Privacy Commissioner Bermuda | Quo Data Ferunt

INDIVIDUALS' GUIDE TO PIPA

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

December 2024

Contents

Advice for individuals
Know your rights
Notice and Transparency
Right to access your personal information8
Right to access your medical records9
Right to have your information corrected 10
Right to have the use of your information blocked12
Right to have your information erased or destroyed14
Writing and submitting your PIPA rights request17
What can I expect after submitting a PIPA rights request with an organisation?
What can I do if the organisation does not respond to my request or if I am dissatisfied with the outcome of my PIPA rights request?
Making a complaint
What does "manifestly unreasonable" mean?
Compensation for financial loss or distress

Advice for individuals

Data-driven and data-sharing technologies permeate literally every aspect of our professional, as well as personal lives, both offline and online. This means that when we interact with organisations, we share our personal information, such as our name, address, date of birth, and at times our sensitive personal information, for example, our race, colour, national or ethnic origin, sex and sexual orientation. We share our information every time we visit a website, email someone, use a search engine to look for something or use social media. For most people, the sharing of personal information happens several times a day.

While these technologies are designed to make our lives easier, we need to take good care of our personal information. At the end of the day, it is *our* personal information. How we feel about our personal information, however, is not always how others may feel about it. They, too, need to take good care of our personal information, especially if they use it to improve and grow their business.

The relationship goes in both directions: it is – or, at least, should be – reciprocal. Organisations who have been entrusted with holding our personal information are obliged to act in ways that demonstrate responsible, ethical, and accountable stewardship. That is exactly the purpose that data protection and privacy laws and regulations such as the Personal Information Protection Act 2016 (PIPA) serve.

PIPA not only protects you and your personal information, but it also empowers you by telling you what your rights are with respect to your personal information. That is exactly why the Office of the Privacy Commissioner for Bermuda (PrivCom) has produced this guide on the rights of individuals under PIPA.

Know your rights

Under PIPA, you have the right to request access to the personal information that an organisation holds about you. You also have the right to know the purposes for which the organisation holds the information and the names of the persons or other organisations with whom your information has been shared.

This is called **the right of access**. This right can be found under section 17 of PIPA, Access to personal information, which is discussed on p. 8 of this guide.

You also have **the right to access your medical records**. This right can be found under section 18 of PIPA, Access to medical records, which is discussed on p. 9 of this guide.

Your other privacy rights are as follows:

- the right to have your information corrected (section 19(1) of PIPA), pp.10-11 of this guide;
- the right to have your information blocked (section 19(6) of PIPA), pp. 12-13 of this guide; and
- the right to have your information erased or destroyed (section 19(10) of PIPA), pp. 14-16 of this guide.

However, it is important to note that some legal exemptions may apply.

Notice and Transparency

In a seashell:

An organisation must inform you if it is using your personal information. This level of transparency is part of PIPA's principle of Fairness. Under the Fairness principle, an organisation must use personal information in a lawful and fair manner. The use of the personal information must be:

- in compliance with PIPA, Bermuda's privacy law,
- transparent, and
- neither harmful nor against the interests of the individual.

Certain specific aspects regarding the use of personal information by organisations must be communicated as part of a "privacy notice".

The organisation is obliged to provide individuals with a clear and easily accessible statement (i.e., a privacy notice) which outlines the organisations practices and policies with respect to personal information held by the organisation. The privacy notice must provide details on the following aspects of your personal information:

- the fact that personal information is being collected and used;
- why and for what purpose(s) the organisation is using your personal information;
- what type(s) of personal information the organisation is using;
- how long the organisation will keep your personal information;
- whether the organisation is going to transfer your personal information to overseas third parties, the names or categories of recipients, and the reasons for the transfer;
- whether the organisation is going to transfer your personal information overseas, including the country involved and what will be done with the information;
- what your rights with respect to your personal information are;
- where the organisation obtained your information;
- ways to contact the organisation about its use of your personal information;
- your right to complain to the Office of the Privacy Commissioner for Bermuda (PrivCom).

The organisation is obliged to give you this information either before or at the time of collection of personal information.

Organisations must describe in their privacy notice how you can contact their Privacy Officer.

People ask:

When is an organisation not required to inform me of its use of my personal information?

Generally, organisations must give you notice, but there are some circumstances in which they don't have to. An organisation is not required to provide a copy of its privacy notice in the following situations:

- where all of the personal information it holds is publicly available; or
- the organisation can reasonably determine that all uses of your personal information are within what you would reasonably expect to happen to your personal information.

Page | 8

Right to access your personal information

In a seashell:

Under section 17 of PIPA, Access to personal information, you have the right to access the personal information that an organisation holds about you. However, there are situations where an organisation may refuse your request to access your personal information.

People ask:

1. What is the right of access?

Under PIPA, you have the right to ask an organisation whether it is using or storing your personal information. You can also ask the organisation for copies of your personal information. In order to request an organisation to provide you with copies of your personal information, you must do so in **writing**, using the contact details provided in the organisation's privacy notice.

This is called **the right of access** and is also commonly known as **making an access request**.

2. Why do individuals make an access request?

You can make an access request to find out:

- what personal information an organisation holds about you;
- how the organisation is using it;
- who the organisation is sharing it with; and
- where the organisation got your information from.

The information obtained through an access request can also help you effectively exercise your other privacy rights: **the right to have your information corrected, blocked, erased or destroyed**.

If or when you make a request to an organisation in relation to any of these rights, they are generally referred to as a **PIPA rights request**, or an **individual rights request**.

It is important to be aware that **none of these rights are absolute**. This means there are conditions under PIPA, under which organisations may lawfully refuse your PIPA rights request. This may include situations when an organisation:

- is not required to provide access; or
- is restricted from providing access.

This guidance will help you understand the circumstances when organisations may refuse your PIPA rights request.

Right to access your medical records

In a seashell:

Under section 18 of PIPA, Access to medical records, you have the right to access personal information of a medical or psychiatric nature that an organisation holds about you.

In order to request an organisation to provide you access to your medical records, you must contact the organisation in writing, using the contact details provided in the organisation's privacy notice and let them know what medical information you want to access.

However, there are a few exceptional situations in which you can't access it your medical records, or your personal information kept for the purposes of, or obtained in the course of, carrying out social work relating to you.

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

If an organisation refuses your request to access your medical records, you can ask the organisation to provide access to your personal information to a health professional who has expertise in relation to the subject matter of the record. The health professional will then determine whether or not disclosure of your medical information to you would be likely to prejudice your physical or mental health.

Page | 10

Right to have your information corrected

In a seashell:

Under section 19 (Correction, blocking, erasure and destruction) of PIPA, you have the right to make a written request to an organisation to correct an error or omission in any of your personal information which the organisation holds about you. This is known as **the right to correction**. If your information is inaccurate or incomplete, you can ask the organisation to correct the personal information or complete it by adding more details.

If there is an error or omission in the personal information that an organisation holds on you, you can ask the organisation to correct it. Upon receiving your written request for a correction, the organisation must make the requested changes to your personal information as soon as reasonably practicable. The organisation may ask you for additional information as supporting evidence to honour your right to correction.

Additionally, where the organisation has shared the incorrect information with other organisations, the organisation is required to send a notification containing the corrected information to each organisation with which the incorrect information has been shared, if it is reasonable to do so.

Scenario

After collecting your health insurance card from your employer, you notice the insurance company has misspelt your surname. You should contact your insurance company with a request to get your personal information corrected.

People ask:

1. How do I get my information corrected?

In order to request an organisation to correct the incorrect or inaccurate information, you must contact the organisation in writing, using the contact details provided in the organisation's privacy notice and let them know what personal information you want them to correct.

You must inform the organisation in writing that your personal information is inaccurate and that you want it corrected. You should:

- state clearly what personal information you believe is inaccurate or incomplete;
- explain how the organisation should correct it; and
- where available, provide evidence of the inaccuracies.

The added value of having everything in writing is that it will allow you to explain your concern, give evidence and state your desired solution. It will also provide clear proof of your actions if you decide to challenge the organisation's initial response.

2. What if the information refers to an error?

If there is an error in the personal information that has been corrected, the organisation will likely maintain a record of the error alongside the correct information to ensure the organisation can take into account the period of time before correction.

Scenario

An optician finds that a patient has a specific eye condition and notes it in their medical records. Sometime later, this diagnosis is found to be wrong. The medical records should likely include both the initial diagnosis and the final findings as this gives an accurate record of the patient's treatment. As long as the medical record contains the up-to-date findings, and this is made clear in the patient's record, it would be difficult to argue that the record is inaccurate and should be corrected. Recording the error may be necessary to explain why certain medicine was prescribed at the time.

3. How should I raise my concern with an organisation about how they have mishandled my information?

Please refer to p. 26 of this guide. When submitting your written request, you can use the master template on pp. 18-19 to help you raise your concern. The use of the master template is intended to serve as guidance when formally communicating with the organisation. Any other written format that you deem appropriate may also be used to raise your concern.

4. What should organisations do?

When an organisation is asked to correct information, it should take reasonable steps to investigate and confirm whether the information is accurate. To do this, the organisation should consider the evidence you provide. The organisation should be able to demonstrate what measures it has taken in response to your request.

The organisation should then contact you to:

- confirm it has acted on your instruction; or
- inform you that the organisation will not correct the information and provide an explanation as to why it believes the information is accurate.

As a matter of good practice, if the organisation refuses to correct the information, the organisation should record that you have challenged the information's accuracy, along with the reasons why you did so.

5. When can an organisation say no?

The organisation can refuse to comply with a request for correction if it believes that the request is "manifestly unreasonable" (see page 30). The organisation should explain why it believes that it does not have to comply with your request and let you know about your right to complain about this decision to PrivCom or through courts. For more information, see pp. 27-29 (Making a complaint).

Right to have the use of your information blocked

In a seashell:

Under section 19 of PIPA, you have the right to request an organisation **to cease (i.e., to stop), or not to begin**, using your personal information in two instances:

- if the personal information is used for the purposes of advertising, marketing or public relations, or
- where the use of that personal information is causing or is likely to cause substantial damage or substantial distress to you or to another individual.

This is called **the right to block**.

People ask:

1. How can I ask an organisation to stop, or not to begin, using my personal information?

You should contact the organisation using the contact details provided in the organisation's privacy notice and let them know what personal information you want them to block.

To exercise your right to block the use of your personal information, you must:

- submit your request in writing directly to the organisation; and
- in your submission, state what information you want the organisation to stop, or not to begin, using and why.

Scenario A

Previously, you agreed to receive specific adverts directly from an organisation but are no longer interested in receiving them. Consequently, you have asked the organisation to stop using your information for direct marketing purposes.

You should inform the organisation in writing that you no longer want them to use your information as previously agreed. In your right to block request, you will need to explain why you would like the organisation to stop using your information in this way.

Scenario B

You agreed to take part in a market research study and no longer want to participate. You gave consent to the organisation's use of your personal information but have now withdrawn your consent.

When submitting your written request, you can use the master template on pp. 18-19 to help you raise your concern. The use of the master template is intended to serve as guidance when formally communicating with the organisation. Any other written format that you deem appropriate may also be used to raise your concern.

The added value of having everything in writing is that it will allow you to explain your concern, provide evidence and state your desired solution. It will also provide clear proof of your actions if you decide to challenge the organisation's initial response. You will also have clear proof of your actions if you decide to challenge the organisation's response.

2. What should organisations do?

On receiving a written request, an organisation must:

- stop, or not begin, using the personal information; or
- provide you with written reasons as to why the use of such personal information is justified.

The organisation cannot refuse your request to stop the use of your personal information for direct marketing purposes and must stop using your information for such purposes. For example, they cannot carry on using your information to try to sell or promote things to you if you request the organisation to stop using your personal information as part of their direct marketing activities.

However, this does not automatically mean that the organisation will erase all your personal information. The organisation may put you on their 'suppression list' – this is their list of people who have said that they don't want their information used for direct marketing purposes. Having a suppression list means that if the organisation obtains any new direct marketing lists, they can check against the suppression list to make sure they don't use your information for direct marketing when you have asked them not to.

3. When can an organisation say no?

Additionally, an organisation may still be able to legitimately continue using your information for other purposes, for example:

- for contractual relations or
- if there is a law that tells the organisation it must collect your information.

PIPA also contains exemptions. If an exemption applies, the organisation can either fully or partly refuse to comply with your request (see pages 23-24).

If, after considering your request, the organisation decides it does not need to stop, or not to begin, using your information, it must still respond to you. The organisation should explain to you why it believes it does not have to comply with your request and let you know about your right to complain about this decision to PrivCom, or through the courts. For more information, see pp. 27-29 (Making a complaint).

Right to have your information erased or destroyed

In a seashell:

Under section 19 of PIPA, you have the right to request an organisation to erase or destroy your personal information where that personal information is no longer relevant for the purposes for which it was originally collected.

The right to get your information erased or destroyed is also known as **the right to erasure**. In some circumstances, an organisation can refuse your right to erasure request.

The right to erasure applies in situations where:

1. An organisation no longer needs your information for the purpose for which it was originally used:

Scenario A

You have cancelled your gym membership, your account has been settled, and the appropriate retention period has expired. The gym should delete your personal information since it no longer needs to keep details of your name, address, age, and health conditions (sensitive personal information).

2. You have requested that an organisation stop the use of your information for direct marketing purposes:

Scenario B

You agreed to receive specific adverts directly and are no longer interested in them, and now want the information erased.

3. The organisation using your personal information has collected or used your information unlawfully:

Scenario C

The organisation hasn't complied with the privacy rules under PIPA, so it does not meet the legal condition to use the information. You want them to erase what they hold. The organisation has a legal obligation to erase your information.

Scenario D

You used social media or a gaming app as a child according to your parents' consent, and you wish to withdraw your consent and have the information erased.

PIPA gives children special protection, especially online. Children are vulnerable and therefore may be less aware of the risks and consequences of giving their information to organisations.

People ask:

1. How do I ask for my information to be erased or destroyed?

You should contact the organisation using the contact details provided in their privacy notice and let them know what personal information you want them to erase.

When submitting your written request, you can use the master template on pp. 18-19 to help you raise your concern. The use of the master template is intended to serve as guidance when formally communicating with the organisation. Any other written format that you deem appropriate may also be used to raise your concern.

The added value of having everything in writing is that it will allow you to explain your concern, give evidence and explain what you want to happen. It will also provide clear proof of your actions if you decide to challenge the organisation's response.

2. What should the organisation do?

The organisation must:

- erase or destroy the personal information identified in the request; or
- provide you with written reasons as to why the continued use of such personal information is justified.

The organisation must erase and/or destroy your information, unless a <u>PIPA exemption</u> applies. If a PIPA exemption applies, the organisation can either fully or partly refuse to comply with your request (see pages 23-24).

The organisation should also tell anyone else that they have shared your information with about the erasure.

If you ask, the organisation must also tell you that they have shared your information with other organisations.

If your information has been made public online – such as on social networks, forums or websites – then the organisation must take reasonable steps to inform the organisations with whom the information has been shared and to erase links or copies of that information.

3. When can the organisation say no?

The organisation can refuse to erase your information under certain circumstances, such as:

- when keeping your information is necessary for reasons of freedom of expression and information (this includes journalism and academic, artistic and literary purposes);
- when the organisation is legally obliged to keep your information such as to comply with financial or other regulations;
- when the organisation is carrying out a task in the public interest or when exercising their official authority;
- when keeping your information is necessary for establishing, exercising, or defending legal claims; and
- when erasing your information would prejudice scientific or historical research or archiving that is in the public interest; and
- when keeping your sensitive personal information is necessary for reasons of public health in the public interest.

The organisation can also refuse your request if it is "manifestly unreasonable" (see page 30).

If, after considering your request, the organisation decides it does not need to erase or destroy your information, it must still respond to you. It should explain to you why it believes it does not have to comply with your request and let you know about your right to complain about this decision to PrivCom, or through the courts. For more information, see pp. 27-29 (Making a complaint).

Writing and submitting your PIPA rights request

Organisations should describe in their privacy notice how to submit a PIPA rights request. They may have a form or a tool that you can use. In the absence of such an organisational form or tool, you may need to write your request independently and submit it to the organisation.

Be sure to use the contact method stated in the organisation's privacy notice. The organisation's privacy notice will have the contact information for the individual or team who deal with PIPA rights requests, such as the designated Privacy Officer.

People ask:

1. What should my PIPA rights request say?

Do's:

- your request should have a clear label (e.g., for your email subject line or a heading for your letter, use "PIPA rights request");
- include the date of your request;
- include your name (including any aliases, if relevant);
- include any additional information used by the organisation to identify or distinguish you from other individuals (e.g., customer account number or employee number);
- include your up-to-date contact details;
- include a comprehensive list of what personal information you want to access, based on what you need;
- include any details, relevant dates, or search criteria that will help the organisation identify what you want.

Don'ts:

- don't include other information with your request, such as details about a wider customer service complaint;
- don't include a request for all the information the organisation holds on you, unless that is what you want (if an organisation holds a lot of information about you, it could take them an extra 30 days to respond, or make it more difficult for you to locate the specific information you need in their response); or
- don't use threatening or offensive language.

Note: PIPA does not contain a "portability" clause, where you can demand your personal information in a certain format. You can tell the organisation how you would like to receive the information (e.g., by email or printed out), but they are not necessarily obliged to comply with this request. The organisation is only required to provide the information in a reasonable manner.

2. What should my PIPA rights request look like?

You can use the below PIPA rights request letter/email **master template** as a guide, adding exactly what information you are asking for from the organisation.

[Your full address] [Your phone number] [The date]

[Name and address of the organisation] [Reference number (if provided within the initial response)]

Dear [Sir or Madam / name of the Privacy Officer or person you have been in contact with]

SUBJECT: Personal Information Concern or Rights Request

[Your full name and address and any other details such as account number to help identify you]

This letter relates to the following matter under the Personal Information Protection Act 2016 (PIPA):

[Choose one as appropriate from a., b., or c.:]

a. I am concerned that you have not used my personal information properly.

[a. Give details of your concern, explaining clearly and simply what has happened and, where appropriate, the effect it has had on you.]

[or]

b. I wish to exercise my right to access my personal information.

[b. Give details of the personal information you wish to access]

Please supply the personal information you hold about me, which I am entitled to request under the Personal Information Protection Act 2016. [Give specific details of the information and, if known, where to search for the personal information you want, for example:

• my personnel file;

- emails between 'person A' and 'person B' (from 1 September 2019 to 1 October 2019)
- my medical records (between 2019 and 2023) held by 'Dr C' at 'hospital D'; and
- footage from the CCTV camera situated at ('location E') on 1 June 2021 between 11am and 5pm.]

If you need any more information, please let me know as soon as possible.

[or]

c. I wish to exercise my right to have my information corrected/blocked/erased/destroyed under PIPA

[c. Give details of what personal information you want corrected/erased/destroyed]

I understand that before reporting this matter to the Office of the Privacy Commissioner for Bermuda (PrivCom), I should give you an opportunity to address it.

If, after receiving your response, I would still like to report this matter to PrivCom, I will give PrivCom a copy of your response to consider.

You can find guidance on your obligations under privacy rights legislation on PrivCom's website (privacy.bm) as well as information on their regulatory powers and the action they can take.

Please acknowledge this message as soon as possible and send a full response within 45 days. If you cannot respond within that timescale, please let me know when you will be able to respond and why.

If there is anything you would like to discuss with me in relation to my letter of concern, please contact me on the following number [telephone number].

If you need advice on dealing with this request, the Office of the Privacy Commissioner for Bermuda can assist you. Their website is privacy.bm, or they can be contacted on 543-7748.

Regards, [Signature]

In the absence of a standard form provided by the organisation, you can also use any other written format that you deem appropriate.

3. Should I use an organisation's standard form?

Standard forms are not always provided. However, if a standard form is provided, the organisation may require you to use it. This means that if you fail to use the form provided by the organisation, the organisation may refuse your request. The Commissioner may require you to use available mechanisms before submitting a complaint to PrivCom. As a general rule, using an organisation's form should be the best way to get a response from the organisation.

Standard forms can make it easier for an organisation to deal with your PIPA rights request. They can:

- structure your request;
- prompt you to include necessary details and supporting documents; and
- let you know the best contact point at the organisation.

If you submit a complaint to PrivCom, you can ask us to review whether the standard form is reasonable.

4. Can someone else make a request on my behalf?

You can authorise someone else to make a PIPA rights request for you. However, you should consider whether you want the other person to have access to some or all of your personal information.

Examples of individuals making requests on behalf of other people include, but are not limited to:

- someone with parental responsibility, or guardianship, asking for information about a child
 or young person (for further information, please read our <u>Guide to PIPA</u> for organisations
 on requests for information about children under the age of 14);'
- a person appointed by a court to manage someone else's affairs;
- a solicitor acting on their client's instructions; or
- a relative or friend that the individual feels comfortable asking for help and has authorised to act on their behalf.

An organisation receiving the request needs to be satisfied that the other individual is allowed to represent you. The other person should provide evidence of authorisation to act on your behalf when the organisation asks them to do so. It is strongly recommended that they provide the evidence.

The organisation may ask for formal supporting evidence to show this, such as:

- written authorisation from you; or
- a power of attorney.

5. Should I keep a record of my request?

Yes. It is strongly recommended that you:

- keep a copy of any documents or written correspondence for your own records;
- keep any proof of postage or delivery (such as a postal reference number), if available; and

¹ Section 16 of PIPA

• take a screenshot before submitting your request if using an online submission form.

Where relevant documents are not available for you to copy, consider making a written log of your request. This should include key details, for example:

- 1. the date and time of your request;
- 2. the location (e.g., if your request was made in person);
- 3. the contact number or submission form you used;
- 4. the details of any contacts you have interacted with;
- 5. notes about any personal information you asked for;
- 6. any further information that the organisation may have asked you to provide; and
- 7. any reference numbers given to you and other relevant information.

This written log will provide helpful evidence if you wish to:

- follow up your request;
- make a complaint; or
- complain about an organisation's response at a later stage.

What can I expect after submitting a PIPA rights request with an organisation?

People ask:

1. How long does an organisation have to respond to my request?

An organisation typically has **45 days to respond** to your request.

If your request is complex, the organisation may need extra time to consider your request, and they can take up to **an extra 30 days to respond** under certain conditions.

If they are going to do this, they should let you know promptly why they need more time and when you can expect to receive their response.

The organisation might need you to prove your identity. However, they should only ask you for just enough information to be sure you are the right person.

Additionally, the organisation may ask you for further information if they believe that your request is incomplete.

If the organisation asks you to prove your identity or your request is incomplete, then the 45-day time period for the organisation to respond to your request begins from when they receive this additional information.

2. Can an organisation charge a fee?

Following consultation with the Commissioner, the Minister responsible for PIPA may prescribe any applicable fees.

Note: An organisation cannot charge you a fee if there is an error or omission in the personal information that it holds on you and you are requesting the organisation to correct the inaccurate personal information.

3. What should an organisation send back to me?

When an organisation responds to your request, they should typically tell you whether or not they use your personal information and, if they do, give you copies of it. The organisation should also include:

- what purpose(s) they are using your information for;
- who they are sharing your information with;
- how long they will store your information, and how they made this decision;

- details on your right to challenge the accuracy of your information, your right to have your information deleted, and your right to block the use of your information;
- your right to complain to PrivCom;
- details about where they got your information from; and
- whether and how they have transferred your information to a third party outside Bermuda.

If you wish to receive specific details, it is highly recommended that you state this in your request.

4. Will I always receive everything I asked for?

You may not always receive everything you have asked for. Depending on the circumstances:

- you may receive only part of the information you asked for; or
- the organisation may not provide you with any personal information at all (for exemptions, see page 24).

If you make a request for access to your personal information of a medical or psychiatric nature, or your personal information is kept for the purposes of, or obtained in the course of, carrying out social work relating to you, an organisation may refuse to provide access to personal information if disclosure of your personal information would be likely to prejudice your physical or mental health.²

If an organisation refuses your medical records access request, you can ask the organisation to provide access to your personal information to a health professional who has expertise in relation to the subject matter of the record.³ The health professional will then determine whether or not disclosure of your personal information to you would be likely to prejudice your physical or mental health.

An organisation can also refuse to comply with your PIPA rights request if they think it is "manifestly unreasonable" (see page 30).

There can be other reasons why you may not receive all the information you requested, e.g., when an exemption applies, or the type of information you asked for is not covered by an access request.

5. Am I entitled to receive copies of entire documents?

You are not. Your right of access does not entitle you to receive full copies of original documents held by an organisation: only your personal information contained in the document.

Scenario

You ask your bank to access your personal information, including full copies of your bank statements. Your bank is not required to provide copies of the actual bank statements. However, they must

² Section 18(1) of PIPA

³ Section 18(2) of PIPA

provide you with your personal information contained within them. For example, the bank may provide you with a list of transactions. By doing so, they have complied with your access request without having to give you a full copy of the original bank statements.

6. What is an exemption?

An organisation may withhold all or some of your personal information because of an exemption stipulated in PIPA.⁴ Exemptions protect specific types of information or how certain organisations process information.

In rare cases, an organisation may not even have to let you know whether they hold your personal information.

An organisation may also refuse your request to access your information if it includes personal information about someone else, except in situations where:

- the other individual has agreed to the disclosure; or
- it is reasonable to give you this information without the other individual's consent.

When deciding on your access right, an organisation must balance your right of access to your personal information against the other individual's rights with respect to their own information. This may lead the organisation to refuse your access request. An organisation may not provide access to your personal information if the disclosure of your personal information could reasonably be expected to threaten the life or security of another individual.

Alternatively, the organisation may attempt to remove or edit out (redact) the other individual's information before sending your information to you. This could mean you only receive partial information – such as copies of documents showing blacked-out text or missing sections.

The organisation will still need to:

- tell you why they are not taking action;
- explain how you can challenge this outcome.

If you want to learn more about exemptions and exclusions under PIPA, see our <u>Guide to PIPA</u> and <u>Guidance on uses of personal information for organisations</u>.

7. What if the organisation requires proof of identity (ID)?

Organisations must take reasonable steps to verify the identity of the applicant. This may include an ID check. These steps are part of an organisation's measures to protect your personal information from unauthorised access.

⁴ Sections 22-25 of PIPA

If an organisation requires proof of ID (e.g., valid driver's licence, passport, etc.), your PIPA rights request is not considered complete until you provide it. Therefore, the 45-day time period for the organisation to respond does not begin until they have received proof of ID from you.

8. What information is not covered by my request?

The right of access does not cover all types of information or uses of personal information. Examples include:

- information used for personal/domestic purposes (e.g., family members' pictures of you);
- images of you captured on a domestic CCTV system within the boundary of your domestic property; and
- information about the medical records of a relative who has been dead for at least 20 years.

Section 4 of PIPA describes other situations where the use of personal information is excluded from the Act.

9. Can I resubmit the same request?

Yes, you can ask an organisation for access to your information more than once. However, they may be able to refuse your request if:

- they haven't yet had the opportunity to deal with your earlier request; or
- not enough time has passed since your last request (e.g., your information has not changed since then).

Remember! An organisation may ask the Commissioner to authorise the organisation to disregard one or more of your requests due to the repetitive and systematic nature of your request(s)⁵ if:

- your request has been made with no real purpose except to cause the organisation harassment or disruption to their business activities;
- you have no genuine intention of accessing your personal information (e.g., you may offer to withdraw your request in return for some kind of benefit, such as a payment from the organisation); or
- your requests would amount to an abuse of the right to make those requests or are otherwise frivolous and vexatious.

10. How should I raise my concerns about how an organisation has used my information?

Initially, you should reach out directly to the organisation to raise concerns (see page 26). You must reach out to the organisation in writing. If necessary, you can adjust the master template provided on pp. 18-19 to help you raise your concern.

⁵ Section 30 of PIPA

What can I do if the organisation does not respond to my request or if I am dissatisfied with the outcome of my PIPA rights request?

You can resolve many problems by directly communicating with the organisation.

Step 1. Send your concerns to the organisation

If you are concerned about how an organisation is using your personal information, you can write to them.

If you are unhappy with how the organisation has handled your request, you should:

- express to the organisation that you are not satisfied; and
- ask them in writing to respond.

When raising a concern, the organisation may or may not provide forms or tools that can assist you.

If you have already received a response but are unhappy with it, you should first send your concerns to the organisation. You must do so in writing.

The added value of having everything in writing is that it will allow you to explain your concern, give evidence and state your desired solution. It will also provide clear proof of your actions if you decide to challenge the organisation's initial response.

If you think personal information is missing from their response, you should clearly list what other information you think they hold and would like access to. This may help the organisation review their records.

Remember to always keep copies of any correspondence about your request or concern.

When writing to the organisation, you may choose to use the master template provided on pp. 18-19. PrivCom recommends that you adjust the master template to include the details of your concern. The use of the master template is intended to serve as guidance when formally communicating with the organisation.

Making a complaint

In a seashell:

You also have the right to complain to an organisation if you think the organisation has not used your personal information responsibly, ethically, fairly, lawfully, and in line with good practice.

If you have sent your request to an organisation and you still haven't received a response, or if you remain unhappy with the organisation's handling of your personal information and/or your PIPA rights request, you can make a written complaint to PrivCom.

People ask:

1. When can I make a complaint to an organisation?

You can complain to an organisation about how it is using your personal information, if the organisation:

- has not properly responded to your PIPA rights request (see the previous section, pp. 26-27);
- is not keeping information secure;
- holds inaccurate information about you;
- has shared information about you in a way that is not described in its privacy notice;
- is keeping information about you for longer than is necessary;
- has collected information for one purpose and is using it for something else; and/or
- has not upheld any of your privacy rights (i.e., right to access your personal information, right to access your medical records, right to have your information corrected, right to have your information blocked, right to have your information erased or destroyed.

2. How do I make a complaint to an organisation?

Step 1. Address your complaint directly to the organisation.

Before bringing your complaint to PrivCom, you should give the organisation an opportunity to address the issue at hand and sort it out. Many privacy complaints can be resolved quickly and easily with the organisation. Make sure to double check the organisation's address and contact details are correct.

You can use the master template provided on pp. 18-19 to email or send a letter to the organisation.

Include full details of your concern at the beginning of your email/letter. Include all relevant details in your email/letter, such as an account/patient/customer reference number to help the organisation identify you. To evidence your complaint, enclose copies of all relevant documents that you have

available. Do not send the originals: you might need them later. Don't include unnecessary documentation.

If the organisation responds to your complaint but it looks like they have misunderstood you or not fully addressed the concern that you previously communicated to them, follow up with the organisation in writing and let them know that your concern remains unresolved.

Step 2. Give the organisation 45 days to respond to your complaint.

It may take the organisation time to consider your complaint. However, the organisation should acknowledge receipt of your complaint promptly and let you know the estimated date of their response.

If you have not heard back from the organisation within 45 days of submitting the complaint, or your complaint remains unresolved after 45 days following the organisation's acknowledgement of your complaint, follow up with the organisation politely.

Step 3. If you don't understand or you're unhappy with the response you receive from the organisation, ask them for clarification.

Organisations are obliged to explain to you why they use your personal information in the manner they do and/or why they have refused your PIPA rights request.

If the organisation responds to the complaint in a way that you do not understand, follow up in writing and ask for clarification. You may want to use the master template on pp. 18-19.

Step 4. If you are unhappy with the organisation's response to your complaint, report your complaint to PrivCom.

If the organisation does not respond to your written request within 45 days and/or you remain unsatisfied with the outcome of your PIPA rights request, you may submit a written complaint to PrivCom.

3. What do I need to do before I can complain to PrivCom?

You can complain to PrivCom about the way an organisation has handled personal information.

Before you complain to us, you need to have:

- complained directly to the organisation;
- followed up with the organisation if you <u>have not</u> received an acknowledgement of your complaint after 45 days;
- followed up with the organisation if you <u>have</u> received an acknowledgement of your complaint and it remains unresolved after 45 days; and/or

• asked for clarification from the organisation if you have had a response you don't understand.

If you have taken these steps and the organisation is still refusing to respond to you, you can submit a complaint to PrivCom.

Remember that PrivCom cannot:

- act as legal representation;
- award compensation for financial or emotional harm caused; or
- determine whether an organisation has committed an offence.

However, if PrivCom is of the view that the organisation has not processed your request as it should have, PrivCom can:

- give the organisation advice on how to properly respond to a PIPA rights request;
- provide instructions on how the organisation may address the problem;
- issue public admonishments and formal warnings;
- issue directive orders requiring the organisation to act; and
- refer the matter to the Department of Public Prosecutions (the "DPP") where the organisation may be subject to criminal penalties following litigation in court.

When submitting a written complaint to PrivCom, send copies of all the documents you have in order to support your complaint.

If you suffer financial loss or emotional distress as a result of an organisation's failure to comply with PIPA, a court may grant you compensation from the organisation.⁶

⁶ Section 21 of PIPA

What does "manifestly unreasonable" mean?

Under PIPA, an organisation is not required to comply with your access request or the other PIPA rights requests outlined above – right to correction, right to erasure, right to block – if they think your request is "manifestly unreasonable".

There is no set definition of what makes a PIPA rights request "manifestly unreasonable". It will depend on the specific circumstances of your request. An organisation should explain the reasons for their decision, and as part of a written complaint you can ask PrivCom to review this decision.

For example, an organisation may consider a request to be "manifestly unreasonable" when it is clear that:

- it has been made with no real purpose except to cause them harassment or disruption to their business activities;
- the person making the request has no genuine intention of accessing their information (e.g., they may offer to withdraw their request in return for some kind of benefit, such as a payment from the organisation); or
- the organisations hasn't yet had the opportunity to deal with your earlier request.

To decide whether a PIPA rights request is "manifestly unreasonable", an organisation must consider each request on a case-by-case basis and be able to explain their reasoning to you.

For example, an organisation may consider your PIPA rights request to be "manifestly unreasonable" when it is clear that the request has been made with no real purpose except to cause harassment or disruption to the organisation.

In such circumstances, the organisation can refuse to deal with the request.

In either case, the organisation will need to inform you and justify the decision.

The above-mentioned examples are not intended to be an exhaustive list of the types of individual rights that may be considered "manifestly unreasonable". The facts of the matter shall dictate such a determination.

The organisation must still respond to you. It should explain to you why it believes your request is manifestly unreasonable and let you know about your right to complain about this decision to PrivCom or through courts. For more information, see pp. 27-29 (Making a complaint).

Compensation for financial loss or distress

In a seashell:

Under section 21 of PIPA, if you suffer financial loss or emotional distress as a result of an organisation's failure to comply with PIPA, a court may grant you compensation from the organisation if you bring legal action.

People ask:

1. How much am I entitled to in compensation in the event an organisation has failed to use my personal information lawfully and fairly?

The court will determine the amount of compensation you are entitled to for each violation of PIPA.

2. Do I need to contact PrivCom if I intend to pursue the matter in court?

No, but you are welcome to inform PrivCom for our awareness. In the event PrivCom decides to refer a matter to the Department of Public Prosecutions if the organisation is found having committed an offence under section 47 of PIPA, the organisation may be held liable.

The Individuals' Guide to PIPA does not constitute legal or other professional advice. You should consult with your professional legal advisor for legal or other professional advice.