GUIDE TO PIPA

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

April 2024

Contents

Guide to PIPA

The Guide to PIPA is part of the guidance issued by the Office of the Privacy Commissioner for Bermuda (PrivCom). It is designed for privacy officers (POs) and others responsible for data protection and privacy on a day-to-day basis.

It explains the data protection and privacy law that applies to organisations in Bermuda. It covers the Personal Information Protection Act (PIPA), partially enacted by the Bermuda government in 2016. The date of the full implementation of PIPA is 1 January 2025.

The Guide to PIPA explains each of the data protection and privacy principles, individual rights, and the obligations that organisations have under PIPA.

The guide summarises the key points you need to know, answers frequently asked questions, and contains practical checklists to help you comply.

Key definitions

Who does PIPA apply to?

- PIPA applies to every organisations that uses personal information in Bermuda.
- An organisation determines the purposes and means of using personal information.
- If you are an organisation, PIPA places specific legal obligations on you; for example, you are required to maintain records of personal information and processing activities. You will have legal liability if you are responsible for a breach.
- If you are an organisation, you are not relieved of your obligations where an overseas third party is involved – PIPA places further obligations on you to ensure your contracts with overseas third parties comply with PIPA.
- PIPA as a whole or some sections does not apply to certain activities including processing covered by law enforcement, use of personal information for national security purposes and use of personal information for artistic, literary, or journalistic purposes with a view to publication in the public interest, or personal or domestic purposes.
- Depending on how an organisation uses personal information, there are three basic levels of privacy programme compliance with PIPA:
    - **Full compliance**, meaning PIPA applies fully to how an organisation uses personal information;
    - **Partial exemption** for uses of personal information that are exempt under sections 22 (National security exemption), 24 (Regulatory activity and honours exemption) and 25 (General exemption). Uses of personal information are usually only exempt from provisions of PIPA to the extent that PIPA would interfere with the intended purpose. The **minimum requirements** still apply; and
    - **No compliance** is required for uses of personal information that are *excluded* under section 4 Exclusions.

What is privacy?

- Privacy is the right of an individual to be left alone and in control of information about oneself. In addition to the protections in PIPA, the right to privacy or private life is enshrined in the United Nations' Universal Declaration of Human Rights (Article 12) and the European Convention of Human Rights (Article 8).

What are the minimum requirements?

- "Minimum requirements" means the requirements of sections 5 (Responsibility and compliance), 8 (Fairness), 11 (Proportionality), 12 (Integrity of personal information), and 13 (Security safeguards).

What is personal information?

- Under PIPA, "personal information" means any information that relates to an identified or identifiable individual.

- Understanding whether you as an organisation are processing the personal information of individuals in Bermuda is critical to understanding whether PIPA applies to your activities.

- Examples include names, dates of birth, photographs, video footage, email addresses, and telephone numbers.

- "Use" of personal information is a defined term in PIPA that 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."

- "Sensitive personal information" is a defined term in PIPA that includes information relating to such aspects as place of origin, race, colour, sex, sexual life, health, disabilities, religious beliefs, and biometric and genetic information. (Note: For a complete list, see section 7 of PIPA.)

- The information that identifies an individual could be as simple as a name or a number, it may include other identifiers such as an IP address or a cookie identifier, or other factors of identification.

- If it is possible to identify an individual from the information you are using as an organisation, then that information may be personal information.

- If one cannot directly identify an individual from that information, as an organisation, you need to consider whether the individual is still identifiable. You should consider the information you are using in conjunction with all the means reasonably likely to be used by either you or any other person in the organisation to identify that individual.

- When considering whether information 'relates to' an individual, you need to take into account "nature, scope, context, and risk" per section 5, including the content of the information, the purposes for which you are using it and the likely impact or effect of that use on the individual.

- It is possible that the same information is personal information for the purposes of one organisation but is not personal information for the purposes of another organisation because context can help identify individuals.

- If information that seems to relate to a particular individual is inaccurate – i.e., it is factually incorrect or is about a different individual – the information is still personal information since it relates to that individual.

Organisations ask:

What is personal information?

- PIPA applies to the use of personal information that is:
    - used wholly or partly by automated means; and
    - used other than by automated means of personal information which form, or are intended to form, part of a structured filing system.

- Personal information only includes information relating to natural persons who:
    - can be identified or who are identifiable from the information in question; or
    - can be identified from that information used in conjunction with other available information.

- Personal information may also include sensitive personal information. This information is considered more sensitive and you may only use it in more limited circumstances.

- Information about organisations (i.e., companies and public authorities) is not personal information.

- PIPA does not apply to the use of business contact information for the purpose of contacting an individual in their capacity as an employee or official of an organisation.

- However, information about individuals acting as sole traders, employees, partners, and company directors, where they are individually identifiable and the information relates to them as an individual, may constitute personal information.
- PIPA does not apply to personal information about an individual who has been dead for at least 20 years.

- PIPA does not apply to personal information about an individual that has been in existence for at least 150 years.

What are identifiers and related factors?

- An individual is "identified" or "identifiable" if you can distinguish them from other individuals.

- A name is the most common means of identifying someone. However, whether any potential identifier actually identifies an individual depends on the context.

- A combination of identifiers may be needed to identify an individual.

- Identifiers may include:

    - name;
    - identification number such as social insurance number;
    - location information; and
    - "online identifiers" such as IP addresses or "cookie" identifiers which may be personal information.

Can we identify an individual from the information we have?

- If, by looking solely at the information you are using, you can distinguish an individual from other individuals, that individual will be identified or identifiable.

- One doesn't have to know someone's name for them to be identifiable, a combination of other elements may be sufficient to identify the individual.

- If an individual is identifiable from the information, this will constitute personal information.

Can we identify an individual from the information we have in conjunction with other available information?

- It is important to be aware that the information you hold may identify an individual and therefore constitute personal information.

- Even in situations where you may need additional information to be able to identify someone, they may still be identifiable. That additional information may be information that you already hold, or it may be information that you need to obtain from another source.

- In some circumstances, there may be a slight hypothetical possibility that someone might be able to reconstruct the information in such a way that identifies the individual. However, this is not necessarily sufficient to make the individual identifiable in terms of PIPA. You are obliged to consider all the factors.

You have the continuing obligation to consider whether the likelihood of an individual being identified or identifiable has changed over time (e.g., as a result of the latest developments in technology).

What does "any information about an identified or identifiable individual" mean?

- "Any information about an identified or identifiable individual" constitutes personal information.

- This means that it must concern the individual in some way.

- To decide whether or not such information is personal information, you may have to consider:

    - The content of the information: it is about the individual or their activities?;
    - The purpose you will use the information for; and
    - The results or the effects on the individual from using the information.

- Information can reference an identifiable individual and not be personal information about that individual as the information is not about them.

- There may be circumstances where it may be difficult to determine whether information is personal information. As a matter of good practice, in such situations, you should treat the information with care, ensure that you have a clear reason for using the information, and ensure that you hold and dispose of the information securely.

- Inaccurate information may still be personal information if it relates to an identifiable individual.

What do "use" and "using" mean?

- Under PIPA, "use" or "using", in relation to 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.

What happens when different organisations use the same information for different purposes?

- Although information does not relate to an identifiable individual for one organisation, it may in the hands of another organisation.

- When used for a different purpose, or in conjunction with additional information available to another organisation, the information is about the identifiable individual. Therefore, in order to decide whether the information relates to an individual, it is necessary to consider carefully the purpose for which the organisation is using it.

- Organisations should take care when they make an analysis of this nature.

Organisations and overseas third parties

In a seashell:

- Under PIPA, "organisation" refers to "any individual, entity or public authority that uses personal information", and

- "Overseas third party" means an organisation not domiciled in Bermuda.

- Understanding your role and obligation as an organisation in relation to the personal information you are using is crucial in ensuring that you are PIPA-compliant and the fair treatment of individuals.

- 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.

- The Office of the Privacy Commissioner for Bermuda has the power to take action against organisations under PIPA.

- Under section 21, individuals can bring claims against an organisation and may be entitled to compensation awarded by a court for financial loss and emotional distress.

- Organisations should take the time to assess and document the status in respect of all the personal information and processing activities that the organisation carries out.

Principles

In a seashell:

PIPA sets out 12 key principles and rules:

- Responsibility and compliance
- Conditions for using personal information
- Sensitive personal information
- Fairness
- Privacy notices
- Purpose limitation
- Proportionality
- Integrity of personal information
- Security safeguards
- Breach of security
- Transfer of personal information to an overseas third party
- Personal information about children in the information society

These principles and rules should lie at the heart of your approach to using personal information.

They are based on the internationally recognized Fair Information practices (FIPs) and incorporated into international privacy principles hyperlink such as the GDPR or the OECD Privacy Principles.

All organisations, even organisations with some exceptions, will be subject to the minimum requirements. "Minimum requirements" means the requirements of sections 5 (Responsibility and compliance), 8 (Fairness), 11 (Proportionality), 12 (Integrity of personal information), and 13 (Security safeguards).

Organisations ask:

What are the principles and rules?

Part 2, sections 5-16 of PIPA, sets out the aforementioned 12 key principles and rules hyperlink that lie at the core of Bermuda's data protection and privacy law.

Why are they important?

The principles and rules are set out right at the start of the legislation, and inform everything that follows.

The principles don't give hard and fast rules; rather, they embody the spirit of the general data privacy regime. There are very limited exceptions to these rules and principles.

Compliance with these key principles and the detailed provisions that PIPA sets is therefore a fundamental building block for good data privacy practice.

Failure to comply with the principles may leave you open to investigation, enforcement, and/or prosecution for an offence.

Minimum requirements

In a seashell:

The term "minimum requirements" means the requirements of PIPA's Part 2, sections 5 (hyperlink to Responsibility and compliance), 8 (hyperlink to Fairness), 11 (hyperlink to Proportionality), 12 (hyperlink to Integrity of personal information), and 13 (hyperlink to Security safeguards).

Minimum requirements apply to all organisations, even those whose use of personal information may qualify for other exemptions.

Responsibility and compliance

In a seashell:

Section 5, Responsibility and compliance, states that:

(1) Every organisation shall adopt suitable measures and policies to give effect to its obligations and to the rights of individuals set out in this Act.

(2) The measures and policies in subsection (1) 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.

(3) 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.

(4) An organisation shall designate a representative ("privacy officer") for the purposes of compliance with this Act who will have primary responsibility for communicating with the Commissioner.

(5) A group of organisations under common ownership or control may appoint a single privacy officer provided that a privacy officer is accessible from each organisation.
(6) A privacy officer designated under subsection (4) may delegate his duties to one or more individuals.

(7) In meeting its responsibilities under this Act, an organisation shall act in a reasonable manner.

Organisations may use personal information in many ways and for many different purposes, which means that there is no "one-size-fits-all" approach.

"Suitable measures and policies" therefore entail something different for each of the different organisations: as such, they require a tailored approach. Organisations should implement measures and policies that cover the following programmatic elements:

- Conducting an inventory and classifying (or, "mapping") what personal information is used;
- Documenting personal information use practices in policies and procedures;
- Providing appropriate training and awareness training and awareness to staff or others with access to personal information;
- Analysing the privacy risk in context, utilizing tools such as "Privacy Impact Assessments," and identifying protective measures;

- Developing an action plan to respond to incidents or potential breach of security;

- Developing procedures to respond to PIPA Rights Requests.

The exact nature of these may differ, and the depth or intensity with which an organisation executes them will vary based on the particular circumstances. By having "suitable measures and policies" in place, organisations demonstrate that they understand the nature, scope, context and purpose of the personal information they use, and the potential risk posed to individuals by their use of the personal information.

Note that organisations are responsible for all uses of personal information, including transfers of personal information to overseas third parties. See page 48, Transfer of personal information to an overseas third party.

Conditions for using personal information

In a seashell:

Section 6, Conditions for using personal information, states that:

Subject to subsections (2), (3) and (4), an organisation may use an individual's personal information only if one or more of the following conditions are met—

(a) the personal information is used with the consent of the individual where the organisation can reasonably demonstrate that the individual has knowingly consented;

(b) 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 does not prejudice the rights of the individual;

(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;

(d) the use of the personal information is pursuant to a provision of law that authorises or requires such use;

(e) the personal information is publicly available information and will be used for a purpose that is consistent with the purpose of its public availability;

(f) 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;

(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; or

(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.

(2) For the purpose of relying on consent as a condition for the use of personal information under subsection (1)(a)—

(a) an organisation shall provide clear, prominent, easily understandable, accessible mechanisms for an individual to give consent in relation to the use of his personal information;

(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;

(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;

(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.

(3) If an organisation is unable to meet any of the conditions of subsection (1), then it may use personal information only if—

(a) the personal information was collected from, or is disclosed to, a public authority which is authorised 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.

(4) Where an organisation transfers personal information to an overseas third party, in addition to complying with the obligations of subsections (1) to (3), the organisation must also meet the obligations under section 15.

Sensitive personal information

In a seashell:

- Organisations in Bermuda are prohibited from using sensitive personal information without lawful authority, e.g., unless the individual that the personal information relates to has given their consent.
- Sensitive personal information is 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.

Subsections 7(2)-7(4) state that:

(2) No organisation shall, without lawful authority, use sensitive personal information identified in subsection (1) in order to discriminate against any person contrary to any provision of Part II of the Human Rights Act 1981.

(3) For the purposes of subsection (2), sensitive personal information is used with lawful authority if and only to the extent that it is used—

(a) with the consent of any individual to whom the information relates;

(b) in accordance with an order made by either the court or the Commissioner;

(c) for the purpose of any criminal or civil proceedings; or

(d) in the context of recruitment or employment where the nature of the role justifies such use.

(4) The Minister may make an order, subject to the negative resolution procedure, to amend the definition of "sensitive personal information" in subsection (1).

Organisations ask

What is sensitive personal information? For the full list, see above and/or see s 7. Also, see page 7.

Fairness

In a seashell:

- You must identify valid, lawful grounds under PIPA for using personal information.
- You must ensure that you do not use the information in breach of any other laws.
- You must use personal information in a manner that is fair. This means you must not process the information in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must inform people clearly, openly, and honestly from the start about how you will use their personal information.

Checklist: Lawful manner

☐ We use the information in a lawful manner and identify the law requiring use of personal information.

☐ If we are using sensitive personal information or criminal offence information, we have identified a condition for processing this type of information.

☐ We don't do anything unlawful with personal information.

Checklist: Fairness

☐ We have considered how the processing of information may affect the individuals concerned and can justify any adverse impact.

☐ We only handle people's information in ways they would reasonably expect, or we can explain why any unexpected processing is justified.

☐ We do not deceive or mislead people when we collect their personal information.

Organisations ask

What is the fairness principle?

Section 8, Fairness, states that:

"An organisation shall use personal information in a lawful and fair manner".

Lawfulness and fairness overlap, but you must make sure you satisfy both. It is not enough to show your processing is lawful if it is fundamentally unfair to or hidden from the individuals concerned.

What is "a lawful manner"?

To use personal information in a lawful manner, you need to identify specific grounds for the processing. This is called a "lawful manner" of using personal information. There are also specific additional requirements for using some especially sensitive types of personal information.

If information is not used in a lawful manner, it means your organisation's processing will be unlawful and in breach of this principle.

It also means that you don't do anything with the personal information which is unlawful in a more general sense. This includes statute and common law obligations, whether criminal or civil. If processing involves committing a criminal offence, it will be unlawful. However, processing may also be unlawful if it results in, for example:

- a breach of a duty of confidence;
- your organisation exceeding its legal powers or exercising those powers improperly;
- an infringement of copyright;
- a breach of an enforceable contractual agreement;
- a breach of industry-specific legislation or regulations; or
- a breach of the Human Rights Act 1981.

This list is not exhaustive. You may need to take your own legal advice on other relevant legal requirements.

Although the examples of using personal information in breach of copyright or industry regulations involve unlawful processing in breach of this principle, allegations that are primarily about breaches of copyright, financial regulations, or other laws are likely outside PrivCom's remit and expertise as data privacy regulator. In such situations, there are likely to be other legal or regulatory routes of redress where the issues can be considered in a more appropriate forum.

If you have used personal information unlawfully, PIPA gives individuals the right to erase that information or block your use of it.

What is fairness?

Use of personal information must always be fair as well as lawful. If any aspect of your processing is unfair you will be in breach of this principle – even if you can show that you have a lawful basis for the processing.

In general, fairness means that you should only handle personal information in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal information, but also about whether you should.

Assessing whether you are using information fairly depends partly on how you obtain it. In particular, if anyone is deceived or misled when the personal information is obtained, then this is unlikely to be fair.

To assess whether or not you are processing personal information fairly, you must consider more generally how it affects the interests of the people concerned – as a group and individually. If you have obtained and used the information fairly in relation to most of the people it relates to but unfairly in relation to one individual, there will still be a breach of this principle.

Personal information may sometimes be used in a way that negatively affects an individual without this necessarily being unfair. What matters is whether or not such detriment is justified, as the following scenario shows.

Scenario

Where personal information is collected to impose a fine for speeding, the information is being used in a way that may cause detriment to the individuals concerned, but the proper use of personal information for these purposes will not be unfair.

You should also ensure that you treat individuals fairly when they seek to exercise their rights over their information. This ties in with your obligation to facilitate the exercise of individuals' rights.

Privacy notices

In a seashell:

- You need to specify your purposes in your privacy notice for individuals.
- You must provide individuals with a clear and easy to understand statement about your practices and policies with respect to personal information.
- Privacy notices have specific requirements beyond the general obligation for transparency in the fairness principle.

Section 9, Privacy notices, states that:

> (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—
>
> (a) the fact that 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 details of the privacy officer;
> (f) the choices and means the organisation provides to an individual for limiting the use of, and for accessing, correcting, blocking, erasing and destroying, his personal information.
>
> (2) Organisations shall 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 thereafter as is reasonably practicable.
>
> (3) Organisations are not obliged to provide a privacy notice if—
> (a) all of the personal information held by it 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.

A privacy notice should precede any collection of personal information. Privacy notices are both good practice and are increasingly required by law in various jurisdictions.

Privacy notices should provide the individual with answers to the following questions:

- Who is collecting the personal information and by which methods?
- What personal information is being collected?
- How will the personal information be used?
- How can consent for collection and use of the personal information be provided and removed?
- With whom will the personal information be shared?
- How long will the personal information be retained?

The notice should contain details about the life cycle of personal information:

- How personal information is collected and by whom?
- How the personal information will be used?
- To whom will the personal information be disclosed? and
- How long information will be retained.

Details about how personal information is destroyed are not generally disclosed in a privacy notice.

Privacy notices: Checklist

☐ We have clearly, easily, and accessibly stated our practices and policies for using personal information.

☐ We include details of our purposes in our privacy notice for individuals.

☐ We regularly review our privacy notice for individuals.

Purpose limitation

In a seashell:

- You must be clear about what your purposes for use of personal information are from the start.
- You need to record your purposes as part of your obligations to adopt "suitable measures and policies" and specify them in your privacy policy.
- You can only use the personal information for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear obligation or function set out in law.

Section 10, Purpose limitation, states that:

> (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—
> (a) when the use of the personal information is with the consent of the individual whose personal information is used;
> (b) when the use of the personal information is necessary to provide a service or product required by the individual;
> (c) where the use of personal information is required by any rule of law or by the order of the court;
> (d) where the use of the personal information is for the purpose of detecting or monitoring fraud or fraudulent misuse of personal information; or
> (e) where the personal information is used for the purposes of scientific, statistical or historical research subject to the appropriate safeguards for the rights of the individual.

Purpose limitation: Checklist

☐ We have clearly identified our purposes for using personal information.

☐ We have documented the purposes.

☐ We include details of our purposes in our privacy notice for individuals.

☐ We regularly review our use of personal information and where necessary, update our documentation and our privacy notice for individuals.

☐ We make sure that we only use personal information in accordance with the original purpose for which we collected it or as identified in section 10.

Organisations ask:

What is the purpose limitation principle?

Section 10(1) says:

"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."

Section 9(1)(b) says:

"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 purpose for which personal information is or might be used."

In practice, this means that as an organisation you must:

- be clear from the outset why you are using personal information and what you intend to do with it;
- comply with your obligations to specify and document your purposes;
- comply with your obligations to inform individuals about your purposes; and
- ensure that if you plan to use or disclose personal information for any purpose that is additional to or different from the originally specified purpose, the new use is lawful and fair.

Why do we need to specify our purposes?

This requirement aims to ensure that you are clear and open about your reasons for obtaining personal information, and that what you do with the information is in line with the reasonable expectations of the individuals concerned.

Specifying your purposes is necessary to comply with numerous obligations under PIPA. Doing so from the outset helps you to be accountable for your use of personal information. It also helps individuals understand how you use their personal information, make decisions about whether they are happy to share their details, and assert their rights over their information where appropriate. It is fundamental to building public trust in how you use personal information.

There are clear links with other principles – in particular, the fairness principle. Being clear about why you are processing personal information will help you to ensure you use personal information in a manner which is lawful and fair. And if you use personal information for unfair, unlawful, or "invisible" reasons, you will be likely to be in breach of the principle.

Specifying your purposes is necessary to comply with your accountability obligations.

How do we specify our purposes?

When you comply with your responsibility obligations, you still need to comply with the requirement to specify your purposes in the following ways:

- You need to specify your purposes for using personal information within the suitable measures and policies you are required to adopt as part of your obligations under section 5(1) of Responsibility and compliance.

- You also need to specify your purposes in your privacy notice for individuals.

However, you may need to do more. You should also remember that whatever you document, and whatever you tell people, this cannot make fundamentally unfair use of personal information fair and lawful.

If you have not provided a privacy notice because you are only using personal information for an obvious purpose that is within the reasonable expectations of individuals, the "specified purpose" should be taken to be the obvious purpose.

You should regularly review your use of personal information, documentation, and privacy notice to check that your purposes have not evolved over time beyond those you originally specified.

Once we collect personal information for a specified purpose, can we use it for other purposes?

Under PIPA, if your purposes change over time or you want to use personal information for a new purpose which you did not originally anticipate, you can only go ahead if:

- you get the individual's specific consent for the new purpose; or

- you can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority.

You must also use the personal information in a manner which is lawful. The original basis you used to collect the information may not always be appropriate for your new use of that information.

If your new purpose aligns with the original one and your use of the personal information is necessary for that purpose, you can generally be confident it will also be lawful. In most cases, the appropriate basis for your new use of the personal information is likely to be fairly obvious.

However, you should remember that if you originally collected the personal information on the basis of consent, you usually need to get fresh consent to ensure your new use is fair and lawful.

You need to make sure that you update your privacy notice to describe this other purpose.

Under section 10(2)(e), PIPA specifically lists the following purposes where subsection (1) does not apply:

- scientific,
- statistical or
- historical research purposes.

Otherwise, you need to conduct an assessment to decide whether your organisation's new purpose aligns with the original one. The assessment should take into account the following, which is not an exhaustive list:

- any link between your original purpose and the new purpose;
- the context in which you originally used the personal information – in particular, your relationship with the individual and what they would reasonably expect;
- the nature and scope of the personal information – e.g., is it particularly sensitive;
- the possible consequences for individuals of the new use of their information; and
- whether there are appropriate safeguards - e.g., encryption or anonymization.

What you need to take into account depends on the particular circumstances.

As a general rule, if the new purpose is either very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is likely not to align with your original purpose. In practice, you are likely to need to ask for specific consent to use or disclose personal information for this type of purpose.

Scenario

A lawyer discloses his client list to his husband who runs an entertainment agency, so that he can offer special event deals to the lawyer's clients. Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

Proportionality

In a seashell:

You must ensure the personal information you are using is:

- adequate – sufficient to properly fulfil your stated purposes;
- relevant – has a rational, justifiable link to the purposes; and
- not excessive in relation to the purposes for which it is used – you don't hold more information than you need for those purposes.

Note: Other jurisdictions such as the UK or EU refer to "data minimisation" to describe this concept.

Proportionality checklist

☐ We only collect personal information we actually need for our purposes.

☐ We have sufficient personal information to properly fulfil those purposes, and not extra.

☐ We periodically review the information we hold and dispose of safely anything we don't need.

Organisations ask:

What is the proportionality principle?

Section 11, Proportionality, states that:

"An organisation shall ensure that personal information is adequate, relevant, and not excessive in relation to the purposes for which it is used."

Here, a general "less is more" rule applies. As an organisation, you should identify the minimum amount of personal information you need to fulfil your purpose. You should hold only that amount of information, not more. You need to be able to demonstrate that you have appropriate processes to ensure that you only collect and hold the personal information you need.

Under the right to correction, organisations must complete any incomplete information which is inadequate for your purpose. Individuals have the right to get you to delete any information that is not necessary for your purpose, under the right to erasure.

How do we decide what is adequate, relevant, and not excessive?

PIPA does not define these terms. This will depend on your purposes for collecting and using the personal information. It may also differ from one individual to another.
To assess whether you hold the right amount of personal information, you must first be clear about why you need it.

For sensitive personal information, it is particularly important to make sure you collect and retain only the absolute minimum amount of information.

You may need to consider this separately for each individual, or for each group of individuals sharing relevant characteristics. In particular, you should consider any specific factors that an individual brings to your attention – for example, as part of an objection, request for correction of incomplete information, or request for erasing unnecessary personal information.

You should periodically review your use of personal information to check that the personal information you hold is still relevant and adequate for your purposes and delete anything you no longer need.

When could we be processing too much personal information?

You should not have more personal information than you need to achieve your purpose. Nor should the information include irrelevant details.

Scenario

A debt collection agency is engaged to find a particular debtor. It collects information on several people with a similar name to the debtor. During the enquiry some of these people are disregarded. The agency should delete most of their personal information, keeping only the minimum information needed to form a basic record of a person they have removed from their search. It is appropriate to keep this small amount of information so that these people are not contacted again about debts which do not belong to them.

If you need to process particular information about certain individuals only, you should collect it just for those individuals – the information is likely to be excessive and irrelevant in relation to other people.

Scenario

An employment agency places workers in a variety of occupations. It sends applicants a general questionnaire, which includes specific questions about health conditions that are only relevant to particular manual occupations. It would be irrelevant and excessive to obtain such information from an individual who was applying for an office job.

You must not collect personal information on the assumption that it might come in handy in the future. However, you may be able to hold information for a foreseeable event that may never occur if you can justify it.

Scenario

An employer holds details of the blood groups of some of its employees. These employees do hazardous work and the information is needed in the event of an accident. The employer has in place safety procedures to help prevent accidents so it may be that this information is never needed, but it still needs to hold this information in case of emergency.

If the employer still holds the blood groups of those members of the workforce who have left, though, such information is likely to be irrelevant and excessive as they no longer work for the employer.

If you are holding more information than is actually necessary for your purposes, this is likely to be unlawful, as well as a breach of the proportionality principle. Individuals will also have the right to erasure.

When could we be processing inadequate personal information?

If the processing you carry out is not helping you to achieve your purposes, the personal information you have is probably inadequate. You should not use personal information if it is insufficient for its intended purpose.

In some circumstances you may need to collect more personal information than you had originally anticipated using so that you have enough information for the purpose in question.

Scenario

A researcher is undertaking a sociological study that consists of conducting interviews and focus groups with individuals from a racial/ethnic minority group, asking them about their experiences of discrimination. The researcher obtains consent from each of the participants in the interviews and focus groups, especially as the interviews and focus groups are likely to refer to their personal sensitive information. When holding the interviews and focus groups, the researcher also explains to the participants that it is possible that after the interview and the focus group, some other topics may emerge which the researcher would like to ask the participants about later. Indeed, as the research proceeds, it becomes necessary to collect additional information about the participants. The researcher collects more information from those participants who give additional consent to provide it.

Information may also be inadequate if you are making decisions about someone based on an incomplete understanding of the facts. In particular, if an individual asks you to supplement incomplete information under their right to correction, this could indicate that the information might be inadequate for your purposes.

Having inadequate personal information is an issue – but you must be careful not to go too far the other way and collect more information than you actually need.

Additionally, you must not keep personal information longer than you need it:

- You need to think about – and be able to justify – how long you keep personal information. This will depend on your purposes for holding the personal information.
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- You should also periodically review the personal information you hold and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of personal information. Individuals have a right to erasure if you no longer need the information.
- You can keep personal information for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.
- Be sure to consider legal requirements to retain information. These requirements will be part of your purpose and notice.

Checklist

☐ We know what personal information we hold and why we need it.

☐ We carefully consider and can justify how long we keep personal information.

☐ We have a policy with standard retention periods where possible, in line with documentation obligations.

☐ We regularly review personal information and erase or anonymise information when we no longer need it.

☐ We have appropriate processes in place to comply with individuals' requests for erasure.

☐ We clearly identify any personal information that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

Integrity of personal information

In a seashell:

- You should take all reasonable steps to ensure the personal information you hold is not incorrect or misleading as to any matter of fact.
- You may need to keep the personal information updated, although this will depend on what you are using it for.
- If you discover that personal information is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- You must carefully consider any challenges to the accuracy of personal information.
- You must ensure that you have appropriate security measures in place to protect the integrity of the personal information you hold.
- Integrity of personal information is vital to accurate decision-making.
- Integrity maintains the consistency, accuracy, and trustworthiness of personal information over its entire lifecycle.
- Integrity means that personal information is protected from unintentional modification and modified only by those who have the proper authority.

Section 12, Integrity of personal information, adds that:

(1) "An organisation shall ensure that any personal information used is accurate and kept up to date to the extent necessary for the purposes of use."
(2) An organisation shall ensure that personal information for any use is not kept for longer than is necessary for that use.

Integrity checklist

☐ We ensure the accuracy of any personal information we use.

☐ We have appropriate processes in place to check the accuracy of the information we collect, and we record the source of that information.

☐ We have a process in place to identify when we need to keep the information updated to properly fulfil our purpose, and we update it as necessary.

☐ If we need to keep a record of a mistake, we clearly identify it as a mistake.

☐ Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.

☐ We comply with the individual's right to correction and carefully consider any challenges to the accuracy of the personal information.

☐ As a matter of good practice, we keep a note of any challenges to the accuracy of the personal information.

Organisations ask:

When is personal information "accurate" or "inaccurate"?

PIPA does not specify what the definition of "accurate" is. However, the most commonly accepted meaning of "inaccurate" is "incorrect or misleading as to any matter of fact". Whether personal information is accurate may be obvious. However, if it is not obvious, the organisation should ask the individual for further clarification.

You must always be clear about what you intend the record of the personal information to show. What you use it for may affect whether it is accurate or not. For example, just because personal information has changed doesn't mean that a historical record is inaccurate – but you must be clear that it is a historical record.

Scenario

If an individual moves from Devonshire to Pembroke, a record saying that they currently live in Devonshire is obviously inaccurate. However, a record saying that the individual once lived in Devonshire remains accurate even though they no longer live there.

Does personal information always have to be up to date?

This depends on what you use the information for. If you use the information for a purpose that relies on it remaining current, you should keep it up to date. For example, you should update your employee payroll records when there is a pay rise. Similarly, you should update your records for customers' changes of address so that goods are delivered to the correct location.

In other cases, it will be equally obvious that you do not need to update information.

Scenario

An individual places a one-off order with a delivery company. The organisation will probably have good reason to retain a record of the order for a certain period for accounting reasons and because of possible complaints. However, this does not mean that it has to regularly check that the customer is still living at the same address.

You do not need to update personal information if this would defeat the purpose of the processing. For example, if you hold personal information only for statistical, historical, or other research reasons, updating the information might defeat that purpose.
In some cases, it is reasonable to rely on the individual to tell you when their personal information has changed, such as when they change address or other contact details. It may be sensible to periodically ask individuals to update their own details, but you do not need to take extreme measures to ensure your records are up to date, unless there is a corresponding privacy risk which justifies this.

However, if an individual informs the organisation of a new address, it should update its records. And if a mailing is returned with the message "no longer at this address" marked on the envelope – or any other information comes to light which suggests the address is no longer accurate – the organisation should update its records to indicate that the address is no longer current.

What steps do we need to take to ensure accuracy?

When you use your own resources to compile personal information about an individual, you must make sure the information is correct. You should take particular care if the information could have serious implications for the individual.

In order to ensure that your records are not inaccurate or misleading in this case, you must:

- accurately record the information provided;
- accurately record the source of the information;
- take reasonable steps in the circumstances to ensure the accuracy of the information; and
- carefully consider any challenges to the accuracy of the information.

"Reasonable steps" will depend on the circumstances and, in particular, the nature of the personal information and what you will use it for. If you are using the information to make decisions that may significantly affect the individual concerned or others, you need to put more effort into ensuring accuracy.

Scenario

A taxi company (organisation) recruiting a taxi driver will want proof that the individuals they interview are entitled to drive the type of vehicle involved. The fact that an applicant states in their work history that they worked as shop assistant a department store 20 years ago may not need to be checked for this particular job.

If your information source is someone you know to be reliable, or is a well-known organisation, it is usually reasonable to assume that they have given you accurate information. However, in some

circumstances you need to double-check – for example, if inaccurate information could have serious consequences, or if common sense suggests there may be a mistake.

Scenario

A customer (individual) emails their mobile operator (organisation) requesting a change in its records about their willingness to receive marketing material. The organisation amends its records accordingly without making any checks. However, when the customer emails again asking the operator to send their bills to a new address, they carry out additional security checks before making the requested change.

Even if you originally took all reasonable steps to ensure the accuracy of the information, if you later get any new information which suggests it may be wrong or misleading, you should reconsider whether it is accurate and take steps to erase, update or correct it in light of that new information as soon as possible. There are clear links here to the right to correction, which gives individuals the right to have inaccurate personal information corrected.

What should we do if an individual challenges the accuracy of their personal information?

If this happens, you should consider whether the information is accurate and, if it is not, you should delete or correct it. Remember that individuals have the right to have incorrect personal information corrected – see page 62, Correction, blocking, erasure and destruction, for more information.

Individuals don't have the right to erasure just because information is inaccurate. However, you must take all reasonable steps to erase or correct inaccurate information without delay, and it may be reasonable to erase the information in some cases. If an individual asks you to delete inaccurate information, it is therefore good practice to consider this request.

Measures used to support integrity include using tools to ensure software does not delete the personal information you hold unintentionally or limiting data entry, so only valid types of information can be entered (for example, limiting entry of dates to number format).

PIPA's integrity principle is complemented by the security principle outlined below.

Security safeguards

In a seashell:

- PIPA requires you to implement appropriate safeguards against risk that the personal information that you hold may be exposed to.

Section 13, Security safeguards, states that:

(1) An organisation shall protect personal information that it holds with appropriate safeguards against risk, including—
(a) loss;
(b) unauthorised access, destruction, use, modification or disclosure; or
(c) any other misuse.

(2) Such safeguards shall be proportional to—
(a) the likelihood and severity of the harm threatened by the loss, access or misuse of the personal information;
(b) the sensitivity of the personal information (including in particular whether it is sensitive personal information); and
(c) the context in which it is held,
and shall be subject to periodic review and reassessment.

Although PIPA does not specify what such appropriate safeguards protecting the personal information an organisation holds are, encryption is often a best practice and highly recommended.

Consider having an encryption policy in place that governs how and when you implement encryption, and also training your staff in the use and importance of encryption.

When storing or transmitting personal information, it is good practice to use encryption and ensure that your encryption solution meets current standards. You should be aware of the residual risks of encryption and have steps in place to address these.

Encryption checklist

☐ We understand that encryption can be an appropriate technical measure to ensure that we process personal information securely.

☐ We have an appropriate policy in place governing our use of encryption.

☐ We ensure that we educate our staff on the use and importance of encryption.

☐ We have assessed the nature and scope of our processing activities and have implemented encryption solution(s) to protect the personal information we store and/or transmit.

☐ We understand the residual risks that remain, even after we have implemented our encryption solution(s).

☐ Our encryption solution(s) meet current standards (such as FIPS 140-2 and FIPS 197 as of July 2023).

☐ We ensure that we keep our encryption solution(s) under review in the light of technological developments.

☐ We have considered the types of processing we undertake, and whether encryption can be used in this processing.

Organisations ask:

What is encryption?

- Encryption is a mathematical function that encodes data in such a way that only authorised users can access it.
- It is a way of safeguarding against unauthorised or unlawful processing of personal information and may be one way in which you can demonstrate compliance with the security principle.
- Encryption can protect information stored on mobile and static devices and in transmission.
- There are a number of different encryption options available.
- You should consider encryption alongside other technical and organisational measures, taking into account the benefits it can offer and the risks it can pose.
- You should have a policy in place governing the use of encryption, including appropriate staff education.
- You should also be aware of any sector-specific guidance that applies to you, as this may require you to use encryption.

Encryption and data storage

- Encrypting data whilst it is being stored often provides effective protection against unauthorised or unlawful processing.
- Most modern operating systems have full-disk encryption built-in.
- You can also encrypt individual files or create encrypted containers.
- Some applications and databases can be configured to store data in encrypted form.
- Storing encrypted data still poses residual risks. You will need to address these depending on the context of your processing, such as by means of an organisational policy and staff training.

Encryption and data transfer

- Encrypting personal information whilst it is being transferred often provides effective protection against interception by a third party.
- You should use encrypted communications channels when transmitting any personal information over an untrusted network.
- You can encrypt information prior to transmission over an insecure channel and ensure it is still protected. However, a secure channel provides assurance that the content cannot be understood if it is intercepted. Without additional encryption methods, such as encrypting the information itself prior to transmission, the information will only be encrypted whilst in transit.
- You should look to use HTTPS protocol across your entire website. While there are some circumstances that can make this difficult you still need to take appropriate steps such as ensuring that all areas of user input are protected.
- Encrypted data transfer still poses residual risks. You will need to address these depending on the context, such as by means of an organisational policy and staff training.

What types of encryption are there?

- The two types of encryption in widespread use today are symmetric and asymmetric encryption.
- With symmetric encryption, the same key is used for encryption and decryption. Conversely, with asymmetric encryption, different keys are used for encryption and decryption.
- When using symmetric encryption, it is critical to ensure that the key is transferred securely.

- The technique of cryptographic hashing is sometimes equated to encryption, but it is important to understand that encryption and hashing are not identical concepts, and are used for different purposes.

How should we implement encryption?

- When implementing encryption, it is important to consider four things:
    - choosing the right algorithm,
    - choosing the right key size,
    - choosing the right software, and
    - keeping the key secure.

- **Very important!** Over time, vulnerabilities may be discovered in encryption algorithms that can eventually make them insecure. You should regularly assess whether your encryption method remains appropriate.

- It is important to ensure that the key size is sufficiently large to protect against an attack over the lifetime of the information. You should therefore assess whether your key sizes remain appropriate.

- The encryption software you use is also crucial. You should ensure that any solution you implement meets current standards such as FIPS 140-2 and FIPS 197 (as of July 2023).

- Encryption solutions are widely available and can be deployed at relatively low cost.

- You should also ensure that you keep your keys secure and have processes in place to generate new keys when necessary to do so.

Encryption is just one example of a security practice. Be sure to consider all practices that are reasonable in your circumstances.

Breach of security

In a seashell:

- PIPA introduces a duty on all organisations to report breaches of security leading to the loss or unlawful destruction or unauthorised disclosure of or access to personal information to the Commissioner without undue delay.
- You must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place.
- You must also keep a record of any personal information breaches, regardless of whether you are required to notify.

Section 14, Breach of security, states that:

(1) In case of a breach of security leading to the loss or unlawful destruction or unauthorised disclosure of or access to personal information which is likely to adversely affect an individual, the organisation responsible for that personal information shall, without undue delay—
(a) notify the Commissioner of the breach; and
(b) then notify any individual affected by the breach.

(2) The notification to the Commissioner under subsection (1) shall describe—
(a) the nature of the breach;
(b) its likely consequences for that individual; and
(c) the measures taken and to be taken by the organisation to address the breach,
so that the Commissioner can determine whether to order the organisation to take further steps and for the Commissioner to maintain a record of the breach and the measures taken.

Checklist: Preparing for a personal information breach

☐ We know how to recognise a breach of personal information.

☐ We understand that a breach of personal information isn't only about loss or theft of personal information.

☐ We have prepared a response plan for addressing any breaches of personal information that occur.

☐ We have allocated responsibility for managing breaches to a dedicated person or team.

☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Checklist: Responding to a personal information breach

☐ We have in place a process to assess the likely risk to individuals as a result of a breach.

☐ We have a process to inform affected individuals about a breach when they are likely to be adversely affected.

☐ We know we must inform affected individuals without undue delay.

☐ We know who the regulator is.

☐ We have a process to notify the Commissioner of it without undue delay, even if we do not have all the details yet.

☐ We know what information we must give the Commissioner about a breach.

☐ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.

☐ We document all breaches, even if they don't need to be reported.

Organisations ask:

What is a personal information breach?

A personal information breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just losing personal information.

Personal information breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by an organisation or an overseas third party;
- sending personal information to an incorrect recipient;
- computing devices containing personal information being lost or stolen;
- alteration of personal information without permission; and
- loss of availability of personal information.

A personal information breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal information. In short, there will be a personal information breach whenever any personal information is accidentally lost, destroyed, corrupted, or

disclosed; if someone accesses the information or passes it on without proper authorisation; or if the information is made unavailable and this unavailability has an adverse effect on individuals.

When do we need to tell individuals about a breach?

If a breach is likely to adversely affect an individual, PIPA says you must inform the Commissioner and those concerned directly and without undue delay. In other words, this should take place as soon as possible.

Scenario

A hospital suffers a breach that results in accidental disclosure of patient records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the information and their confidential medical details becoming known to others. This is likely to result in an adverse effect, so they would need to be informed about the breach.

A university experiences a breach when a member of staff accidentally deletes a record of alumni contact details. The details are later re-created from a backup. This is unlikely to result in an adverse effect on those individuals. They don't need to be informed about the breach.

If you decide not to notify the Commissioner or individuals, you will still need to document your analysis that demonstrates that the breach is unlikely to adversely affect individuals. You should also remember that the Commissioner has the power to compel you to inform affected individuals if we consider there is a high risk of harm to individuals. In any event, you should document your decision-making process in line with the requirements of the responsibility and compliance principle.

What information must we provide to individuals when informing them about a breach?

You need to describe, in clear and plain language, the nature of the personal information breach and, at least:

- the name and contact details of any data privacy officer you have, or other contact point where more information can be obtained;
- a description of the likely consequences of the personal information breach; and
- a description of the measures taken or proposed to deal with the personal information breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

If possible, you should give specific and clear advice to individuals on the steps they can take to protect themselves, and what you are willing to do to help them. Depending on the circumstances, this may include such things as:

- resetting a password;
- advising individuals to use strong, unique passwords; and
- telling them to look out for phishing emails or fraudulent activity on their accounts.

What breaches do we need to notify the Commissioner about?

When a personal information breach occurs, you need to establish the likelihood of an adverse effect on individuals. If a risk or harm is likely, you must notify the Commissioner; if a risk is unlikely, you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

What role do overseas third parties have?

If your organisation uses an overseas third party to process the personal information and they suffer a breach, it must inform you without undue delay as soon as it becomes aware of the breach. As an organisation, you are still responsible.

Scenario

Your law firm (organisation) contracts an IT services firm (overseas third party) to archive and store customer records. The IT firm detects an attack on its network that results in personal information about its clients being unlawfully accessed. As this is a personal information breach, the IT firm promptly notifies you that the breach has taken place. You notify the Commissioner, if reportable.

This requirement allows you to take steps to address the breach and meet your breach-reporting obligations under PIPA.

If you use an overseas third party, the requirements on breach reporting should be detailed in the contract between you and your overseas third party, as required under section 15(4) and section 15(5).

How much time do we have to report a breach?

You must report a notifiable breach to the Commissioner without undue delay. If you fail to do so, you must give reasons for the delay.

What information must a breach notification to the Commissioner contain?

When reporting a breach, under PIPA, you must describe:

- the nature of the personal information breach;
- the likely consequences for that individual; and
- the measures taken, or to be taken by the organisation to address the personal information breach.

Scenario

Your organisation detects an intrusion into your network and becomes aware that access has been gained to files containing personal information, but you don't know how the attacker gained entry, to what extent that information was accessed, or whether the attacker also copied the information from your system.

You notify the Commissioner of the breach without undue delay, explaining that you don't yet have all the relevant details, but that you expect to have the results of your investigation within a few days. Once your investigation uncovers details about the incident, you give the Commissioner more information about the breach without delay.

Does PIPA require us to take any other steps in response to a breach?

You should ensure that you record all breaches. Section 14(2) requires you to document the facts regarding the breach, its effects, and the remedial action taken. This is part of your overall obligation to comply with the responsibility and compliance principle and allows us to verify your organisation's compliance with its notification duties under PIPA.

As with any security incident, you should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented. Human error is the leading cause of reported personal information breaches. To reduce the risk, consider:

- mandatory data protection and privacy induction and refresher training;
- support and supervising until employees are proficient in their role;
- updating measures, policies, and procedures for employees;
- working to a principle of "check twice, send once";
- implementing a culture of trust – employees should feel able to report incidents of near misses;
- investigating the root causes of breaches and near misses; and
- protecting your employees and the personal informaiton you are responsible for. This could include:
    - restricting access and auditing systems, or
    - implementing technical and organisational measures, e.g., disabling autofill.

As part of your breach management process, you should undertake a risk assessment and have an appropriate risk assessment matrix to help you manage breaches on a day-to-day basis. This will help you assess the impact of breaches and meet your reporting and recording requirements. This will provide a basis for your breach policy and help you demonstrate your accountability as an organisation.

What else should we take into account?

The following aren't all PIPA requirements regarding breaches, but you should take them into account when you've experienced a breach.

As a result of a breach, an organisation may experience a higher volume of data protection and privacy requests or complaints, particularly in relation to access requests and erasure. You should have a contingency plan in place to deal with the possibility of this. It is important that you continue to deal with those requests and complaints, alongside any other work that has been generated as a result of the breach. You should also consider how you might manage the impact on individuals, including explaining how they may pursue compensation should the situation warrant it.

It is important to be aware that you may have additional notification obligations under other laws if you experience a personal information breach.

You may also need to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

What happens if we fail to notify the Commissioner of all notifiable breaches?

Failing to notify the Commissioner of a breach when required to do so is an offence.

In accordance with section 47(3), 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.

It is important to make sure you have a robust breach-reporting process in place to ensure you detect and notify of breaches on time and to provide the necessary details, unless the personal information breach is unlikely to result in an adverse effect on individuals. If you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

Transfer of personal information to an overseas third party

In a seashell:

- PIPA applies to organisations in Bermuda.
- People risk losing the protection of Bermuda's data protection laws if their personal information is transferred outside of Bermuda.
- On that basis, PIPA contains rules about transfers of personal information to overseas third parties located outside of Bermuda. People's rights regarding their personal information must be protected or one of a limited number of exceptions must apply. For more information, see our Guidance on vendors, third parties, and overseas data transfers.

Section 15, Transfer of personal information to an overseas third party, states that:

(1) 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 this Act in relation to that personal information.

(2) Before making any such transfer, the organisation shall assess the level of protection provided by the overseas third party for that personal information.

(3) When assessing the level of protection in subsection (2), an organisation shall consider the level of protection afforded by the law applicable to such overseas third party and the Minister, on the recommendation of the Commissioner, may designate any jurisdiction as providing a comparable level of protection for the purposes of this section.

(4) If the organisation reasonably believes that the protection provided by the overseas third party is comparable to the level of protection required by this Act, which may be evidenced by the third party's adoption of a certification mechanism recognised by the Commissioner, the organisation may rely on such comparable level of protection while the personal information is being used by the overseas third party.

(5) Where subsection (4) is not satisfied, the organisation shall employ contractual mechanisms, corporate codes of conduct including binding corporate rules, or other means to ensure that the overseas third party provides a comparable level of protection.

(6) Notwithstanding subsections (1) to (5), an organisation may transfer personal information to an overseas third party for use by that overseas third party on behalf of the organisation or for the overseas third party's own business purposes, if—.

(a) the transfer of the personal information is necessary for the establishment, exercise or defence of legal rights; or

(b) the organisation assesses all the circumstances surrounding the transfer of personal information to the overseas third party and reasonably considers the transfer of personal information is—

(i) small-scale;

(ii) occasional; and

(iii) unlikely to prejudice the rights of an individual.

Scenario

A Bermuda-based company uses a centralised human resources service in the US provided by its US parent company. The Bermuda company passes information about its employees to its US parent company in connection with the HR service. This is a transfer of personal information to an overseas third party.

Organisations ask:

Do we need to make a transfer of personal information to an overseas third party?

Before making a transfer of personal information to an overseas third party, you should consider whether you can achieve your aims without actually sending personal information.

If you anonymise the information so that it is never possible to identify individuals, it is not personal information. If this is the case, the restrictions do not apply and you are free to transfer the anonymised information outside of Bermuda.

For fairness, you should tell people:

- the identity of the overseas third party;
- the country or countries to which the personal information is to be transferred;
- why you need to make the transfer;
- the type of information to be transferred;
- that they are able to withdraw consent if applicable; and
- importantly, the possible risks involved in making a transfer to a country which does not provide a comparable level of protection for personal information and without any other protection measures in place.

Consider and document the following (to the extent not already documented as part of a separate transfer risk assessment):

- Is there a section 15 transfer mechanism in place for any of the information? (If there is, you should have carried out a transfer risk assessment in relation to this section 15 transfer mechanism and identified whether there is a residual risk that some or all the information will not be sufficiently safeguarded.)
- Who is the information going to? What kind of organisation is the overseas third party (e.g., a public regulator like PrivCom, an IT company, a parent or service company in your group)
- Where is the overseas third party located?

- Will the overseas third party send the information to any other organisations? If so, what kind of organisation are they and where are they located?

- Why are you making the transfer? What will the overseas third party be doing with the information? If the information is going to be sent to other organisations, what will they be doing with the information?

- If you have carried out a transfer risk assessment, what risks have you identified as not being sufficiently safeguarded by the section 15 transfer mechanism?

- Who is the information about? Set out the categories of individuals (e.g., customers, employees, or business contacts).

- What type(s) of information are you transferring and does it include any sensitive personal information, or other more risky types of information such as financial transaction data, location data, or confidential records?

- Are there protections for the information because of the type of organisation or individual the overseas third party is? Does the overseas third party have to comply with professional rules or other rules which apply in addition to the general legal regime of the destination country (e.g., if the importer is a law firm, it may be subject to rules of professional conduct or rules of privilege)?

- Are there any other contractual protections (e.g., a confidentiality agreement)?

- What technological and organisational security measures will the overseas third party have in place to protect the information (e.g., is the information anonymised? Encrypted?)?

- What is the format of the transferred information (e.g., plain text)?

- How are you sending the information (e.g., are you transmitting it by email, website encryption or secure file transfer protocol (SFTP))? Or does it involve remote access to information stored in Bermuda?

- For how long can the overseas third party access the information?

- How often will these transfers occur?

- How much personal information are you transferring?

- When and how would the overseas third party return the information when the purpose is completed?

Personal information about children in the information society

In a seashell:

If you as an organisation use children's personal information about an individual under the age of 14 in provision of a service delivered by means of digital or electronic communications ("information society service"),

- you should think about the need to provide the specific protection required by section 16 from the outset and design your processing, products, and systems with this in mind.

- This is vital if you regularly or systematically process children's personal information.

- It is usually easier to incorporate child friendly design into a system or product as part of your initial design brief than to try and add it in later. We recommend that you use a Privacy Impact Assessment (PIA) to help you with this, and to assess and mitigate privacy and data protection risks to the child. You should also take into account the risk of harm for the child so that their freedom to learn, develop, and explore (particularly in an online context) is only restricted when this is proportionate.

Section 16, Personal information about children in the information society, states:

(1) Where an organisation uses personal information about a child in the provision of an information society service and—

(a) the service is targeted at children; or

(b) the organisation has actual knowledge that it is using personal information about children,

and consent is relied upon, subject to subsection (2) the organisation must obtain consent from a parent or guardian before the personal information is collected or otherwise used.

(2) An organisation—

(a) shall be reasonably satisfied that consent obtained under subsection (1) is verifiable so that it can be obtained only from the child's parent or guardian; and

(b) shall establish procedures to verify whether the individual is a child when it is reasonably likely that the organisation will use personal information about a child.

(3) When providing an information society service to a child, an organisation shall not seek to obtain personal information from the child about other individuals, including in particular, personal information relating to the professional activity of parents or guardians, financial information or sociological information except that personal information about the identity and address of the child's parent or guardian may be used for the sole purpose of obtaining the consent under subsection (1).

(4) When complying with its obligations under section 9, an organisation delivering an information society service to a child shall provide a privacy notice that is easily understandable and appropriate to the age of the child.

(5) In legal proceedings brought against an organisation for failure to comply with a requirement of this section, it is a defence for the organisation to prove that it had taken such care as in all circumstances was reasonably necessary to comply with such requirement.

Organisations ask:

How important are fairness and compliance with the data protection principles?

As with any other instance of using personal information, the principles of fairness, responsibility, and compliance should lie at the heart of all your use of children's personal information. The purpose of these principles is to protect the interests of the individuals, and this is particularly important where children, who are often considered vulnerable, are concerned.

These principles apply to everything you do with personal information and are key to complying with PIPA.

What about the best interests of the child?

The principle of fairness requires organisations to consider the best interest of individuals. The notion of the best interests of the child comes from Article 3 of the United Nations (UN) Convention on the Rights of the Child (UNCRC). Although it is not referenced in PIPA, it is something that the Commissioner will take into account when considering compliance, and that you should consider when making decisions about the processing of children's personal information. Article 3 of the UNCRC states that:

'In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.'

What if we're not sure whether the individuals are children or not?

This can be an issue, particularly with online or other remote use of personal information. If you aren't sure whether the individuals who personal information you use are children, or what age range they fall into, then you usually need to adopt a cautious and risk-based approach. This may mean:

- designing your processing so that it provides sufficient protection for children;
- putting in place proportionate measures to prevent or deter children from providing their personal information;

- taking appropriate actions to enforce any age restrictions you have set; or
- implementing up-front age verification systems.

The choice of solutions may vary depending upon the risks inherent in the processing, the rights, and freedoms of the child, and the particular provisions of PIPA that apply to your use of personal information. You should always think about both the target age range for your use of personal information and the potential for children outside the age range providing their personal information.

Rights of individuals

Access to personal information

In a seashell:

- Individuals have the right to request access to:
    - a copy of their personal information and other supplementary information, including
    - the purposes for which the personal information is used by the organisation;
    - the names of the persons to whom their personal information has been disclosed; and
    - the circumstances in which the personal information has been disclosed.
- Individuals who want to obtain access to their personal information need to make the request in writing.
- An organisation may charge a fee to deal with the applying individual's (applicant's) request not exceeding the prescribed maximum fee for access to the individual's personal information.
- An organisation may not charge a fee where the request results in the correction of an error or omission in the individual's personal information that the organisation controls.
- An organisation may not charge a fee if the organisation is prevented from doing so by its professional regulatory body.
- An organisation must respond to an applicant within 45 days.
- This 45-day time period is for the completed request, and is separate from an initial acknowledgement or confirmation of receipt.
- An organisation must provide receipt of the request to the individual "promptly" per section 20(3) along with any requests by the organisation for clarification.
- If the substance of the request meets the characteristics of section 20(6), then the response time period may be extended by 30 days. If this is the case, then the organisation must notify the individual as described in section 20(7).
- It is good practice to provide the information securely, in an accessible, concise, and intelligible format.
- An organisation can only refuse to provide the information if an exemption or restriction applies, or if the request is manifestly unreasonable.

Section 17, Access to personal information, states:

(1) Subject to subsections (2) to (4) and to section 18, at the request of an individual for access to his personal information, and having regard to that which is reasonable, an organisation shall provide the individual with access to—

(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 circumstances in which the personal information has been and is being disclosed.

(2) An organisation may refuse to provide access to personal information under subsection (1) 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;

(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.

(3) An organisation shall not provide access to personal information under subsection (1) if—

(a) the disclosure of the personal information could reasonably be expected to threaten

(b) the life or security of an individual;

(c) the personal information would reveal personal information about another individual; or 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,

unless it is reasonable in all the circumstances to provide access.

(4) If an organisation is reasonably able to redact the information referred to in subsection (2)(b) or (3)(b) or (c) from the personal information about the individual who requested it, the organisation shall provide the individual with access to his personal information after redacting the former information.

Procedure for making an access request

Section 20, Procedure for making a request under section 17, 18 or 19, states:

(1) In order to obtain access to his personal information or make a request for a correction to his personal information, the individual (in this section referred to as the "applicant") shall make a written request to the organisation 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.

(2) The applicant may ask for a copy of his personal information or ask to examine his personal information.

(3) An organisation shall promptly acknowledge in writing receipt of a request, including the date of the request, and the organisation shall at the same time inform the applicant, if there is insufficient detail in the request, what information is required to complete his request.

(4) Subject to subsection (5), when a completed request has been received, an organisation shall respond to an applicant not later than—
(a) 45 days from the day on which the organisation receives the applicant's written request referred to in subsection (1); or
(b) the end of an extended time period if the time period is extended under subsection (6).

(5) An organisation is not required to comply with subsection (4) whilst any requests to the Commissioner made by the applicant or organisation regarding the scope of rights or obligations pertaining to the applicant's request under section 17, 18 or 19 are pending.

(6) An organisation may, with respect to a request made under section 17, 18 or 19, extend the period for responding to the request by no more than 30 days, or for such longer period as the Commissioner may permit, 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.

(7) If the period for responding is extended under subsection (6), the organisation shall inform the applicant of the following—
(a) the reason for the extension; and
(b) the time when a response from the organisation can be expected.

(8) An organisation may charge an applicant who makes a request under section 17 or 18 a fee not exceeding the prescribed maximum for access to the applicant's personal information, except

where any such request results in the correction of an error or omission in the personal information about the individual that is under the control of the organisation.

(9) A fee may not be charged under subsection (8) if the organisation is prevented from charging such a fee by its professional regulatory body.

(10) If an organisation is intending to charge an applicant a fee for a service, the organisation may require the applicant to pay all or part of the fee in advance, as determined by the organisation.

(11) The Minister may, in consultation with the Commissioner, prescribe any applicable fees.

(12) An organisation is not required to comply with section 17, 18 or 19 of this Act if the request is manifestly unreasonable.

(13) If an organisation refuses to take action at the request of an applicant, the organisation shall inform the applicant in writing of the reasons for the refusal and of the right to contact the Commissioner to make a complaint.

Checklist: Preparing for access requests

☐ We know how to recognise an access request and we understand when the right of access applies.

☐ We understand what steps we need to take to verify the identity of the applicant, if necessary.

☐ We understand when we can pause the time limit for responding if we need to ask for clarification.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

☐ We understand the nature of the supplementary information we need to provide in response to an access request.

☐ We have suitable information management systems in place to allow us to locate and retrieve information efficiently.

Checklist: Complying with access requests

☐ We have processes in place to ensure that we respond to an access request without undue delay and within 45 days of receipt.

☐ We understand how to perform a reasonable search for the information.

☐ We understand what we need to consider if a third party makes a request on behalf of an individual.

☐ We are aware of the circumstances in which we can extend the time limit to respond to a request.

☐ We understand how to assess whether a child is mature enough to understand their rights.

☐ We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child.

☐ We understand what we need to consider if a request includes information about others.

☐ We are able to deliver the information securely to an individual, and in the correct format.

Organisations ask:

What is the right of access?

The right of access gives individuals the right to obtain a copy of their personal information, as well as other supplementary information. It helps individuals to understand how and why you are using their information, and check you are doing it lawfully.

How do we recognise an access request?

An individual can make an access request in writing only. A request is valid if it is clear that the individual is asking for their own personal information. An individual does not need to use a specific form of words, or refer to legislation.
An individual may ask a third party (e.g., a relative, friend or lawyer) to make an access request on their behalf. You may also receive an access request made on behalf of an individual through an online portal. Before responding, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of their authority.

What about requests for information about children?

Before responding to a request for information held about a child, you should consider whether the child is mature enough to understand their rights. If the request is from a child and you are confident they can understand their rights, you should usually respond directly to the child. You may, however,

allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child. If a child is competent, they may authorise someone else, other than a parent or guardian, to make an access request on their behalf.

What should we consider when responding to a request?

You must comply with an access request within 45 days of receiving the request. You can extend the time to respond by a further 30 days if the request is complex.

If you process a large amount of information about an individual, you may be able to ask them to specify the information or processing activities their request relates to, if it is not clear. The time limit for responding to the request is paused until you receive clarification, although you should supply any of the supplementary information you can do within 45 days.

Can we ask an individual for ID?

Yes. You need to be satisfied that you know the identity of the applicant (or the person the request is made on behalf of). If you are unsure, you can ask for information to verify an individual's identity. The timescale for responding to a request does not begin until you have received the requested information. However, you should request ID documents promptly as part of the request acknowledgement.

Can we charge a fee?

You may charge a fee not exceeding the prescribed maximum fee for access to the individual's personal information (more details to come). You may not charge a fee where the request results in the correction of an error or omission in the individual's personal information that the organisation controls. You may not charge a fee if the organisation is prevented from doing so by its professional regulatory body.

How do we find and retrieve the relevant information?

You should make reasonable efforts to find and retrieve the requested information. However, you are not required to comply if the request is manifestly unreasonable.

How should we supply information to the applicant?

An individual is entitled to request access to their personal information and to other supplementary information (which largely corresponds with the information that you should provide in a privacy notice). If an individual makes a request electronically, you should provide the information in a commonly used electronic format, unless the individual requests otherwise.

When deciding what format to use, you should consider both the circumstances of the particular request and whether the individual has the ability to access the information you provide in that

format. It is good practice to establish the individual's preferred format prior to fulfilling their request. Alternatives can also include allowing the individual to access their information remotely and download a copy in an appropriate format.

When can we refuse to comply with a request?

Where an exemption applies, you may refuse to provide all or some of the requested information, depending on the circumstances. You can also refuse to comply with an access request if it is manifestly unreasonable.

If you refuse to comply with a request, you must inform the individual of:

- the reasons why; and
- their right to make a complaint to PrivCom.

What should we do if the request involves information about other individuals?

Where possible, you should consider whether it is possible to comply with the request without disclosing information that identifies another individual. If this is not possible, you do not have to comply with the request except where the other individual consents to the disclosure or it is reasonable to comply with the request without that individual's consent.

You need to respond to the applicant whether or not you decide to disclose information about a third party. You must be able to justify your decision to disclose, withhold, or redact information about a third party, so you should keep a record of what you decide and why.

Can the right of access be enforced?

Yes. In appropriate cases, PrivCom may take action against an organisation if they fail to comply.
If you fail to comply with an access request, the applicant may apply for a court action, such as to seek compensation. It is a matter for the court to decide what action to take.

Access to medical records

In a seashell:

- Under PIPA, individuals have the right to request access to their medical records.
- Medical records or other health-related information is sensitive personal information.

Section 18, Access to medical records, states:

(1) On the request of an individual for access to—
(a) personal information of a medical or psychiatric nature relating to the individual; or
(b) personal information kept for the purposes of, or obtained in the course of, the carrying out of social work in relation to the individual,

an organisation may refuse to provide access to personal information if disclosure of the personal information to the individual would be likely to prejudice the physical or mental health of the individual.

(2) Where, under subsection (1), an organisation refuses to grant a request, the organisation shall, if requested to do so by the individual, provide access to personal information referred to in that subsection to a health professional, within the meaning of section 2 of the Bermuda Health Council Act 2004, who has expertise in relation to the subject matter of the record, and the health professional shall determine whether disclosure of the personal information to the individual would be likely to prejudice the physical or mental health of the individual.

(3) Notwithstanding anything else in this section, in response to a request under subsection (1), an organisation—
(a) may refuse to provide access to personal information by relying on section 17(2); and
(b) shall refuse to provide access to personal information pursuant to section 17(3).

(4) If an organisation is reasonably able to redact information which is referred to in section 17(2)(b) or section 17(3)(b) or (c) or information which would be likely to prejudice the physical or mental health of the individual from other personal information about the individual who requested it, the organisation shall provide the individual with access to the other personal information after redacting the former information or the information which would be likely to prejudice the physical or mental health of the individual.

Organisations ask:

As a health facility (organisation), do we have to always provide access to personal information/medical records when requested by the individual to whom it relates?

No, as an organisation, you may refuse to provide access to the individual's medical records if disclosure of the personal information to the individual would be likely to prejudice their physical or mental health.

Alternatively, you may provide access to the individual's medical record to a health professional who has expertise in relation to the subject matter of the medical records.

Correction, blocking, erasure, and destruction

In a seashell:

- PIPA includes a right for individuals to have inaccurate personal information corrected, or completed if it is incomplete.
- An individual must make a request for correction in writing.
- You as an organisation have 45 days to respond to a request.
- In certain circumstances you can refuse a request for correction.
- This right is closely linked to the organisation's obligations under the integrity principle of PIPA.

Checklist: Preparing for requests for correction

☐ We know how to recognise a request for correction and we understand when this right applies.

☐ We have a policy for how to record requests we receive in writing.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Checklist: Complying with requests for correction

☐ We have processes in place to ensure that we respond to a request for correction without undue delay and within 45 days of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

☐ We have appropriate systems to correct or complete information or provide a supplementary statement.

☐ We have procedures in place to inform any recipients if we correct any information we have shared with them.

Organisations ask:

What is the right to correction?

Under section 19 of PIPA, individuals have the right to have inaccurate personal information corrected. An individual may also be able to have incomplete personal information completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete information.

This right has close links to the integrity of personal information principle of PIPA (section 12). However, although you may have already taken steps to ensure that the personal information was accurate when you obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.

What do we need to do?

If you receive a request for correction, you should take reasonable steps to satisfy yourself that the information is accurate and to correct the information if necessary. You should take into account the arguments and evidence provided by the applicant.

What steps are reasonable will depend on the nature of the personal information and what it will be used for. The more important it is that the personal information is accurate, the greater the effort you should put into checking its accuracy and, if necessary, taking steps to correct it. For example, you should make a greater effort to correct inaccurate personal information if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

You may also take into account any steps you have already taken to verify the accuracy of the information prior to the challenge by the individual.

When is information inaccurate?

PIPA does not specify what the definition of "accurate" or "accuracy" is. However, the most commonly accepted meaning of "inaccurate" is "incorrect or misleading as to any matter of fact". It will usually be obvious when personal information is accurate.

You must always be clear about what you intend the record of the personal information to show. What you use it for may affect whether it is accurate or not. For example, just because personal information has changed doesn't mean that a historical record is inaccurate – but you must be clear that it is a historical record.

What should we do about information that records a mistake?

Determining whether personal information is inaccurate can be more complex if the information refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of

the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made and the correct information should also be included in the individual's information.

Scenario

If a patient is diagnosed by a GP as suffering from a particular illness or condition, but it is later proved that this is not the case, it is likely that their medical records should record both the initial diagnosis (even though it was later proved to be incorrect) and the final findings. Whilst the medical record shows a misdiagnosis, it is an accurate record of the patient's medical treatment. As long as the medical record contains the up-to-date findings, and this is made clear in the record, it would be difficult to argue that the record is inaccurate and should be corrected.

What should we do about information that records a disputed opinion?

It is also complex if the information in question records an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be corrected.

What should we do while we are considering the accuracy of the information?

As a matter of good practice, you should block the use of the personal information in question whilst you are verifying its accuracy.

What should we do if we are satisfied that the information is accurate?

You should let the individual know if you are satisfied that the personal information is accurate, and tell them that you will not be amending the information. You should explain your decision and inform them of their right to make a complaint to PrivCom.

It is also good practice to place a note on your system indicating that the individual challenges the accuracy of the information and their reasons for doing so.

Can we refuse to comply with the request for correction for other reasons?

You can refuse to comply with a request if it is manifestly unreasonable.

To be able to decide if a request is manifestly unreasonable, you must consider each request on a case-by-case basis. You should not have a blanket policy.

You must be able to demonstrate to the individual why you consider the request is manifestly unreasonable and, if asked, explain your reasons to the Commissioner.

What does "manifestly unreasonable" mean?

A request may be manifestly unreasonable if:

- the individual clearly has no intention to exercise their right to correction. For example, an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or

- the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption.

This is not a simple tick list exercise that automatically means a request is manifestly unreasonable. You must consider a request in the context in which it is made and you are responsible for demonstrating that it is manifestly unreasonable.

Also, you should not presume that a request is manifestly unreasonable because the individual has previously submitted requests which have been manifestly unreasonable or if it includes aggressive or abusive language.

The inclusion of the word "manifestly" means there must be an obvious or clear quality to it being unreasonable. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request will be manifestly unreasonable.

Scenario

An individual believes that information held about them is inaccurate. They repeatedly request its correction, but you have previously investigated and told them you regard it as accurate.

The individual continues to make requests along with unsubstantiated claims against you as the organisation.

You refuse the most recent request because it is manifestly unreasonable and you notify the individual of this.

What should we do if we refuse to comply with a request for correction?

You must inform the individual without undue delay and within 45 days of receipt of the request about:

- the reasons you are not taking action; and

- their right to make a complaint to PrivCom.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How can we recognise a request?

PIPA specifies that an individual (applicant) must make a written request to the organisation 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.

A request to correct personal information does not need to mention the phrase "request for correction" or section 19 of PIPA to be a valid request. As long as the individual has challenged the accuracy of their information and has asked you to correct it or has asked that you take steps to complete the information held about them that is incomplete, this will be a valid request under section 19.

You have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore, you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request and refer them to your privacy notice. Additionally, it is good practice to have a policy for recording details of the requests you receive. You may wish to check with the applicant that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of all requests.

How long do we have to comply?

You must comply with a request for correction without undue delay and at the latest within 45 days of receipt of the request, or within an additional 30 days if section 20(6) applies.

Can we extend the time for a response?

You can extend the time to respond by a further 30 days if the request is complex or you have received several requests from the individual. You must let the individual know, explain the reason why the extension is necessary and the time when a response from the organisation can be expected.

Can we ask an individual for ID?

Yes. You need to be satisfied that you know the identity of the applicant (or the person the request is made on behalf of). If you are unsure, you can ask for information to verify an individual's identity. The timescale for responding to a request does not begin until you have received the requested information. However, you should request ID documents promptly as part of the request acknowledgement.

Do we have to tell other organisations if we correct personal information?

If you have disclosed the personal information to other organisations, you must notify each of the organisations and inform them of the correction or completion of the personal information - unless

it would be unreasonable to do so. You must also inform the individual about the organisations to whom their personal information has been disclosed.

Consent

In a seashell:

- Consent is a condition for the use of personal information under PIPA's subsection 1(a).
- Organisations are obliged to provide clear, prominent, easily understandable, accessible mechanisms for an individual to give consent in relation to the use of their personal information.
- Consent means offering individuals real choice and control. Consent should put individuals in charge, build trust and engagement, and enhance your reputation.
- In order for an individual to knowingly consent, a very clear and specific statement of consent is needed.
- Keep your consent requests separate from other terms and conditions.
- Get separate consent for separate things. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any overseas third party who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people. Save old versions of privacy notices.
- Keep consent under review, and refresh it if anything changes.
- It is good practice to avoid making consent to processing a precondition of a service.
- Public authorities and employers will need to take extra care to show that consent is freely given.
- You should avoid over-reliance on consent.

Checklist: Asking for consent

☐ We have made the request for consent prominent and separate from our terms and conditions.

☐ We use clear, plain language that is easy to understand.

☐ We specify why we want the information and what we're going to do with it.

☐ We give separate distinct options to consent separately to different purposes and types of using personal information.

☐ We name our organisation and any overseas third party who will be relying on the consent.

☐ We tell individuals they can withdraw their consent.

☐ We ensure that individuals can refuse to consent without detriment.

☐ We avoid making consent a precondition of a service.

☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental/guardian-consent measures for younger children) in place.

Checklist: Recording consent

☐ We keep a record of when and how we got consent from the individual.

☐ We keep a record of exactly what they were told at the time.

Checklist: Managing consent

☐ We regularly review consents to check that the relationship, the use, and the purposes have not changed.

☐ We have processes in place to refresh consent at appropriate intervals, including parental consents.

☐ We consider using privacy dashboards or other preference-management tools as a matter of good practice.

☐ We make it easy for individuals to withdraw their consent at any time and publicise how to do so.

☐ We act on withdrawals of consent as soon as we can.

☐ We don't penalise individuals who wish to withdraw consent.

Organisations ask

Why is consent important?

The standard for consent set by PIPA means that organisations may use an individual's personal information under the condition that the personal information is used with the consent of the individual where the organisation can reasonably demonstrate that the individual has knowingly consented.

Consent is only one condition of use that may be relied upon.

Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

You must keep clear records to demonstrate consent.

Consent can be given and withdrawn freely.

You need to tell people about their right to withdraw consent, and offer them easy ways to withdraw consent at any time.

Public authorities, employers, and other organisations in a position of power may find it more difficult to show consent that is valid and freely given. For example, if an individual will suffer criminal penalties if they do not provide consent, it is not freely given. The organisation should rely on a different condition of use.

You need to review existing consents and your consent mechanisms to check they meet the standard set by PIPA. If they do, there is no need to obtain fresh consent.

Genuine consent should put individuals in control, build trust and engagement, and enhance your reputation.

Relying on inappropriate or invalid consent could destroy trust and harm your reputation – and may leave you open to legal action or enforcement.

What types of consent are there?

Consent may be explicit or implied.

Explicit, active, or "express" consent requires the individual to act in a way that specifically communicates consent. Some examples of explicit consent include requiring the individual to:

- click or tick a checkbox on a web-based or data-entry form;
- respond to an automatically generated email;

- provide verbal authorisation.

Implied, or passive, consent does not require specific action – there is no checkbox to mark or paper to sign. Instead, there could be a sign at the entrance to a building stating that surveillance cameras are in use. Entering the premises implies the individual gives consent to be recorded.

Another example is a business that includes language in a privacy notice stating that it collects personal information as part of a specific service, process, or programme; for example: "By downloading this program, you consent to the collection of information about you and your activities for the purpose of X."

For implied consent to be valid, the organisation must have notified the individual about the purposes, and the implication must be reasonable.

Implied consent cannot be relied upon for uses of sensitive personal information.

When is consent appropriate?

Consent is appropriate if and when you can offer people real choice and control over how you use their information and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal information without consent, asking for consent is misleading and inherently unfair.

If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis, or to meet the principle of fairness.

Public authorities, employers, and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given.

What is valid consent?

Consent must be freely given, which means giving people genuine ongoing choice and control over how you use their information.

Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise, easy to understand, and user-friendly.

Consent must specifically cover the organisation's name, the purposes of the use of personal information and the types of processing activity.
Consent must be expressly confirmed in words rather than by any other positive action.
There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

How should we obtain, record, and manage consent?

Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand. Include:

- the name of your organisation;
- the name of any overseas third party who will rely on the consent;
- why you want the personal information;
- what you will do with it; and
- that individuals can withdraw consent at any time.

You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or other default settings. Wherever possible, give separate options to consent to different purposes and different types of processing.

Keep records to evidence consent:

- who consented,
- when,
- how, and
- what they were told.

Make it easy for people to withdraw consent at any time they choose. Consider using preference-management tools.

Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes.

Maintain copies of older drafts or versions of privacy notices or consent forms.

Exemptions

In a seashell:

- PIPA sets out exemptions from some of the rights and obligations in some circumstances.
- Whether or not you can rely on an exemption often depends on why you use personal information.
- You should not routinely rely on exemptions; you should consider them on a case-by-case basis.
- You should justify and document your reasons for relying on an exemption.
- If no exemption covers what you do with personal information, you need to comply with PIPA as normal.

Exemptions checklist

☐ We consider whether we can rely on an exemption on a case-by-case basis.

☐ Where appropriate, we carefully consider the extent to which the relevant PIPA requirements would be likely to prevent, seriously impair, or prejudice the achievement of our processing purposes.

☐ We justify and document our reasons for relying on an exemption.

☐ When an exemption does not apply (or no longer applies) to our processing of personal information, we comply with PIPA requirements as normal.

Organisations ask:

What are exemptions?

In some circumstances, PIPA provides an exemption from particular PIPA provision. If an exemption applies, you may not have to comply with all the usual rights and obligations.

There are several different exemptions; these are detailed in Part 4 of PIPA.

The exemptions in PIPA can relieve you of some of your obligations for things such as:

- the right to be informed;
- the right of access;
- dealing with other individual rights;
- reporting personal information breaches; and
- complying with some of the principles.

Some exemptions apply to only one of the above, but others can exempt you from several things.

Use of personal information by organisations in Bermuda

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

- **Full compliance**, meaning PIPA applies fully to how an organisation uses personal information;

- **Partial exemption** for uses of personal information that are exempt under sections 22 (National security exemption), 24 (Regulatory activity and honours exemption) and 25 (General exemption). Uses of personal information are usually only exempt from provisions of PIPA to the extent that PIPA would interfere with the intended purpose. The **minimum requirements** still apply; and

- **No compliance** is required for uses of personal information that are *excluded* under section 4 Exclusions.

Under PIPA, a number of exclusions are listed at section 4. In practice they work a bit like an exemption. Here are some examples of exclusions:

- **Domestic purposes:** personal information processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity, is outside PIPA's scope. This means that if you only use personal information for such things as writing to friends and family or taking pictures for your own enjoyment, you are not subject to PIPA.

- **Artistic, literary, or journalistic purposes**: personal information used for these purposes with a view to publication in the public interest in so far as is necessary to protect the right to freedom of expression is outside PIPA's scope.

- **The use of business contact information for the purpose of contacting** an individual in their capacity as an employes or official of an organisation is outside PIPA's scope.

- **The use of personal information transferred to an archival institution** where access to the personal information was unrestricted or governed by an agreement between the archival institution and the donor of the personal information before the coming into operation of this Act is outside PIPA's scope.

- **The use of personal information contained in a court file** and used by a judge or competent authorities **for law enforcement purposes** is outside PIPA's scope (e.g., the Police investigating a crime).

- **The use of personal information contained in a personal note**, communication or draft decision created by or for an individual who is acting in **a judicial, quasi-judicial or adjudicative** capacity is outside PIPA's scope.

- **The use of personal information used by a member of the House of Assembly or the Senate** where such use relates to the **exercise of his political function** and the personal information is covered by **parliamentary privilege** is outside PIPA's scope.

How do exemptions work?

Whether or not you can rely on an exemption generally depends on your purposes for processing personal information.

Some exemptions apply simply because you have a particular purpose. But others only apply to the extent that complying with PIPA would:

- be likely to prejudice your purpose (e.g., have a damaging or detrimental effect on what you are doing); or

- prevent or seriously impair you from processing personal information in a way that is required or necessary for your purpose.

Exemptions should not routinely be relied upon or applied in a blanket fashion. You must consider each exemption on a case-by-case basis.

If an exemption does apply, sometimes you will be obliged to rely on it (for instance, if complying with PIPA would break another law), but sometimes you can choose whether or not to rely on it.

In line with the accountability principle, you should justify and document your reasons for relying on an exemption so you can demonstrate your compliance.

If you cannot identify an exemption that covers what you are doing with personal information, you must comply with PIPA as normal.

Under PIPA, the following exemptions are available:

1. National security exemption

2. Communication provider exemption

3. Regulatory activity and honours exemption

4. General exemption

1. National security exemption

If you use personal information to safeguard national security, there is a partial exemption provided for at section 22 of PIPA.

Section 22, National security exemption, states:

(1) Except for the minimum requirements, Parts 2 and 3 do not apply to the use of personal information required for the purpose of safeguarding national security.

(2) In order to rely on subsection (1), an organisation shall first obtain a certificate ("an exemption certificate") signed by the Minister, in consultation with the Minister responsible for national security, certifying that an exemption from all or any of the provisions of Parts 2 and 3, other than the minimum requirements, is required for that purpose.

(3) The Minister shall not sign an exemption certificate unless satisfied that the exemption is necessary and proportionate for the purpose of safeguarding national security.

(4) An exemption certificate may identify the personal information to which it applies by means of a general description and shall be expressed to have prospective effect.

(5) An individual or organisation directly affected by the Minister's decision whether or not to issue an exemption certificate may appeal to the Supreme Court against the Minister's decision.

You may be able to apply this exemption if you process personal information under PIPA.

You must always ensure that your processing is lawful and that you use the personal information in a fair manner under section 8. There is no exemption from the requirement to use personal information lawfully.
You must always comply with your general responsibility and compliance obligations.

This is not a blanket exemption. You must be able to show that the exemption from specified privacy and data protection standards is required for the use of personal information required for the purposes of safeguarding national security. When deciding whether to use this exemption, we suggest you consider whether complying with PIPA would raise a real possibility of an adverse effect on national security. (Further guidance to come.)

2. Communication provider exemption

If you use personal information as an organisation that acts as a communication provider, there is a partial exemption provided for at section 23 of PIPA.

Section 23, Communication provider exemption, states:

(1) An organisation that acts as a communication provider and its directors, officers or authorised agents are not liable under this Act for any breach committed while acting as a communication provider.

(2) In this section "communication provider" means an internet service provider, telecommunications and such other organisation that acts as a conduit for personal information transmitted by a third party and who does not determine the purpose of using that personal information.

This means that if you are a director, officer, or an authorised agent at the organisation, you are not liable under PIPA for any breach committed while acting as a communication provider.

3. Regulatory activity and honours exemption

Section 24, Regulatory activity and honours exemption, states:

(1) Except for the minimum requirements, Parts 2 and 3 of this Act do not apply to the use of personal information if such use is required for the purposes of discharging functions to which this subsection applies to the extent to which the application of those Parts would be likely to prejudice the proper discharge of those functions.

(2) Subsection (1) applies to any relevant function which is designed—
  (a) to protect members of the public against—
    (i) 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;
    (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 authorised to carry on any profession or other activity;
  (b) to protect charities against misconduct or mismanagement (whether by trustees or other persons) in their administration;
  (c) to protect the property of charities from loss or misapplication, or to recover such property;
  (d) to secure the health, safety and welfare of individuals at work; or
  (e) to protect the public against risk to their health or safety arising out of or in
  (f) connection with the actions of individuals at work.

(3) In subsection (2), "relevant function" means—
  (a) any function conferred on any person by or under any statutory provision;
  (b) any function of the Crown, a Minister of the Crown or a government department; or
  (c) any other function which is of a public nature and is exercised in the public interest.

(4) Parts 2 and 3 of this Act, except for the minimum requirements, do not apply to the use of personal information if such use is required for the purposes of the conferring by the Crown or Premier of any honour or dignity.

4. General exemption

This exemption at section 25 applies if you process personal information for the purposes of:

- the prevention and detection of crime and compliance with international obligations regarding the detection, investigation and prevention of crime;
- the apprehension or prosecution of offenders; or
- the assessment or collection of any tax or duty;
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professionals; or
- the economic and financial interest 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.

It exempts you from PIPA provisions under Parts 2 and 3 on:

- the right to be informed;
- all the other individual rights;
- notifying individuals of personal information breaches;
- the lawfulness and fairness principle, except the requirement to use personal information in a lawful manner;
- the purpose limitation principle; and
- all the other principles, but only so far as they relate to the right to be informed and the other individual rights.

Very important! However, the exemption only applies to the extent that complying with these provisions would be likely to prejudice your purposes of use of personal information. If this is not so, you must comply with PIPA as normal.

Scenario

A bank conducts an investigation into suspected financial fraud. The bank wants to pass its investigation file, including the personal information of several customers, to the Financial Intelligence Agency (FIA) for further investigation. The bank's investigation and proposed disclosure to the FIA are for the purposes of the prevention and detection of crime. The bank decides that, were it to inform the individuals in question about this processing of their personal information, this would be likely to prejudice the investigation because they might abscond or destroy evidence. Therefore, the bank relies on the general exemption and, in this case, does not comply with the right to be informed.