanged post-PIPA effectiveness. In the course of its business, BDA Reenters into certain reinsurance agreements with the Japanese insurer which include a definition of "personal information", and BDA Re is considering broadening the definition of "personal information" on the basis that any use of personal information in Bermuda (even if such information is received unintentionally and potentially in breach of such agreement) could give rise to obligations under PIPA.

From BDA Re's perspective, they are conscious that broadening the scope of how personal information is defined under their reinsurance agreements may leave them open to certain additional risks including BDA Re itself inadvertently breaching this personal information provision, and triggering the Japanese insurer's recapture right (a provision that gives the cedant insurer an option to recapture upon an event or trigger occurring).

Question: Would policy ID numbers and/or post codes related to individual Japanese policyholders of policies reinsured to BDA Re as part of a reinsurance transaction with the Japanese insurer be considered personal information under PIPA (i.e. if BDA Re received this information from the Japanese insurer, would it be considered personal data under PIPA)? In the event, BDA Re received personal information from the Japanese insurer in breach of its reinsurance agreement, what would be the expectation on BDA Re (i.e. BDA accidentally receives unsolicited personal information for which it may not have applicable policies and procedures to address as it has specifically tried to avoid this event)?

Suggested Analysis: It would depend on whether the individual Japanese policyholders could be considered identified or identifiable from a document which contained only their post codes and policy ID numbers. If such document containing other information (e.g. name, DOB, etc.), then it would likely be in scope. However, where individual Japanese policyholders could not be identified from such document alone then it would be out of scope.

Where BDA Re receives personal information from the Japanese insurer in breach of its reinsurance agreement, or even if not in breach but unsolicited, provided that the occurrence is infrequent and/or accidental and the use of such personal information in Bermuda is limited to deletion of such from BDA Re's system, then such event in and of itself would not bring BDA Re within the scope of PIPA (i.e. it would not trigger obligations under PIPA where such obligations had not previously applied). BDA Re should document its processes for such scenarios to demonstrate accountability.

2. **Use of personal information by Corporate Service Provider and/ or Insurance Manager and not by the Bermuda company itself**

Context: A Bermuda exempted company as holding company or licensed as captive insurer or limited purpose insurer ("**ABC**") which has its registered office and principal addresses in Bermuda, but has no employees or physical premises in Bermuda. In compliance with the Companies Act 1981 and the Insurance Act 1978, ABC outsources certain functions to its Bermuda Corporate Service Provider ("**CSP**") and Insurance Manager ("**IM**"). ABC itself does not hold or use personal information in Bermuda, however, in compliance with applicable legislation and regulations, CSP and IM must hold and use certain personal information.

The personal information that CSP and IM must hold in Bermuda at CSP and IM's offices on behalf of ABC is limited to KYC information on directors, officers and beneficial owners. ABC maintains services agreements with each of CSP and IM. A foreign affiliate of ABC (e.g. ABC Group Inc. in New York) will procure and provide the statutory information on the ABC directors, officers and beneficial owners (all of whom are foreign individuals which are not Bermudian nationals or Bermuda resident) directly to CSP and IM. It is noted that CSP and IM must each themselves comply with their respective PIPA obligations

Question: ABC's position is that ABC itself does not use any personal information in Bermuda, and therefore it does not need to comply with PIPA as it is out of scope.

Suggested Analysis: As stated in the fact pattern, ABC itself does not use any personal information in Bermuda. CSP and IM require the directors, officers, and beneficial owners of ABC to provide statutory information (i.e. personal information) in compliance with legal and regulatory obligations of CSP and IM. Notwithstanding the contractual relationship (and obligations to procure that such directors and beneficial owners provide statutory information to CSP and IM) between ABC and CSP and IM, ABC itself does not use any personal information in Bermuda. However, depending on the facts regarding the contractual relationship this analysis may change.

3. A Bermuda company which is a licensed in Bermuda as a captive insurer ("Captive"). Once in effect, PIPA will apply to any organisation that uses personal information in Bermuda, and therefore while operating in Bermuda Captive would be obligated to comply with PIPA.

Pursuant to section 9 of PIPA, an organisation must provide individuals with a clear and easily accessible statement ("privacy notice") about its practices and policies with respect to personal information which must include the particulars set out in section 9(1)(a)-(f). Section 9(3) of PIPA provided that only in limited circumstances are organisations not obliged to provide privacy notices, which are where either (i) all of the personal information held by the organisation is publicly available information; or (b) the organisation can reasonably determine that all uses made, or to be made, of the personal information are within the reasonable expectations of the individual to whom the personal information relates.

Captive is considering whether or not it would be required to provide a privacy notice in the following scenarios where Captive receives the types of personal information from the sources and for the purposes noted below (all of which are external to Bermuda and from non-Bermudian resident persons):

1. Case 1 – Directors, Officers & Signing Officers
    1. *Source* – Provided by the individual.
    2. *Personal Information* – Name, address, passport/drivers license, date of birth, etc.
    3. *Purpose* – For registration, banking, payment, etc.
    4. *Privacy Notice Required* – Yes. PIPA does not require a specific means of delivery, but does require that the notice is clear and easily accessible and that reasonably practical steps are taken to provide the notice in advance or at the time of collection.
2. Case 2 – Insurance Claims
    1. *Source* – Provided by a third-party administrator ("**TPA**") (which is a non-Bermuda company providing operational services such as claims processing and employee benefits management under contract with Captive) or other third parties in relation to auto insurance or workers compensation claims. Insurance claims are not received directly from the individual insureds. Note that Captive effectively has no direct contact with the individuals whose personal information is being provided to and processed by Captive.
    2. *Personal Information* – Name, occupation, age, sex, drivers license, etc.
    3. *Purpose* – Processing auto or workers compensation insurance claims.
    4. *Privacy Notice Required* – No, as Captive would rely on section 9(3)(b) of PIPA. Captive should retain records to demonstrate its reasonable determination, such as the notice in which the insured was informed.

3. Case 3 – Conducting Litigation

    1. *Source* – Provided by a TPA or directly from claimants who are litigants (i.e. in general liability suits for which they are conducting the lawsuit, and noting that discovery in such lawsuits would be protected by something other than personal information protection legislation). Note that Captive may not have any direct contact with the individuals whose personal information is being provided to and processed by Captive.
    2. *Personal Information* – Name, occupation, age, sex, drivers license, etc.
    3. *Purpose* – Defending claims or conducting litigation.
    4. *Privacy Notice Required* – No, as Captive would rely on section 9(3)(b) of PIPA. Captive should retain records to demonstrate its reasonable determination, such as the lawsuit papers or official court records and may redact other information.