Victorian Data Sharing Act 2017

Guidance for departments and agencies

VICTORIA State Government | Premier and Cabinet

Victorian Data Sharing Act 2017

Guidance for departments and agencies

The *Victorian Data Sharing Act 2017* (the Act) commenced on 6 December 2017. This document is intended to support Victorian departments and agencies understand the Act.

Contents

General overview of the Act

Background

Why is the Act needed?

The Victorian Government collects a lot of data when serving the community. For too long this data has been in silos. There is an opportunity to more widely share and use this data to improve policy and services for Victorians.

The *Victorian Data Sharing Act 2017* (the Act) promotes data sharing across government by:

- creating a clear framework for sharing and using data for policy making, service planning and design
- establishing the Chief Data Officer (CDO) who leads the Victorian Centre for Data Insights (VCDI) in working to transform how government uses data.

What is the approved purpose of data sharing under the Act?

The Act allows for data-sharing:

- within government departments and agencies (**not** with community organisations or businesses)
- for the approved purpose of 'policy making and service planning and design' (**not** for targeting services or regulatory activities to individuals).

How does the Act help your organisation share data?

The Act gives your organisation the clear permission to share:

- identifiable data (personal and health information) with the CDO on request and with departments (as data analytics bodies)
- data that Victorian laws might otherwise prevent your organisation from sharing with the CDO, where the CDO requests this data. These laws are called 'secrecy provisions' under the Act.

How will the Chief Data Officer work with your organisation?

The CDO is set up under the Act to help government use data better.

The Act allows the CDO to carry out functions like:

- conducting data projects with your organisation
- working with your organisation to build public sector data analytics capability
- making the results of data projects available if appropriate.

How does the data request process work?

The CDO has the power to request data or information about data held by your organisation to inform policy making, service planning and design.

Generally, the CDO will only request data after agreeing with your organisation the purpose, scope and nature of the data request.

What type of data can the CDO request from your organisation?

The CDO can request any data or information about data held by your organisation.

However, the CDO cannot request data that could:

- prejudice national security
- disclose the identity of a confidential source or someone in a witness protection program
- disclose investigative measures or procedures.

Who can the CDO request data from?

The CDO can request data or information about data from most departments and agencies.

These bodies fall into two groups:

- 'data sharing bodies' (departments, administrative offices, statutory agencies, and Victoria Police) which **must** respond to a request from the CDO, either by providing the data or providing reasons for refusing the request
- 'designated bodies' (judicial bodies like courts and tribunals, and independent and oversight bodies like Independent Broad-based Anti-corruption Commission, the Victorian Electoral Commission and the Victorian Ombudsman) which can, but **do not have to** respond to a request from the CDO.

Click here for more information on how the Act applies to your organisation.

Making sure data is used in the right way

How does the Act protect and safeguard data sharing and use?

The Act provides a range of protections and safeguards, including:

- requiring all data to only be used for informing policy making, service planning and design
- providing for how identifiable data should be handled

- annual reporting and notifying of possible breaches to the Office of the Victorian Information Commissioner (OVIC) and the Health Complaints Commissioner (HCC)
- providing that existing obligations under privacy laws continue
- new offences for unauthorised access, use or disclosure of information.

How will the Act protect identifiable data?

The Act allows your organisation to share identifiable data (personal or health information) for informing policy making and service planning and design.

After receiving identifiable data, the CDO and departments (as data analytics bodies) must take reasonable steps to de-identify the data appropriately. For more information on this requirement, see the De-identification Guideline issued by the CDO.

What independent oversight mechanisms exist for the CDO?

The CDO must report annually to Victoria's privacy regulators: the OVIC and HCC. This report must include matters, such as the steps taken to ensure compliance with privacy laws, the data projects that have been undertaken, details of data requests and refusals, and the issues and challenges that have arisen.

The Act also requires the CDO and departments (as data analytics bodies) to report any breach of privacy laws to the privacy regulator and original data provider.

How will data be kept secure under the Act?

While not directly addressed in the Act, the CDO and all other departments and agencies must comply with the Victorian Protective Data Security Framework and Standards. This requires departments and agencies to apply security controls when sharing data, including through investing in security management, information security, ICT security and personnel security.

What if there has been unauthorised access, use and disclosure of data?

The Act creates two new offences:

- a general offence for unauthorised access, use or disclosure of data or information (with a penalty of 2 years imprisonment or 240 penalty units or both)
- a more serious offence where the person knows or is reckless that the data or information may be used to endanger life or safety, assist in committing an offence or impede justice (with a penalty of 5 years imprisonment or 600 penalty units or both).

How the Act works with other laws and jurisdictions

How does the Act interact with privacy laws?

Privacy laws allow identifiable data to be shared where this is authorised by another Victorian law. The Act works within privacy laws by providing a new 'authorisation by law' for sharing and using identifiable data (in addition to existing privacy exceptions).

Otherwise, obligations under privacy laws (including the information and health privacy principles, and the Victorian Protective Data Security Framework and Standards continue to apply. This means that the sharing of data that is already allowed under privacy laws will not be affected.

How does the Act interact with secrecy provisions?

There are many Victorian laws which prohibit or restrict data sharing within government. These laws are called 'secrecy provisions' under the Act. The Act allows data to be shared on the CDO's request, even if a secrecy provision would otherwise prevent this.

How does FOI apply under the Act?

Requests for data provided by departments and agencies

The Act provides that the *Freedom of Information Act 1982* (FOI Act) does **not** apply to documents that contain data held by the CDO or by departments (as data analytics bodies) that have been provided by departments and agencies under the Act. However, the FOI Act still applies to the data held by those departments or agencies. This is because those departments and agencies are best placed to decide whether the data should be released under FOI.

Where the CDO or departments (as data analytics bodies) receive an FOI request seeking access to data provided to them under the Act, they should ask the applicant to make a new FOI request to the relevant department or agency instead.

Requests for analytics results

The FOI Act **does** apply to any new document created by the CDO or departments (as data analytics bodies) as a result of data integration and analytics. Where the CDO or departments receive an FOI request seeking access to their analytics results, they must decide whether the document should be released under FOI.

Will this Act allow your organisation to share with other jurisdictions?

One of the CDO's functions under the Act is to help lead and coordinate data sharing with other jurisdictions. Other than this, the Act does not directly deal with data sharing with the Commonwealth or other states and territories.

Victorian departments and agencies can still enter into information sharing agreements with the Commonwealth or other jurisdictions to share data, without any impact from the Act.

How does this Act interact with data reform in other jurisdictions?

New South Wales and South Australia also have similar data sharing laws, supported by data analytics centres. The Act has been informed by lessons learnt from these jurisdictions.

How does the Act interact with other Victorian data sharing laws?

The Act is part of a number of Victorian laws that focus on information or data sharing. This includes laws to enable information-sharing to reduce the risk of family violence, to increase hospital safety and quality assurance, and to improve early intervention and services for children.

These laws work together to promote a more sophisticated approach to using data to improve policy and services for Victorians.

Specific guidance for departments and agencies

How does the Act apply to your organisation?

Your organisation has different rights and obligations depending on your 'type' under the Act; as a:

Data sharing body **Designated body** **Data analytics body**

Take these steps to work out which type your organisation falls under:

Question 1.

Is your organisation a department?

→ **Yes** – your organisation is a data sharing body and a data analytics body.

→ **No** – move to Question 2.

Question 2.

Is your organisation an independent or oversight body?

Is it a judicial body (like a Court or tribunal) or does it perform oversight functions like the Independent Broad-based Anti-corruption Commission, the Victorian Electoral Commission and the Victorian Ombudsman?

→ **Yes** – your organisation is a designated body

→ **No** – move to Question 3.

Question 3.

Is your organisation another type of government body?

Is it an administrative office, statutory agency or Victoria Police?

→ **Yes** – your organisation is a data sharing body

→ **No** – your organisation *may not* be covered by the Act. Contact us to make sure.

Please contact us if you need further assistance to work out which type your organisation falls under.

How does the Act affect data sharing bodies?

How can the Act help your organisation?

There are many laws and policies that make it hard for departments and agencies to work out whether and how they can share data.

This Act makes it easier to share data within government for informing policy making and service planning and design.

It gives data sharing bodies the clear permission to share:

- identifiable data (personal and health information) with the CDO on request and with departments (as data analytics bodies)
- data that Victorian laws might otherwise prevent them from sharing with the CDO, where the CDO requests this data. These laws are called 'secrecy provisions' under the Act.

What must your organisation do under the Act?

The Act allows the CDO to request data or information about data from a data sharing body.

There are two key things a data sharing body **must** do under the Act:

1. After receiving a request, a data sharing body must respond by either providing the data or information, or providing reasons for refusing the request
2. If a data sharing body providing data knows that the data is subject to a 'secrecy provision', it must let the CDO know.

How will the CDO request data from your organisation?

The CDO will send a written notice to your organisation that sets out:

- the requested data, or information about data held by you
- why the data or information is required
- how the data or information will be handled.

How long does your organisation have to respond to a data request?

After receiving a data request from the CDO, a data sharing body has 10 business days to respond, or a later time as agreed with the CDO.

Generally, the CDO will only request data after agreeing with your organisation the purpose, scope and nature of the data request.

Who from your organisation can respond to a request?

All data requests are addressed to the head of your organisation ('responsible officer'). Only the head of your organisation can respond to a request, unless this is delegated to someone else.

For example, for departments - the responsible officer will be your Secretary, for administrative offices - this will be your chief executive, and in the case of Victoria Police - your Chief Commissioner.

How does your organisation refuse a request?

A data sharing body may refuse a request for data or for information about data by writing to the CDO and the Secretary of DPC, and setting out the reasons for refusal.

Possible reasons for refusal include if disclosing the data would:

- breach a law
- prejudice a legal process (e.g. an investigation of a breach of law, the enforcement of a law or a court proceeding)
- endanger the safety, health or welfare of an individual or group.

However, your organisation can refuse for any reason.

How should your organisation deal with secrecy provisions?

There are many Victorian laws which prohibit or restrict data sharing within government to improve policy and services. These laws are called 'secrecy provisions' under the Act. The Act allows data to be shared on the CDO's request, even if a secrecy provision would otherwise prevent this.

To ensure this data is appropriately protected, your organisation must:

- let the CDO know as soon as you become aware that a secrecy provision applies
- get the relevant Minister's approval before the CDO can disclose any data that is subject to a secrecy provision.

For highly sensitive types of data, the Act allows secrecy provisions to be preserved by regulations to be made under the Act.

Key things for your organisation to consider:

- **Explore how the Act can help your organisation**. For example, does your organisation want to share and use data in projects for the purpose of policy and service planning and design? Can the Act help to remove some of the legal barriers to data sharing proposed under the project?

- **Decide how your organisation wants to respond to requests**. For example, do you want to provide data or information through a central contact person in your organisation? You may also want to decide if there is a need to delegate the obligation to respond to others in your organisation.

- **Consider your privacy policy and collection notices**. The Act provides a new permitted purpose for sharing and using identifiable data your organisation holds. You may want to review your privacy policy and collection notices to ensure this new purpose is covered. For example, you may want your policy or notice to refer directly to the Act and its approved purpose, or more generally to 'any other purpose permitted by law'. You should also ensure your privacy officer is aware of the approved purpose of the Act. For more information about collection notices more generally, read **OVIC's guidelines on collection notices**.

How does the Act affect designated bodies?

How can the Act help your organisation?

There are many laws and policies that make it hard for departments and agencies to work out whether and how they can share data.

This Act makes it easier to share data within government for informing policy making and service planning and design.

It gives designated bodies the clear permission to share:

- identifiable data (personal and health information) with the CDO on request and with departments (as data analytics bodies)
- data that Victorian laws might otherwise prevent them from sharing with the CDO, where the CDO requests this data. These laws are called 'secrecy provisions' under the Act.

Does the Act create new obligations for your organisation?

No. The Act allows the CDO to request data or information about data from a designated body. However, while your organisation may choose to respond to a request, there is no obligation to do so.

Your organisation can still benefit from the legal permissions under the Act though. This recognises your organisation's independence and oversight role.

Key things for your organisation to consider:

- **Explore how the Act can help your organisation**. For example, does your organisation want to share and use data in projects for the purpose of policy and service design? Can the Act help to remove some of the legal barriers to data sharing proposed under the project?

- **Decide how your organisation wants to respond to requests**. Even though there is no legal obligation to respond, you may want to consider how you want to your organisation's processes should you receive a CDO data request.

- **Consider your privacy policy and collection notices**. The Act provides a new permitted purpose for sharing and using identifiable data your organisation holds. You may want to review your privacy policy and collection notices to ensure this new purpose is covered. For example, you may want your policy or notice to refer to 'any other purpose permitted by law', and ensure your privacy officer is aware of the approved purpose of the Act. For more information about collection notices more generally, read **OVIC's guidelines on collection notices** .

How does the Act affect data analytics bodies?

How can the Act help your organisation?

There are many laws and policies that make it hard for departments and agencies to work out whether and how they can share data.

This Act makes it easier to share data within government for informing policy making and service planning and design.

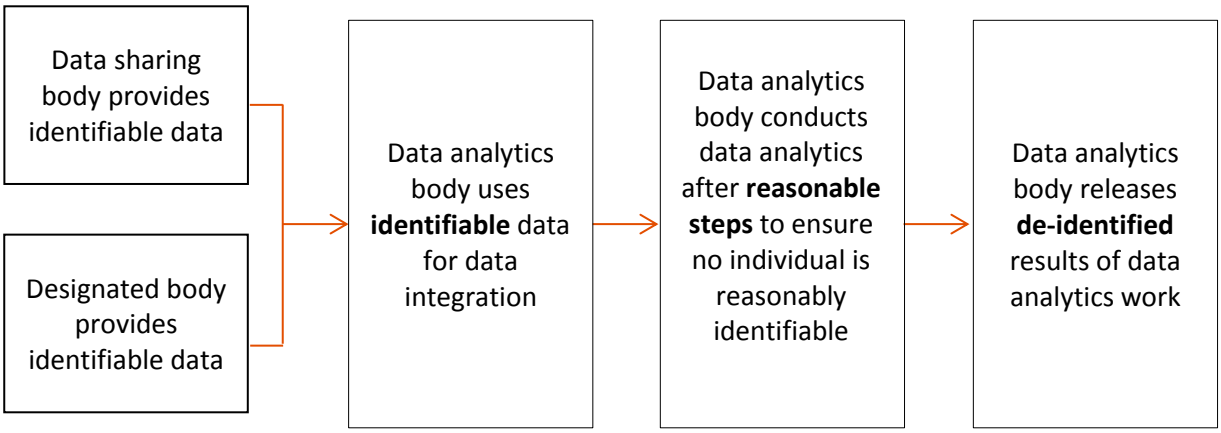
It gives data analytics bodies the clear permission to receive and use identifiable data (personal and health information) to carry out data integration, in order to inform policy making and service planning and design.

What must your organisation do under the Act?

The Act allows the CDO and other departments and agencies to provide identifiable data to a data analytics body.

There are three key things a data analytics body **must** do under the Act:

1. After receiving identifiable data, it must only use it for the purpose of data integration
2. After integrating the data, it must take reasonable steps to ensure that no individual is reasonably identifiable in the data before performing data analytics work
3. Before disclosing the results of data analytics, ensure that no individual can be reasonably identified in the results.



What does using identifiable data for 'data integration' mean?

The Act only allows identifiable data to be used for the purpose of data integration. Data integration is defined broadly, to mean the combination or collation of two or more data sets to better understand a particular issue.

How can your organisation take reasonable steps in the analytics environment?

In deciding whether your organisation has taken 'reasonable steps to ensure that no individual is reasonably identifiable' in the analytics environment, you must consider:

- the de-identification techniques applied to the data
- other privacy safeguards and protections used in the analytics environment

- other considerations in guidelines to be developed by the CDO.

For more information on the techniques and considerations needed to meet this 'reasonable steps' requirement, see the De-identification Guideline issued by the CDO.

What must your organisation do before disclosing results?

Before disclosing the results of data analytics, your organisation must ensure that the data 'no longer relates to a reasonably identifiable individual'. This requirement is consistent with the legal definition of 'de-identified' in privacy law.

The requirement at the disclosure phase is stricter than the requirement at the analytics phase (which is an obligation to 'take reasonable steps to ensure that no individual is reasonably identifiable'). This reflects the fact that analytics takes place in the controlled trusted user environment, while the disclosure of analytics results may be in the public domain.

For more information on the techniques and considerations needed to meet this 'de-identified' requirement, see the De-identification Guideline issued by the CDO..

How should your organisation notify of privacy breaches?

The Act requires data analytics bodies to notify of any past or potential breach of privacy laws to:

- OVIC (where this relates to personal information) or HCC (where this relates to health information), , and
- the original data provider

as soon as your organisation becomes aware. Where the data breach relates to both personal and health information, data analytics bodies must notify both regulators and work with them to clarify which will be a lead regulator in each case.

This obligation to report only applies to data handled under the Act that is in the control of your organisation. It is up to each data analytics body to decide how best to meet this requirements under the Act.

Key things for your organisation to consider:

- **Decide if your organisation wants to use identifiable data**. All Secretaries of departments hold the power to receive and use identifiable data under the Act. Consider if there are parts of your department that should be delegated this power given:

  A. the nature and set up of the team, and how this aligns with the purpose of informing policy making and service planning and design
  B. the proposed uses of the power to use identifiable data, and how this aligns with the purpose of data integration
  C. the proposed safeguards and protections to handle identifiable data

- **Decide how to set up appropriate arrangements to handle identifiable data**. If there is a part of the department delegated the powers to use identifiable data, consider how you want to set up the arrangements to handle identifiable data appropriately, such as ensuring you always take reasonable steps to ensure no individual can be reasonably identified in the analytics environment (considering the De-identification Guideline issued by the CDO), and the checks you want to put in place before any results of analytics work is released. You should also ensure support staff understand their requirements, including how to comply with privacy laws and about the offence provisions

- **Decide how to set up breach notification arrangements**. It is up to you how you wish to comply with this obligation. For example, your organisation may choose to use your existing notice templates and data breach response plan, or develop new ones.

- **Consider your privacy policy and collection notices**. The Act provides a new permitted purpose for sharing and using identifiable data your organisation holds. You may want to review your privacy policy and collection notices to ensure this new purpose is covered. For example, you may want your policy or notice to refer to 'any other purpose permitted by law', and ensure your privacy officer is aware of the approved purpose of the Act. For more information about collection notices more generally, read **OVIC's guidelines on collection notices**