APPLEBY

# DATA PROTECTION GUIDE 2022: BERMUDA

PUBLISHED: 15 SEP 2022

TYPE: LEGAL GUIDE

PRIMARY CONTACT

Duncan Card

PARTNER: BERMUDA

**T** +1 441 298 3270
**E** Email Duncan

PRIMARY CONTACT

Jerome Wilson

PARTNER, HEAD OF TECHNOLOGY & INNOVATION: BERMUDA

**T** +1 441 298 3559
**E** Email Jerome

## PRIVACY, DATA PROTECTION & CYBERSECURITY REGULATION OVERVIEW

Bermuda's laws and regulations concerning the protection and use of personal information, data, and related cybersecurity risk management, currently exists across several statutes and regulations. Several areas of law are now converging to regulate the privacy, security, integrity and reliability of information in the Bermuda economy. Even though Bermuda is a British Overseas Territory (pursuant to the British Overseas Territory Act 2002), domestic privacy and data protection laws are within the constitutional authority of the Bermuda Government. The European Union's (EU) laws and regulations concerning privacy and data protection (EU's General Data Protection Regulation) have also not been enacted in Bermuda. However, the Bermuda Government is cognisant that a "safe harbour" or "adequacy" status, as determined by jurisdictions that have data export restrictions (such as the EU), would be highly beneficial for

international business in Bermuda. The following is a survey of Bermuda's current and expected privacy, data protection, and cybersecurity laws and regulations.

For more on our related legal services, see *Information Technology, Outsourcing, Privacy & Data Protection – Bermuda*.

## ELECTRONIC TRANSACTIONS ACT 1999 (ETA)

In 1999, Bermuda enacted legislation to legally facilitate e-commerce business and operations, which included a set of EU-style "data protection principles", including the concepts of "personal data" and "data processor" among them.

The ETA governs a very broad range of transactions carried out by electronic means and expressly addresses, in part, "electronic records" (any record created, stored, generated, received or communicated by electronic means) and "personal data" (any information relating to an identified or identifiable natural person). Since 1999, the types and scope of business and commercial activities conducted over the internet, and governed by the ETA, has ubiquitously expanded across all sectors and enterprises. Online business as we know it today is no longer the narrow domain of what was narrowly referred to in 1999 as "e-commerce".

Part VI of the ETA, titled "Data Protection", permits the Government to creation of a regime of standards for the use and processing of personal data in the hands of "data controllers" and "data processors". In May 2000, the Bermuda Government prescribed the "Standard for Electronic Transaction" pursuant to Sections 29(3) and 29(5) of the ETA (the **Privacy Standards**). The Privacy Standards include specific personal information protection requirements and obligations, including the following prescriptions for those who are involved in "transactions" (a term not defined by ETA) involving the storage, use or processing, in part, of personal data:

- Section 4(A)(iv) – Protect Personal Data and to respect the privacy, accuracy and security of personal information in accordance with the ETA;
- Section 7(A) – titled, Maintenance of Effective Monitoring Systems;
- Section 7(D) – titled, Establish Systems to Protect Privacy, which includes the following prescriptions:

(i) intermediaries and e-commerce service providers should collect personal data of customers only:

- if relevant for the provision of goods, services or information as agreed with the customer only; and
- as otherwise disclosed to the customer prior to collection of such information.

(ii) intermediaries and e-commerce service providers should use personal data and business records of customers only for:

- internal marketing, billing or other purposes necessary for the provision of services;

- purposes made known to the customer prior to the time the personal data or business records are collected; or
- other purposes with the prior consent of the customer

(iii) intermediaries and e-commerce service providers should endeavour to ensure that the personal data or business records:

- are accurate and if necessary, kept up to date;
- if accurate, are erased or rectified;
- are erased when no longer reasonably required; and

(iv) intermediaries and e-commerce service providers should endeavour to:

- ensure the confidentiality of personal data and business records or customers;
- prevent the sale or transfer of the personal data and business records of customers other than as part of the sale of the intermediaries' or e-commerce service providers' business; and
- prevent the examination of or tampering with personal data or business records other than for the purposes of maintenance or security of the relevant information processing system or data integrity.

The Privacy Standards do not prohibit the disclosure of personal information or business records:

- where the express or implied consent of the person to whom such personal data or business records relates has been secured; or
- as required by law.

However, it is important to note that only Section 7(D) of the Privacy Standards will not apply to the extent any other law or more onerous obligations of confidentiality related to personal data may apply, whether by statute, common law or in equity.

# PERSONAL INFORMATION PROTECTION ACT 2016 (PIPA)

## INTRODUCTION

PIPA received Royal Assent in July 2016 and applies to all organisations in Bermuda that use personal information. With ties to privacy and data protection laws on both sides of the Atlantic, but with a particular reliance on Canadian statutory precedent, PIPA was drafted as a privacy framework to meet Bermuda's unique public policy requirements.

PIPA's administrative provisions came into force in December 2016 to enable the establishment of a Privacy Commission (including the appointment of a Privacy Commissioner). However, the substantive provisions concerning the privacy of personal information in PIPA has not yet been proclaimed into full force in order to allow for a transitional period to permit the readiness of the business community and to allow for the issuance of interpretive guidance to help organisations in Bermuda achieve compliance. As at the date of this Guide's publication (September 2022), the Privacy Commissioner has issued several PIPA guidance publications, and held various PIPA compliance training and educational programmes. Further interpretive guidance concerning PIPA from the Privacy Commission are anticipated before PIPA is fully proclaimed into force.

It is also anticipated that when the Bermuda Government proclaims all of PIPA into force, the overlapping data privacy provisions of the ETA that are currently in effect may be repealed.

PIPA enacts a set of jurisdictional "data protection principles" that are found across numerous jurisdictions, all with the express intention of securing EU and international "adequacy" and "safe harbour" status for personal information to move freely between Bermuda and the rest of the world. Following PIPA's proclamation into force, it is expected that applications to the EU and other jurisdictions will be made by the Privacy Commissioner for "adequacy" status.

PIPA does not adopt the "data controller", "data subject" or "data processor" nomenclature of EU data protection law, referring instead to the more North American terminology of "organisations", "individuals" and "third parties". PIPA does reflect the international principle that the "organisation" – defined as any individual, entity or public authority that uses personal information – is responsible for ensuring compliance with Bermuda's privacy laws at all times. It is important to note that enterprises that perform services to process personal information on behalf of organisations are not directly regulated under PIPA. Organisations can delegate the use of personal information to data processing service providers but organisations cannot delegate their PIPA responsibilities and regulatory accountability to others.

# PERSONAL INFORMATION

"Personal Information" is defined as "any information about an identified or identifiable individual".

PIPA applies to every organisation that uses personal information in Bermuda, and all personal information that is collected by such organisations must be collected and used in a lawful and fair manner. Organisations must further ensure that all personal information that is used is accurate and be kept up to date. Any personal information that is collected must be adequate, relevant and not excessive in relation to the purposes for which it is used. Personal information must not be retained for longer than is necessary. With regard to personal information retention, PIPA is not merely suggestive but mandatory in its prohibition that it must not be kept for longer than is necessary for the purposes for which such data is collected and used.

Organisations are required to formulate and adopt both:

- suitable measures and policies to give effect to their obligations, and to the rights of individuals, under PIPA (section 5(1) of PIPA); and

- provide individuals with a notice about its practices and policies concerning personal information. Those are very distinct obligations, and both are requirements of PIPA.

Organisations have transparency obligations that include the obligation to provide a "privacy notice" to individuals with a statement about its practices and policies concerning personal information. For example, the statements should have the following characteristics/information (among others):

- must be clear;
- must be easily accessible;
- must include a statement about its practices and policies concerning personal information (see below (l);
- must include the fact that personal information is being used;
- must state the purposes for which personal information is or might be used;
- must disclose the identity and types of individuals or organisations to whom personal information might be disclosed;
- must disclose the identity and location of the organisations posting the privacy notice using the personal information;
- must disclose information on how to contact the organisation concerning the organisation's handling of personal information;
- must name the appointed privacy officer;
- must disclose the choices and means the organisation provides to an individual for limiting the use, accessing, rectifying, blocking, erasing and destroying of an individual's personal information;
- must "take all reasonably practicable steps to ensure" the privacy notice is provided before or at the time the personal information is collected;
- the privacy notice's disclosure of the particular practices and policies that are delineated in section 9 (1) and (2) concerning the collection, storage, use and disclosure of personal information is not exhaustive. Therefore, there are other material PIPA requirements that organisations may also wish to disclose.

Small businesses will find helpful assurance in PIPA's stipulation that a privacy notice is not required where the small business' use of personal information will be within the reasonable expectations of the individual to whom such personal information relates. As well, section 11 of PIPA further provides that all

organisations, including small businesses, must ensure that the personal information that they collect and use is adequate, relevant and not excessive for the purposes for which it was gathered and used.

## COLLECTING PERSONAL INFORMATION

Subject to certain limited exceptions, such as where the use is necessary to comply with a court order, organisations can only collect or otherwise use personal information where one or more of the following conditions are met:

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

The use of personal information means carrying out any operation on personal information, including collecting, obtaining, recording, holding, storing, organising, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or otherwise making available, combining, blocking, erasing or destroying it. However, that delineation may not be exhaustive and may include commercial exploitation, reliance upon for business purposes and in order to undertake assessments, and to engage in marketing activities.

Currently, as a matter of corporate governance best practice and in anticipation of PIPA's proclamation into full force, many organisations have posted privacy notices that they may have "borrowed" from affiliated companies outside of the jurisdiction. However, before PIPA is proclaimed into full force, those organisations will want to review and revise where necessary those privacy notices to bring them into bespoke compliance with PIPA.

## WHAT CONSTITUTES VALID CONSENT?

Organisations who wish to rely on an individual's consent to use their personal information are required to provide clear, prominent, easily understandable, accessible mechanisms for the individual to give consent. However, as noted, organisations are not obliged to provide such mechanisms where it can be reasonably implied from the individual's conduct that they consent to their personal information being used for the purposes that they have been notified of. However, organisations cannot rely on implied consent in relation to the use of sensitive personal information (see below).

When an individual consents to personal information disclosure by an intermediary for a specified purpose, that individual will be deemed to have consented to the use of that personal information for the specified use purpose.

An individual will also be deemed to have consented to the use of their personal information for the purpose of coverage or enrolment under an insurance, trust, benefit or similar plan, if the individual has an interest in or derives a benefit from that plan.

Personal information already under an organisation's control as at the date PIPA comes into full force will be deemed to have been collected with the individual's consent. Therefore, personal information may continue to be used for the purposes for which it was collected. However, an individual's consent for the collection and use of their personal information is not irrevocable. Organisations should be prepared to address individuals that may wish to expressly withdraw their consent when PIPA comes into force.

Individuals have the express right under PIPA to request organisations to cease using their personal information : for the purpose of advertising, marketing or public relations; where such use is causing (or is likely to cause) substantial damage, substantial distress to the individual or to another person; or where the personal information is no longer relevant for the purposes of its use.

## SENSITIVE PERSONAL INFORMATION

PIPA, like its North American counterparts, recognises the sensitivity and confidentiality of personal information lies on a continuum of both degree and corresponding regulatory oversight. Therefore, PIPA includes a category of "sensitive personal information" (**SPI**) that demands special treatment. SPI includes information relating to an individual's race, national or ethnic origin, colour, sex, sexual orientation, sexual life, marital status, physical or mental disability, health, family status, religious beliefs, political opinions, trade union membership, and biometric or genetic information. Biometric information is defined as information relating to the physical, physiological or behavioural characteristics of an individual which allows his unique identification, such as facial images or fingerprint information.

Both SPI and all other personal information must be protected and kept secure in a manner "that shall be proportionate" and "appropriate", in part, to the sensitivity of the personal information collected, stored and used by organisations. Therefore, organisations must be cognisant of the additional security safeguards required for sensitive personal information under PIPA. Such proportional safeguards might involve: obtaining separate consent; increased IT security; more frequent security testing and oversight; more onerous security and protection measures contractually imposed on third party data processors; or perhaps even data segregation and enhanced encryption solutions. Organisations retaining third-party service providers to store, process, use or otherwise manage any SPI, whether those service providers are domestic or overseas, must ensure the terms and conditions of those service contracts properly, adequately and robustly reflect (and flow down) the onerous nature of the organisation's duties, requirements and statutory obligations to safeguard and protect such SPI.

## RETENTION OF PERSONAL INFORMATION

Organisations must ensure the personal information they hold is accurate, kept up to date and is not retained longer than is necessary to fulfil the original collection purpose. PIPA does not prescribe data retention periods. Therefore, an assessment will need to be undertaken to determine how long personal information may be legally required to be kept in order to comply with a broad range of PIPA's and other legal requirements, as well as how long it should be retained in accordance with PIPA's "necessity of purpose" test. For example, business records containing personal information may be subject to a broad range of retention term requirements, including employment, as potential evidence in litigation or dispute resolution, or for other regulatory reasons.

## ACCESSING PERSONAL INFORMATION

Individuals are entitled to access and correct their personal information, and to direct that their personal information not be used for advertising, direct marketing or public relations (as noted above).

Individuals have the right to request access to:

- personal information about the individual in the organisation's custody or control;
- the purposes for which the personal information has been and is being used by the organisation; and
- the names or types of persons to whom, and circumstances in which, the personal information has been and is being disclosed.

PIPA does not clearly stipulate whether or not an individual can require the organisation to provide access to only a delineation of the personal information about the individual that has been collected, shared and used by the organisation; or if the organisation is required to provide the individual with access to the actual records or documents in which such personal information is contained. Subject to the issuance of guidance on this topic, it is arguable that the public policy objectives of PIPA achieved as long as an individual can view, correct, qualify, clarify, augment or add to such information, which can be disclosed to the individual

without having to provide the records and documents in which such personal information resides. Such records and documents will often (if not always) contain unrelated confidential and proprietary information of the organisation that would require time-consuming and expensive redaction. The organisation may choose to provide a copy of any such document but it is unclear (at this time) if it is obliged to do so.

When a personal information access request is delivered in writing by an individual to an organisation, the organisation must respond within 45 days. This may be extended by up to 30 days in certain circumstances, including where a large amount of personal information has been requested. The organisation is entitled to charge a reasonable fee for processing the request which may be payable before providing any such access.

## PIPA EXCEPTIONS

Organisations should note that PIPA does not require individual consent for the processing of personal information in connection numerous situations, which include (among others):

- safeguarding national security;
- the protection of members of the public against financial loss due to dishonesty, 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; and
- the protection of charities against misconduct or mismanagement in their administration and from loss or misapplication of their property.

## WHAT HARM IS CAUSED IF PERSONAL INFORMATION IS LOST, MISUSED OR ACCESSED WITHOUT AUTHORISATION?

Section 13 requires organisations to use "appropriate safeguards" to protect the personal information it holds against the risks of loss, unauthorised access, destruction, use, modification or disclosure, and any other misuse. Those safeguards must be proportional to numerous factors, including the likelihood and severity of the harm threatened by the loss, unauthorised access or any misuse.

PIPA further stipulates such safeguards "... shall be proportional to ... the sensitivity of the personal information ... and the context in which it is held ...". In September 2021, the Privacy Commission published its guidance on the non-exhaustive types and severity of harm that may be caused, and hence the possible types of liabilities an organisation may suffer if section 13's safeguarding prescriptions are not adhered to as follows:

- Physical harm
- Reputational harm

- Relationship harm
- Economic harm
- Emotional harm
- Chilling effect
- Discrimination harm
- Thwarted expectation
- Loss of control harm
- Data quality harm
- Lack of informed choice harm
- Disturbance harm
- Loss of autonomy harm

Of particular importance for PIPA compliance, under some other business regulation genres in Bermuda, is that PIPA arguably creates onerous statutory duties, standards of care and conduct prescriptions that, if not complied with, may create direct liability for organisations to compensate and remediate individuals who have been harmed by such failure.

Organisations should note that, data processing and other third-party service providers, including other organisations acting as an intermediary for personal information transmitted by a third party, are not liable under PIPA for any breach committed while acting in that capacity. The liability distinction under PIPA entirely remains with the organisation who contracted for such services. Therefore, the organisation must secure its rights of action and compensation against the third-party service provider pursuant to the terms and conditions of the relevant service contract.

Personal information can also be disclosed as part of a business transaction consisting of:

- the purchase, sale, lease, merger or amalgamation, or any other type of acquisition or disposal of, or the taking of a security interest in respect of, an organisation or a portion of an organisation; or
- any business, activity or business asset of an organisation, and includes a prospective transaction of such a nature.

Except for the minimum requirements, the general principles and rules of PIPA Part 2, and the rights of individuals' provisions of PIPA Part 3, do not apply to several situation, including (among others):

- the prevention or detection of crime and compliance with international obligations regarding the detection, investigation and prevention of crime; and

- the economic or financial interests of Bermuda, including monetary, budgetary and taxation matters, compliance with international tax treaties, and any monitoring inspection or regulatory function exercised by official authorities for monetary, budgetary and taxation purposes in Bermuda;

to the extent that the application of those parts of PIPA would likely prejudice the conduct of any of the matters mentioned above.

## INTERNATIONAL TRANSFERS OF PERSONAL INFORMATION (E.G. OUTSOURCING)

Where an organisation provides any personal information to an overseas third party for use by that third party, whether on behalf of the organisation or for the third party's own business purposes, "the organisation remains responsible for compliance with this Act". Therefore, as a fundamental matter of PIPA compliance governance, organisations are strongly advised to ensure all of its "upstream" PIPA statutory obligations are contractually flowed "downstream" to all such overseas third-party service providers as fundamental and material obligations, duties, covenants, representations and warranties in the relevant service contract.

In addition, before personal information transfers are made to an overseas third party, the organisation must also assess:

- the level of protection actually provided by the overseas third party; and

- the level of protection afforded by the law applicable to such overseas third party.

As noted above, as a practical matter of PIPA compliance, organisations are always strongly advised to contractually ensure all of its PIPA compliance obligations are flowed down to its data processing service providers. Therefore, in all cases where it is reasonable to believe a third-party service provider may not safeguard and protect personal information in accordance with PIPA's requirements, section 15(5) of PIPA requires the organisation to "employ contractual mechanisms, corporate codes of conduct including corporate rules, or other means, to ensure that the overseas third party provides a comparable level of protection".

However, even though such compulsory contractual compliance management obligations will assist organisations to both comply with PIPA and allocate PIPA compliance risk to a service provider, that contractual transfer of risk will not diminish the organisation's most fundamental statutory responsibility to remain fully and completely liable for the organisation's unmitigated compliance with PIPA.

Where an organisation engages (by contract or otherwise) the services of a third party in connection with the use of personal information (whether domestic or overseas), the organisation remains responsible for ensuring compliance with PIPA at all times.

## PIPA'S IMPLICATIONS FOR IT SERVICE CONTRACTS

Increasingly, Bermuda businesses rely on the IT and data processing services of both domestic and overseas providers. The collection and use of personal information is a ubiquitous aspect of those services. Whether delivered as cloud services, back-office outsourcing, software (or data) "as a Service" transactions, or simply as affiliated company shared-service arrangements, the IT service contracts used for those transactions will soon become the subject of onerous legal compliance and regulatory scrutiny.

PIPA will trigger an array of regulatory restrictions and requirements, including: security safeguard requirements; proportional standards of protection; and the direct and non-transferable responsibility and liability of Bermuda organisations to comply with PIPA, regardless of what third-party IT service providers may perform, or in what jurisdiction they are performed. As a matter of both governance and risk management, and PIPA compliance, Bermuda organisations will be forced to re-evaluate and assess all of their existing and prospective IT service contracts from that new and onerous regulatory perspective.

PIPA is clear in its assertion that although Bermuda organisations can delegate the processing of data containing personal information to third-party IT service providers, they cannot delegate to others their unmitigated and direct responsibility to fully comply with PIPA's personal information use, security, and protection duties and obligations. Obviously, the situation that IT executives, in-house counsel and compliance managers want to avoid is having their organisation caught in the middle between its upstream PIPA regulatory requirements and any downstream IT service arrangements that will not satisfy PIPA's obligations.

In the event an IT service provider does not perform such contractually required PIPA obligations, only the Bermuda organisation will be: (1) held responsible and liable to compensate injured individuals and to respond to the Privacy Commission; and (2) exposed to reputational harm (which could be especially damaging if a PIPA breach concerns "sensitive personal information", as defined in PIPA).

Therefore, the most efficient risk management, commercial and legal way for a Bermuda organisation to manage such IT service provider risk and potential liability is by integrating its PIPA obligations into all of its IT service arrangements. By ensuring all of its material PIPA compliance obligations are flowed down to its IT service providers in a well-drafted and robust IT service contract, IT service providers are thereby required to become partners in assisting their Bermuda customers to comply with legal and regulatory obligations.

Only well-drafted contractual privacy protection provisions containing detailed service specifications, service performance inspection rights, requirements for Privacy Commission cooperation, clear PIPA compliance covenants, representations, warranties and indemnities can, as a practical and legal matter, allocate the risk and liability that the Bermuda organisation may suffer for the service failures of their IT service providers (whether as an arms-length or affiliated IT service provider).

# HOW IS DIRECT MARKETING REGULATED?

Bermuda has not enacted Anti-SPAM laws or regulations. However, the collection and use of personal information for direct marketing is subject to the right of an individual to request an organisation to not use, or to cease using, their personal information for advertising, marketing or public relations purposes. An individual may also request the deletion of their personal information by the organisation.

# ENFORCEMENT

PIPA establishes the Office of the Privacy Commissioner as an independent body to supervise and oversee the implementation of, and compliance with, PIPA. The exercise of the Privacy Commissioner's functions "shall not be subject to the direction or control of any other person or authority". The Privacy Commissioner's appointment for a statutorily prescribed term of five years is intended to insulate that office from governmental direction or control.

The Privacy Commissioner has a very broad range of authority to monitor and, investigate and enforce how PIPA is administered and complied with, including (in part):

- conduct investigations concerning compliance with any provision of PIPA;
- educate the public about PIPA;
- engage in, or commission, research into anything affecting the achievement of the purposes of PIPA;
- issue formal warnings, admonish an organisation and bring to its attention any failure by the organisation to comply with PIPA or agree a course of action with an organisation; and
- liaise and co-operate with domestic and foreign law enforcement agencies, and regulators to the extent necessary to ensure the purposes of PIPA are achieved provided that there is no contravention of PIPA.

The Commissioner will also be responsible for liaising with domestic and foreign law enforcement agencies, and regulators in connection with PIPA.

# WHAT ARE THE PENALTIES FOR NON-COMPLIANCE WITH PIPA?

Despite the generally remedial approach of PIPA and the compliance direction authority of the Privacy Commissioner, PIPA also creates the following offences:

(a) subject to certain exceptions, a person commits an offence if that person:

- wilfully or negligently uses or authorises the use of personal information in a manner inconsistent with Part 2, and is likely to cause harm to an individual or individuals;

- wilfully attempts to gain or gains access to personal information in a manner inconsistent with PIPA, and is likely to cause harm to an individual or individuals;

- disposes of or alters, falsifies, conceals or destroys personal information, or directs another person to do so, in order to evade a request for access to the personal information;

- obstructs the Privacy Commissioner or an authorised delegate of the Privacy Commissioner in the performance of the Privacy Commissioner's duties, powers or functions under PIPA;

- knowingly makes a false statement to the Privacy Commissioner or knowingly misleads or attempts to mislead the Privacy Commissioner in the course of the Privacy Commissioner's performance of the Privacy Commissioner's duties, powers or functions under PIPA;

- knowingly or recklessly fails to comply with section 34(1) (restrictions on disclosure by Privacy Commissioner or staff);

(b) subject to certain circumstances, a person commits an offence if that person:

- fails to comply with an order made by the Privacy Commissioner under PIPA;

- fails to comply with a notice served by the Privacy Commissioner under PIPA;

- contravenes section 7 (sensitive personal information);

- disposes of, alters, falsifies, conceals or destroys evidence during an investigation or inquiry by the Privacy Commissioner; or

- fails to notify a breach of security to the Privacy Commissioner in accordance with section 14 (breach of security) of PIPA;

(c) a person who commits an offence under subsection (1) or (2) is liable:

- on summary conviction, in the case of an individual, to a fine not exceeding $25,000 or to imprisonment not exceeding two years or to both; and

- on conviction on indictment, in the case of a person other than an individual, to a fine not exceeding $250,000.

## PIPA & CYBERSECURITY

PIPA addresses cybersecurity in the broader context of information technology regulation and other data security protocols. By requiring organisations to implement appropriate and proportional "safeguards", PIPA arguably stipulates that a broad range of factors concerning personal information security must be

considered which may involve information technology, cybersecurity, data management, personnel access restrictions and training, physical (premises) security and dedicated governance oversight related to such safeguards. As noted, those security measures are also required by PIPA in the context of personal information transfers to overseas third parties because organisations must assess "the level of protection" for personal information that such overseas third parties will provide. Sections 13 (Safeguards) and 15 (Overseas Transfer) are in Part 2 of PIPA, and section 47(1)(a) stipulates that a person commits an offence if that person "wilfully or negligently … authorises the use of personal information in a manner that is inconsistent with Part 2 and is likely to cause harm to an individual or individuals "(emphasis added).

Therefore, simple management decisions to authorise the use of personal information by overseas third parties without contractually requiring all of PIPA's Part 2 security protection prescriptions may constitute an offence under PIPA.

Security breaches leading to the loss, unlawful destruction, unauthorised disclosure of, or access to, personal information which is likely to adversely affect an individual, must be reported by the organisation to the Privacy Commissioner and the affected individual without undue delay. PIPA also prescribes what such notices must disclose.

Failure to notify the Privacy Commissioner or the affected individual without undue delay of a breach is an offence for which the penalties set out above are applicable. Therefore, it is strongly recommended that organisations ensure their existing and future third-party service contracts include provisions requiring the service provider to notify the organisation of any such security breaches in full compliance with PIPA.

# DATA PROTECTION AND INFORMATION TECHNOLOGY SECURITY OBLIGATIONS FOR FINANCIAL SERVICE PROVIDERS

The Bermuda Monetary Authority (**BMA** or **Authority**), through various statutes, is responsible for the supervision, regulation and inspection of Bermuda's financial institutions. Where regulated financial service providers, such as insurance companies, collect and use personal information (including SPI), they will be governed by both PIPA, and Bermuda's laws and regulations related to data security, information technology security and cybersecurity. In that regard, the BMA has separately mandated a series of cyber risk management codes of conduct as regulatory (or proposed regulatory) authority and requirements.

## INSURANCE SECTOR OPERATIONAL CYBER RISK MANAGEMENT: CODE OF CONDUCT, OCTOBER 2020

The Introduction to the above Code of Conduct for cyber risk management states, in part, that:

- the confidentiality, integrity and availability of information, in all its forms, is critical to the daily operation of registrants; and

- the Code is designed to promote the stable and secure management of information technology systems of regulated entities. It is deliberately not exhaustive. Registrants must be able to evidence there is adequate board visibility and governance of cyber risk.

Put into force in October 2020, the insurance/reinsurance sector code of cyber risk management contains numerous categories of data protection and IT infrastructure security for those regulated businesses including (among others):

- Cyber risk management endeavours must be proportional to the actual risks, nature of the business, and the relationship between policyholders and the registrant

- Chief Information Security Officer appointment

- The implementation of an Operational Cyber Risk Management Programme

- Managing Third-Party Service Provider Cyber Risk: the registration must ensure there is the oversight and clear accountability for all outsourced functions, and the registration must ensure that service agreements include terms on compliance with jurisdictional laws and regulations, cooperation with the BMA, and access to data and records in a timely manner (emphasis added)

- Cloud Computing risk management, including an assessment of technological risk, governance and enterprise risk, legal issues, compliance and audit, and information governance (including identification and control of data in the cloud)

- Notification of Cyber Reporting Events to the BMA, as follows:

"A cyber reporting event is defined as: Any act that results in unauthorised access to, disruption or misuse of the electronic systems or information stored on such systems of a licensed undertaking, including any breach of security leading to the loss or unlawful destruction or unauthorised disclosure of or access to such systems or information, where –

- a cyber reporting event has the likelihood of adversely impacting policyholders or clients;

- an insurer has reached a view that there is a likelihood that loss of its system availability will have an adverse impact on its insurance business;

- an insurer has reached a view that there is a likelihood that the integrity of its information or data has been compromised and may have an adverse impact on its insurance business;

- an insurer has become aware that there is a likelihood that there has been unauthorised access to its information systems whereby such would have an adverse impact on its insurance business; or

- an event has occurred for which a notice is required to be provided to a regulatory body or government agency.

- Data Protection and Governance, including the requirement that registrants that process "Personally Identifiable Information" must do so "in accordance with data protection/privacy laws relevant to each jurisdiction of operation" (i.e. PIPA upon being proclaimed into force). Arguably, that means a Bermuda registrant may also be in breach of this provision (i.e. Bermuda law) in the event it does not process personally identifiable information in compliance with the privacy laws of another jurisdiction in which it operates and processes such data.

- Penetration Testing

- Use of Cryptography

- Business Continuity and Disaster Recovery Planning

## DIGITAL ASSET BUSINESS OPERATIONAL CYBER RISK MANAGEMENT: CODE OF PRACTICE (PROPOSED DRAFT, MAY 2022)

The BMA's currently proposed Digital Asset Business Cyber Risk Management Code of Practice (July 2022) provides similar data security prescriptions as the 2020 Insurance Sector Code of Conduct. However, the following nuances for cyber risk management in the digital asset sector are proposed by the BMA (amongst others):

- Proportionality of risk must take into account whether the registrant maintains custody of clients' assets or outsources that custody

- The cybersecurity programme should outline under what condition it will hold or suspend trading, or close offending clients' accounts and notify relevant authorities

- Smart Contracts which provides as follows:

"The development of smart contracts must be subject to secure development practices (see section 6.22). In addition, smart contracts should be subject to:

- Benchmarking against a smart contract-specific vulnerability standard (e.g., the Smart Contract Weakness Classification Registry);

- A best practice security assessment relevant to the blockchain environment;

- A review of implementation risks – intrinsic errors that result in unintended smart contract behaviour (e.g., unnecessary functionality that may add vulnerabilities to code, enabling front running transactions; and

- A review of design risks – system features that are exploited to alter intended smart contract behaviour (e.g., lack of privacy).

An assessment of the security testing required must be completed before any new smart contracts are deployed. Any changes to smart contracts must also be assessed to determine what level of security testing is required."

- DLT/Blockchain Security, which provides the following:

"The use of Blockchain services must be risk-assessed. Services interfacing with blockchain should be subject to best-practice security controls to include:

- Enforce identity and access controls to access the blockchain solution and data
- Use privileged access management practices for escalated actions
- Use Application Programming Interface (API) security best practices to safeguard API-based transactions
- Secure communications both internally and externally using transport layer security
- Use strong cryptographic key/certificate management
- Have a security incident and event management capability"

The BMA further provides in the consultation draft of this Code of Practice that, "The Code comes into force on 1 January 2023, and DABs are required to be in compliance by 30 June 2023".

## CYBER RISK MANAGMENT CODE OF CONDUCT CONSULTATION PAPER: BANKS, DEPOSIT COMPANIES, CORPORATE SERVICE PROVIDERS, TRUST COMPANIES, MONEY SERVICE BUSINESSES, INVESTMENT BUSINESS AND FUND ADMINISTRATION PROVIDERS (OCTOBER 2021)

As with the previous two cyber risk management Codes of Conduct, the focus of the above Code of Conduct (the **Bank CRC**) is "information security". It generally follows the prescriptions of the previously reviewed cyber risk management codes except for the following nuances:

- The Bank CRC does not specifically address "Personally Identifiable Information"
- Given the diverse financial services that the Bank CRC will govern, there are numerous statutes, regulations and guidance schedules that the Bank CRC must be read in conjunction with eight other BMA prescribed statutes, and related statutory Schedules (delineated on page 4 of that Code of Conduct)

- The Bank CRC takes a broader approach in to addressing Information Technology (IT) Systems security and also directs registrants to read the Bank CRC in conjunction with the BMA's "Outsourcing Guidance Notes 2019"

## PENDING BROAD INDUSTRY CYBERSECURITY LEGISLATION

At the end of May 2022, the Bermuda Government (Hon. Michael Weeks, Minister of National Security) announced it had issued "drafting instructions" for both cybersecurity legislation and cybercrime legislation to Parliamentary Counsel in Bermuda. In June, 2022, Minister Weeks addressed Bermuda's Legislature to announce that the primary focus of the legislation, which he referred as the CyberSecurity Act, will be to address the management of cyber risk across Bermuda's critical infrastructure.

Considering Bermuda's current critical infrastructure related to telecommunications or energy is not currently regulated to specifically address cybersecurity risk management and response, it remains to be seen whether or not any further cybersecurity legislation will expand the industrial scope of data protection and cybersecurity law in Bermuda.