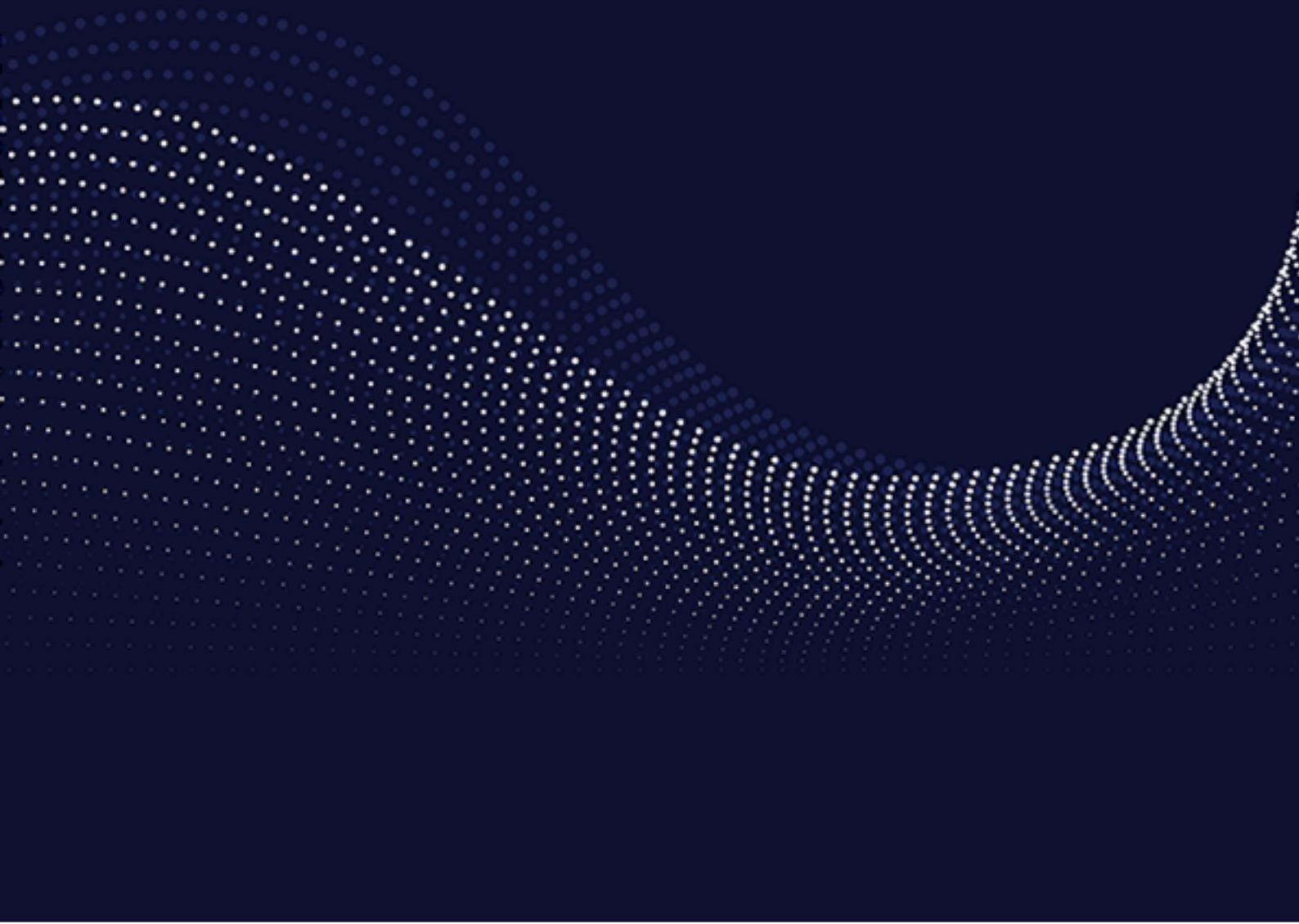
LEXOLOGY
Getting The Deal Through

DATA PROTECTION & PRIVACY

Bermuda



Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: December 22, 2023

LEXOLOGY
Getting The Deal Through

Contents

Data Protection & Privacy

SHARING AND CROSS-BORDER TRANSFERS OF PI

RIGHTS OF INDIVIDUALS

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

SPECIFIC DATA PROCESSING

UPDATE AND TRENDS

Contributors

Bermuda

MJM Barristers & Attorneys

Jennifer Haworth	jhaworth@mjm.bm
Fozeia Rana-Fahy	franafahy@mjm.bm
Michael Goulborn	mgoulborn@mjm.bm
Dan Griffin	dgriffin@mjm.bm
Nicole Cavanagh	ncavanagh@mjm.bm

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The Personal Information Protection Act 2016 (PIPA) is Bermuda's primary legislation protecting personal information. As a British Overseas Territory, UK or European privacy legislation is not part of Bermuda's legal system. However, PIPA draws on concepts from European and North American privacy regulations. When in force, it will create a privacy regime that employs similar concepts to the EU General Data Protection Regulation.

PIPA is scheduled to come into force on 1 January 2025. Implementation is expected to be phased, with larger organisations already subject to privacy regimes in other jurisdictions likely to be required to comply first and local or smaller organisations given more time.

In 2019, parts of PIPA were implemented to create the Office of the Privacy Commissioner of Bermuda (Privacy Commissioner) to issue guidance and oversee compliance were implemented in 2019. Further guidance from the Privacy Commissioner is expected throughout 2023 and 2024.

The Electronic Transactions Act 1999 (ETA) provides for the Bermuda government to prescribe regulations for the standards of processing of personal information. The ETA uses language that will be familiar to UK and European privacy regimes, including the voluntary registration of data controllers and processors, application of standards to data processing based on the country of origin of personal data and the imposition of fines for non-compliance. The ETA appears to have been little used in the context of data privacy in practice.

To protect the use of personal information by private organisations outside of the context of the ETA and prior to the full implementation of PIPA, individuals must primarily rely on contract and common law of breach of confidence, which follow English authorities.

The Public Access to Information Act 2010 and Public Access to Information Regulations 2014 govern the use of personal information by public authorities and provides the right for individuals to request access to information held by public authorities. Decisions on whether access may be granted are overseen by the Information Commissioner's Office. The Personal Information Protection Amendment Act 2023 will incorporate personal information requests to public authorities within PIPA.

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Office of the Privacy Commissioner of Bermuda is the authority responsible for overseeing implementation of PIPA when it comes into force on 1 January 2025.

The Privacy Commissioner's role is multifaceted. They will develop the detail of how organisations may practically comply with PIPA, publish guidance and carry out enforcement.

If the Privacy Commissioner considers that an organisation may not have complied with PIPA, it may conduct an investigation into compliance with PIPA and make an order requiring action by the organisation using personal information.

The Privacy Commissioner has broad powers under section 31 of PIPA to carry out an inquiry, which include:

- making an order for disclosure of information;
- entering premises to obtain information; and
- summoning witnesses for cross-examination.

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The Privacy Commissioner is not obliged to cooperate with other data protection authorities in Bermuda and it is expected that the Privacy Commissioner will be the primary authority dealing with personal information.

PIPA provides that the Privacy Commissioner may cooperate with overseas regulators to the extent necessary to ensure compliance with PIPA.

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

In the case of minor breaches of PIPA, the Privacy Commissioner may issue warnings and formal guidance.

More serious breaches may result in an order by the Privacy Commissioner that an organisation or individual must take action to comply with PIPA.

Any person who breaches PIPA may commit a criminal offence that may result, in the case of an individual, on summary conviction to a fine not exceeding US$25,000 or to imprisonment not exceeding two years, or to both. On conviction on indictment, in the case of a person other than an individual, it may result in a fine not exceeding US$250,000.

Directors, managers, secretaries and other officers, as well as shareholders of body corporates in breach may also be convicted if the offence was committed with their connivance, consent or is attributable to their negligence.

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Any person aggrieved by an order of the Privacy Commissioner may seek permission for judicial review by the Bermuda Supreme Court.

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

PIPA does not specifically exclude any sector or type of organisation from its scope, but does exclude certain purposes for processing personal information.

There are exemptions for information required for the purpose of safeguarding national security, provided that a certificate authorising the exemption is first obtained from the government minister and anyone affected may apply to the Bermuda Supreme Court to have the exemption set aside.

Communication providers (meaning organisations acting as conduits for personal information such as mobile telephone providers and internet service providers) are exempt where they act solely as a communication provider and do not determine the purpose of using personal information.

Information used by public bodies for the purpose of regulatory activities is exempt save for 'minimum requirements' where it might prejudice the discharge of 'relevant functions' such as protecting the public against financial loss, preventing charity misconduct or loss, procuring health, safety and welfare of individuals at work and protecting the public against the actions of individuals at work. A relevant function includes one conferred under a statutory provision, by the Crown or government or any other function that is of a public nature and exercised in the public interest.

There are also general exemptions for personal information used for the prevention or detection of crime, prosecution of offenders, collection of tax, breaches of professional rules of conduct and economic or financial interests of Bermuda when exercised by official authorities in Bermuda.

Exemptions are still subject to the 'minimum requirements' of Parts 2 and 3 of The Personal Information Protection Act 2016 (PIPA) such as the requirement to have a privacy notice, use information fairly, proportionately and for the specific purpose set out in the privacy notice, as well as ensuring its integrity.

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

PIPA does not specifically regulate the interception of communications, electronic marketing or monitoring and surveillance of individuals save for the general principles and rules in Part 2, which govern how organisations must use personal information and the rights of individuals in Part 3, such as the right to object to access personal information or object to its processing.

With regard to electronic marketing, there is presently no equivalent to the European Privacy and Electronic Communications Regulations 2003 providing generally applicable requirements in relation to electronic communications, such as prior consent to receiving electronic marketing. The Electronic Communications Act 2011 provides that specific requirements may be introduced on the use of electronic marketing by licensed communication operators (such as mobile telephone providers).

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

Further laws and regulations by sector are as follows.

Banking

Section 52 Banks and Deposit Companies Act 1999.

FinTech

- Parts 10 and 11 Digital Asset Business Act 2018;
- Digital Asset Business (Cybersecurity) Rules 2018;
- Digital Asset Business (Client Disclosure) Rules 2018;
- Digital Asset Issuance Rules 2020; and
- Digital Asset Business Accounts Rules 2021.

Public authorities

- Public Access to Information Act 2010 (PATI); and
- Public Access to Information Regulations 2014.

Telecoms

- Telecommunications Act 1986;
- Electronic Communications Act 2011; and
- Electronic Transactions Act 1999 (ETA).

PI formats

What categories and types of PI are covered by the law?

PIPA covers all personal information that is defined as 'any information about an identified or identifiable individual'.

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

Only organisations that use personal information in Bermuda must comply with PIPA, regardless of where the organisation is located.

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

PIPA applies to every organisation that uses personal information in Bermuda whether that personal information is used wholly or partly by automated means, and to the use other than by automated means of personal information that form, or are intended to form part of a structured filing system.

No distinction is made between controllers or processors of personal information. 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.

There are a number of exclusions such as use for domestic purposes, journalism, using business contact information about someone to contact them in their capacity as an employee or official, information about someone who has been dead for at least 20 years, archival use, court proceedings and parliamentary privilege.

Information acquired before the coming into force of PIPA will be deemed to have been obtained with the consent of the individual.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The Personal Information Protection Act 2016 (PIPA) requires that organisations may use personal information only if one or more of the conditions at section 6(1) are met. These conditions are comparatively flexible and subjective. They include:

- a reasonable person giving due weight to the sensitivity of the personal information would consider that the individual would not reasonably be expected to object and that the use does not prejudice their rights (except in relation to sensitive personal information);
- use is necessary for the performance of a contract or taking steps at an individual's request with a view to entering into a contract;
- use is pursuant to a law that authorises or requires such use;
- the personal information is publicly available and it will be used for a purpose consistent with that public availability;
- use is necessary to perform a task in the public interest or exercise of official authority vested in the organisation or in a third party to whom the personal information is disclosed;
- use is necessary in the context of an individual's present, past or potential employment relationship with the organisation; and
- consent (where consent can be reasonably demonstrated) subject to further conditions at section 6(2) on the manner in which consent is obtained, which are that the organisation shall provide clear, prominent, easily understandable, accessible mechanisms for giving consent. There is a variety of means by which consent may be deemed such as where it is implied from an individual's conduct, given to an intermediary or where they have enrolled in an insurance, trust benefit or similar plan and they derive a benefit.

If an organisation is unable to meet any of the conditions at section 6(1) and (2) they may only use personal information if:

- it was collected from or disclosed to a public authority authorised or required to provide or collect it;
- to comply with an order made by a court or other body with jurisdiction over the organisation;
- the use is necessary to contact the next of kin of an injured, ill or deceased individual;
- the use is necessary to collect a debt or repay money owed to an individual;
- the use is necessary to disclose to surviving spouse or relative of a living individual; and
- the use is reasonable to protect or defend the organisation in legal proceedings.

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

PIPA imposes more stringent rules on the use of sensitive personal information that includes any personal information relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information.

Sensitive personal information may only be used with the consent of any individual to whom the information relates, in accordance with an order made by either the court or the Privacy Commissioner,

for the purpose of any criminal or civil proceedings; or in the context of recruitment or employment where the nature of the role justifies such use.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The Personal Information Protection Act 2016 (PIPA) requires organisations to provide individuals with a privacy notice about its practices and policies with respect to personal information, including:

- the fact that personal information is being used;
- the purposes for which personal information is or might be used;
- the identity and types of individuals or organisations to whom personal information might be disclosed;
- the identity and location of the organisation, including information on how to contact it about its handling of personal information;
- the name of the privacy officer; and
- the choices and means the organisation provides to an individual for limiting the use of, and for accessing, rectifying, blocking, erasing and destroying, their personal information.

Organisations must take all reasonably practicable steps to ensure that the privacy notice is provided either before or at the time of collection of personal information or where that is not possible, as soon as is reasonably practicable thereafter.

Exemptions from transparency obligations

When is notice not required?

Organisations will not be obliged to provide a privacy notice if all of the personal information held by it is publicly available information, or the organisation can reasonably determine that the use is within the reasonable expectations of the individual to whom the personal information relates.

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

PIPA imposes an integrity requirement; organisations must ensure that that any personal information used is accurate and kept up to date to the extent necessary for the purposes of use.

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

PIPA imposes a proportionality requirement; organisations must ensure personal information is adequate, relevant and not excessive in relation to the purposes for which it is used.

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

PIPA requires that personal information kept for any use is not kept for longer than is necessary for that use.

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

PIPA imposes a purpose limitation that requires that personal information is only used for the specific purposes set out in the organisation's privacy notice or for purposes that are related to that use. The purpose limitation does not apply;

- with consent from the individual;
- when use is necessary to provide a product or service to the individual;
- where use is required by any rule of law or court order;
- where personal information is used for the purpose of detecting or monitoring fraud or fraudulent misuse of personal information; or
- where personal information is used for scientific, statistical or historic research subject to the appropriate safeguards for the rights of the individual.

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

PIPA applies to personal information used wholly or partly by automated means but there are no additional restrictions specific to use by wholly automated means without human intervention.

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Personal Information Protection Act 2016 (PIPA) requires organisations to protect personal information with appropriate safeguards against risk of loss, unauthorised access, destruction, use modification or disclosure, or from any other misuse. Safeguards are proportional to the likelihood and severity of the harm the risks pose, the sensitivity of the personal information and the context in which it is held. Safeguards should be periodically reviewed and reassessed. Guidance from the Privacy Commissioner on appropriate safeguards has emphasised the need for encryption.

The Electronic Communications Act 2011 already imposes similar obligations specifically on electronic communications providers such as internet service providers and mobile telephone providers.

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

PIPA requires reporting of any breach of security leading to the loss or unlawful destruction or unauthorised disclosure of or access to personal information that is likely to adversely affect an individual.

Organisations must report the breach of security 'without undue delay', first by notifying the Privacy Commissioner and then individuals affected by the breach.

The notification to the Privacy Commissioner should describe the nature of the breach, its likely consequences for the affected individual and the measures taken (and to be taken) to address the breach. There are no specific requirements with regard to the notification to affected individuals.

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

The Personal Information Protection Act 2016 (PIPA) requires that every organisation shall adopt suitable measures and policies to give effect to its obligations and to the rights of individuals. The measures and policies 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.

In practical terms this means that all organisations will need to implement a comprehensive privacy programme consisting of an audit of personal information used, documenting use practices, training, conducting risk assessments and develop an action plan to respond to incidents and individual rights requests, preferably all backed by internal policies.

In order to demonstrate compliance organisations will need to keep records of their use of personal information and the reasons for that use by reference to the requirements of PIPA. For example, they will need to record the conditions relied upon for the use of personal information and maintain records of consent where that has been sought.

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

PIPA requires that all organisations appoint a data privacy officer with primary responsibility for communicating with the Privacy Commissioner. Organisations under common ownership or control may appoint a single privacy officer provided that a privacy officer is accessible from each organisation. The privacy officer may delegate their duties.

There is no further formal guidance at present on their legal responsibilities beyond communicating with the Privacy Commissioner, however informal commentary from the Privacy Commissioner suggests that the role will be proportionate to the needs of the organisation, but they will at minimum need to develop the organisation's privacy programme.

The privacy officer should hold a position of authority sufficient to oversee and ensure compliance with PIPA. The role would usually be undertaken by a senior executive, director or owner. However, guidance from the Privacy Commissioner suggests that it could be undertaken by an external expert, even outside of Bermuda. An organisation's existing privacy officer or data privacy manager appointed under similar privacy regimes such as the General Data Protection Regulation (GDPR) is likely to suffice.

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

PIPA does not contain an explicit record keeping requirement; however, organisations must adopt suitable measures and policies to give effect to obligations and the rights of individuals set out in the act. Maintaining internal records of personal information will be necessary to comply with the requirement not to retain personal information for longer than is necessary.

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

PIPA requires that organisations using personal information adopt suitable measures to give effect to their obligations and to the rights of individuals set out in the Act. Guidance from the Privacy Commissioner has stated that this may include conducting a risk assessment to analyse the risk in context and to identify protective measures.

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

PIPA includes a requirement that organisations protect information from risks with appropriate safeguards, but it does not include explicit privacy by design and default obligations when determining the means of use of personal information akin to those at articles 25(1) and 25(2) of the GDPR. However, guidance from the Privacy Commissioner on the implementation of a privacy programme suggests that such an approach will assist organisations in demonstrating that they have acted reasonably when using personal data. The 'Pink Sandbox' initiative provides organisations with access to the Privacy Commissioner when developing new uses of personal information, the objective being to encourage a privacy by design approach.

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

The Personal Information Protection Act 2016 (PIPA) does not distinguish between owners or processors of personal information, instead referring to organisations that use personal information. PIPA does not require organisations to register with a supervisory authority.

Other transparency duties

Are there any other public transparency duties?

PIPA requires organisations to publish a privacy notice explaining the nature of personal information collected, the purpose of its use and how it is used. Organisations must publish the identity and contact information of their data privacy officer.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The Personal Information Protection Act 2016 (PIPA) does not distinguish between data controllers and processors. All organisations that use personal information are subject to the same obligations. If an organisation transfers personal information it has obtained to a third party such an outsourced processing service, the organisation remains responsible for its lawful use.

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

There are no specific restrictions on sharing personal information however the organisation transferring personal information will remain responsible for its use and so must carefully consider whether the recipient's intended use will be lawful.

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

Transfer of personal information to an overseas third party is subject to the requirement that the organisation making the transfer shall undertake a prior assessment of the level of protection provided by the overseas third party for that personal information. When undertaking that assessment the organisation must consider the level of protection afford by the law in that overseas party's jurisdiction. The transfer may only take place if the organisation reasonably believes that the protection provided by the overseas third party is comparable to the level of protection afforded by PIPA.

The organisation may rely on the third party's adoption of a certification mechanism recognised by the Privacy Commissioner. So far, the Privacy Commissioner has recognised the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) System as a certification mechanism for transfers of personal information to an overseas third party.

On the recommendation of the Privacy Commissioner, the government minister may designate any jurisdiction as providing a comparable level of protection for the purpose of PIPA's rules on overseas transfers (analogous to an adequacy decision under the EU General Data Protection Regulation).

In the absence of such a designation contractual mechanisms, binding corporate rules or other means must be used to ensure a comparable level of protection to PIPA.

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

PIPA does not distinguish explicitly between transfers to service providers and onward transfers. However, there are derogations from the restrictions on overseas transfer for the organisation's or overseas third party's own business purpose if the transfer is necessary for the establishment, exercise or defence of legal rights, or the organisation having assessed the circumstances of the transfer reasonably considers that it is small scale, occasional and unlikely to prejudice the rights of the individual.

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There are no requirements to retain personal information in Bermuda provided that restrictions on overseas transfers are complied with.

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

The Personal Information Protection Act 2016 (PIPA) provides that individuals have the right to request access to their personal information used by an organisation. Individuals may exercise this right by submitting a request in writing setting out sufficient detail to enable the organisation, with a reasonable effort, to identify the personal information in respect of which the request is made. The individual may ask for a copy or ask to examine their personal information.

When an organisation receives a request to access personal information it must acknowledge the request and state whether further information is needed to complete it. The request should then be completed within 45 days. This may be extended by no more than 30 days with permission of the Privacy Commissioner if the request concerns a large amount of information, meeting the deadline would unreasonably interfere with the organisation's operations, or if more time is needed to consult with a third party to determine whether to provide access.

The organisation may charge a fee no larger than the prescribed maximum (which is still to be determined).

A request may be refused if it is manifestly unreasonable.

If a request relates to medical records, the organisation may refuse to disclose the personal information to the individual and instead disclose it to another health provider to determine whether its disclosure to the individual might prejudice their physical or mental health.

Other rights

Do individuals have other substantive rights?

PIPA provides individuals with the right to request the rectification, blocking, erasure and destruction of their personal information.

An individual may request an organisation to cease, or not to begin, using their personal information where the use of that personal information is causing or is likely to cause substantial damage or substantial distress to the individual or to another individual.

The organisation may decline a request for the exercise of an individual's rights on giving reasons.

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

PIPA provides individuals with the entitlement to compensation from an organisation for financial loss or emotional distress caused by the organisation's failure to comply with any part of the Act.

It is a defence for an organisation to prove that it had taken such care as in all circumstances was reasonably necessary to comply with the requirement.

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

These rights are exercisable through the court or by initiating a complaint with the Privacy Commissioner.

An individual that has made a request to an organisation respecting his personal information may request that the Privacy Commissioner review the organisation's decision, action or failure to act.

At any time, the Privacy Commissioner may attempt to have the matter resolved by negotiation, conciliation, mediation or otherwise.

The Privacy Commissioner may then investigate, conduct an inquiry and make a finding, including imposing a binding order on the organisation or individual, which once registered is enforceable as a judgment of the court.

The amount of individual claims for compensation will be determined by the court rather than the Privacy Commissioner.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

The Personal Information Protection Act 2016 (PIPA) permits disclosure of personal information without consent for the purpose of a business transaction of almost any type, for example, the purchase, sale, merger or any other acquisition or disposal of a security, asset or part of an organisation. The use must be necessary for the parties to determine whether to proceed with the transaction. The parties must only use the personal information for the purpose of the transaction and the parties must enter into agreement whereby they undertake to only use the personal information for the purposes of the transaction. This exemption does not apply to transactions of which the primary purpose, objective or result is transfer of personal information.

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

There are no specific rules on the use of cookies. However, when in force, PIPA will regulate the use of cookies that obtain personal information about website users. In particular, cookies used for the purpose of third-party advertising that use personal information about website users may pose challenges, since they will likely result in the systemic collection of personal information, which is subject to PIPA controls on overseas transfers.

The Privacy Commissioner is yet to provide guidance on the use of cookies.

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

The Personal Information Protection Act 2016 (PIPA) provides that individuals have the right to request that their personal information is not used for the purpose of electronic communications marketing.

Targeted advertising

Are there any rules on targeted online advertising?

There are no specific rules on targeted online advertising save for the general provisions in PIPA regulating the use of all personal information.

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

PIPA imposes additional rules on the use of sensitive personal information that includes any personal information relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information.

Sensitive personal information may only be used with the consent of any individual to whom the information relates, in accordance with an order made by either the court or the Privacy Commissioner, for the purpose of any criminal or civil proceedings, or in the context of recruitment or employment where the nature of the role justifies such use.

Profiling

Are there any rules regarding individual profiling?

PIPA does not contain specific rules regarding individual profiling, but these are implied in the wording of the Act since PIPA applies to personal information used wholly or partly by automated means.

According to the Privacy Commissioner's guidance, organisations must identify the purpose and legal condition under which they use information, such as by requesting an individual's consent, and in order to get that consent, the organisation would have to explain its profiling or automated decision-making processes. In addition, PIPA restricts the use of personal information to when it is necessary to accomplish a purpose, and often automated decision-making or profiling may not be strictly necessary.

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

PIPA does not contain specific rules regarding cloud services; however, given they are likely to be provided from overseas, the rules on overseas transfers will apply.

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The implementation of the Personal Information Protection Act 2016 (PIPA) on 1 January 2025 will be the greatest change to data privacy law in Bermuda, bringing its regulatory environment into alignment with global trends toward increased protection for personal information.

The Privacy Commissioner is likely to increase its output of guidance on compliance with PIPA, with much of the detail on required practical measures still awaited. The most important topic for many businesses and practitioners in Bermuda will be the extent to which the Privacy Commissioner recognises overseas jurisdictions as affording a level of protection equivalent to PIPA, thereby smoothing international flows of personal information.

The regulators have shown an openness to technological innovation and working with organisations via the 'Pink Sandbox', which provides access to the Privacy Commissioner when developing new uses for personal information, in order to obtain their guidance on likely compliance and potentially a statement from them that the use complies with PIPA.