Office of the Victorian Information Commissioner

OVIC Regulatory Action Policy 2019 – 2021

Freedom of Information | Privacy | Data Protection

Foreword to Regulatory Action Policy

Members of the Victorian community interact with government every day. These interactions can range from the mundane to the profound; and in almost every interaction, information is created or collected.

Victorian State and local government departments and agencies generally understand the importance and the value of the information they hold on behalf of the communities they serve. I have observed that, for the most part, these organisations endeavour to handle information responsibly, hold it securely, and provide fair access to it where appropriate. As such, a central part of my office's role as a regulator is to act as a facilitator and guide, helping departments and agencies do the right thing.

But even though most agencies want to do the right thing, sometimes mistakes are made. At other times, actions are taken for the wrong reasons. And when rules are broken, the community rightly expects that its regulators will take strong action. To allow this to occur, the *Freedom of Information Act 1982* (Vic) (FOI Act) and the *Privacy and Data Protection Act 2014* (Vic) (PDP Act) provide the Office of the Victorian Information Commissioner (OVIC) with a wide range of powers to conduct regulatory action.

The regulatory action that OVIC can take includes informal preliminary enquiries and engagement, audits and examinations, investigations, compliance notices and associated penalties as well as public reports.

This Regulatory Action Policy explains how OVIC will use its powers. Our goal is to continue to instil in the Victorian public sector a culture that promotes fair public access to information while ensuring its proper use and protection. By doing so, we aim to build community trust in government handling of information.

Our focus will continue to be on education, guidance and constructive feedback. But where necessary and appropriate, OVIC will use its statutory powers to investigate serious or concerning practices under both the FOI Act and PDP Act.

Our response to any incident or allegation will be guided by the factors outlined in this policy, which describe a risk-based, proportional and targeted approach to regulatory action.

We will continue to review and improve the practices outlined in the Regulatory Action Policy, to ensure that we are achieving our goals, and doing so transparently, independently and impartially.

Sven Bluemmel
Information Commissioner

OVIC regulates the Victorian Government and advises the community about how the public sector collects, protects, uses and shares information.[1]

This policy articulates OVIC's regulatory approach.[2] In this policy "regulatory action" means OVIC activity that promotes, assures or enforces the *Freedom of Information Act 1982* (Vic) (**FOI Act**) and the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**).

The *Regulatory Action Policy* consists of two parts:

- The first part sets out OVIC's general approach to regulatory action and the common principles that guide OVIC's regulatory activities. It also outlines how OVIC monitors and reports on its performance.
- The second part consists of three schedules dealing with OVIC's three functional areas: privacy, freedom of information and information security. These schedules outline the regulatory functions and powers the PDP Act and the FOI Act confer on OVIC and OVIC's approach to how they are exercised.

Who OVIC regulates

OVIC regulates these bodies under the PDP Act and FOI Act (**regulated body** or **regulated bodies**).

- **Privacy** - "organisations" defined in section 3 and section 13 of the PDP Act including departments, councils, Victoria Police, public entities,[3] courts and tribunals.[4]
- **Freedom of Information –** Section 13 of the FOI Act gives a right to access documents of Ministers and "agencies"[5] such as departments, councils, TAFES, public hospitals and public schools.
- **Information security** – Public sector agencies and bodies defined in section 84 of the PDP Act including departments, public entities[6] and Victoria Police.[7] The PDP Act excludes councils[8], universities, ambulance services, public hospitals, public health services and multipurpose services under the *Health Services Act 1988* (Vic).

Goals of Regulatory action

OVIC uses the regulatory powers in the PDP Act and FOI Act to:

- **Engage constructively with the Victorian public sector** to build capacity and embed a culture that promotes fair access to information while ensuring its proper use and protection.
- **Foster public trust and awareness** of the Victorian public sector's responsibility, ability and

[1] This policy should be read in conjunction with OVIC's Policy and Procedure for Exercising Coercive and Other Powers.

[2] References to OVIC include the Information Commissioner, the Public Access Deputy Commissioner and the Privacy and Data Protection Deputy Commissioner, as appropriate. Some regulatory functions and powers are vested only in the Information Commissioner, or in the Information Commissioner and the relevant Deputy Commissioner.

[3] As defined by section 5 of the *Public Administration Act 2004* (Vic).

[4] Also includes bodies established for a public purpose by an Act, State Contract services providers, ministers, parliamentary secretaries, office holders appointed by a Minister or the Governor in Council.

[5] Agency is defined in section 5 of the FOI Act.

[6] As defined by section 5 of the *Public Administration Act 2004* (Vic).

[7] Other bodies are VCAT, IBAC, VAGO, VEC, the Commissioner for Children and Young People, the Health Complaints Commissioner, the Ombudsman Victoria, the Victim of Crimes Commissioner, the Mental Health Tribunal, the Victorian Inspectorate, Electoral Boundaries Commission, Crime Statistics Agency and OVIC.

[8] Councils may be captured if they are Committees of Management under the *Crown Land Reserves Act 1978* (Vic) or if they are cemetery trusts under the *Cemeteries and Crematoria Act 2003* (Vic).

commitment to handling information in a responsible and accountable manner.

- **Influence government** to consider information rights in developing new policies or programs.
- **Deter conduct** that contravenes or is contrary to the objects of the PDP Act or FOI Act.

Guiding principles

When taking regulatory action, OVIC is guided by the following principles:

- **Independent** – OVIC exercises its regulatory powers independent of government.
- **Collaborative** – OVIC engages with the public and regulated bodies openly and constructively.
- **Targeted and proportional** – OVIC targets issues based on how likely they are to occur and how severe the impact would be if they did occur. OVIC takes action that is proportionate to the issue being addressed.
- **Transparent and consistent** – OVIC's decisions, actions and performance are clearly explained and open to public scrutiny. OVIC's regulatory action is consistent in similar circumstances.

Independent

In its three functional areas, as an independent regulator, OVIC has the following aims.

Privacy

- Independently conciliate disputes about interferences with a person's privacy.
- Guide regulated bodies and the public about the PDP Act and Information Privacy Principles (**IPPs**).
- Audit or investigate a regulated body's privacy practices or prevalent privacy issues.

Freedom of information

- Provide guidance to regulated bodies and the public about the FOI Act.
- Review decisions of regulated body:
  - to refuse access to a document sought under an FOI request;
  - not to waive an application fee imposed in an FOI request;
  - not to amend or annotate a document.
- Resolve complaints against regulated bodies about actions taken or failed to be taken under the FOI Act.
- Develop Professional Standards that describe how regulated bodies should meet their obligations in the FOI Act to promote clear and consistent FOI decisions.
- Investigate how a regulated body performed, or failed to perform, its FOI functions and obligations.

Information security

- Promote continuous improvement through guidance and advice about information security.
- Monitor and assure compliance with the Victorian Protective Data Security Framework (**VPDSF**) and the PDP Act by review of protective data security plans and audits.

Collaborative

OVIC prefers to provide education and support to regulated bodies to promote understanding and proactive adherence to the PDP Act and FOI Act. Nevertheless, OVIC also monitors compliance, and investigates issues that are brought to its attention – for example issues that are reported by the public, self-reported by a regulated body or referred to OVIC by another regulator.

When an issue is identified, OVIC usually starts by contacting the affected regulated body and any complainant. OVIC generally tries to resolve issues by agreement before resorting to formal regulatory action. This approach helps resolve issues or disputes quickly and efficiently.

Working with other regulators

OVIC is part of a broader integrity framework and works with other regulators to limit investigations being duplicated. OVIC works with other regulators formally through referral provisions, and informally through research and education. Regulators that OVIC works with include the Independent Broadbased Anti-corruption Commission, Victorian Ombudsman, the Health Complaints Commissioner, the Mental Health Complaints Commissioner, the Disability Services Commissioner, the Commission for Children and Young People and the Office of the Australian Information Commissioner.

Targeted and proportional

OVIC takes a risk-based approach in deciding when and how to take regulatory action. OVIC considers the harm that the PDP Act and FOI Act aim to reduce, then applies its resources to areas where the risk of that harm is greatest or where that harm would have the most serious impact.

OVIC also monitors trends and consults with regulated bodies to identify emerging issues and in proactively manage these issues.

When taking regulatory action, OVIC takes action that is proportionate to the issue or breach.

Transparent and accountable

Monitoring our performance

OVIC continuously monitors and evaluates its performance including the impact of its regulatory action on regulated bodies and the public. OVIC monitors and evaluates its performance to be accountable to OVIC's use of public money and legislated powers.

OVIC also uses its performance reporting to analyse systemic issues which, in turn, helps OVIC to apply its resources effectively in future regulatory activity. Using qualitative and quantitative data, OVIC develops and implements strategic business plans, while continually improving its approach and performance.

Communicating our regulatory activity

Where appropriate, OVIC publicly reports the outcome of its regulatory action on its website.[9] OVIC also publishes general statistics about its regulatory activity including in its Annual Reports.

OVIC publicly communicates its work in order to:

- Encourage adherence to the PDP Act and FOI Act by increasing awareness and knowledge of information rights and obligations.
- Promote public confidence in OVIC's regulatory activities and enhance community trust in the information handling practices of the Victorian public sector.
- Ensure OVIC's use of regulatory powers is transparent and consistent.

[9] Where a report contains adverse comment about a regulated body or person OVIC will first try to contact that individual or organisation before publication.

Active investigations

OVIC generally does not comment on active regulatory matters. However, if a particular matter receives public discussion or media reporting, OVIC may confirm that it is taking regulatory action without giving detail. OVIC aims for its public statements to be accurate, fair and balanced.

SCHEDULE 1 - PRIVACY REGULATORY ACTIVITIES

This schedule sets out how OVIC[10] takes regulatory action to ensure that regulated bodies understand and comply with the PDP Act including the Information Privacy Principles (**IPPs**).

OVIC prefers to work collaboratively with regulated bodies and any affected person to try to resolve issues before taking formal action through Compliance Notices or penalties. Nevertheless, where the risk associated with a privacy issue is high, or where a breach of the PDP Act is flagrant, OVIC may take formal action immediately.

Role of OVIC in regulating information privacy

OVIC has different roles and functions in relation to the regulation of information privacy:

- **Advice, education and guidance** — OVIC works with regulated bodies to encourage and support best practice. This includes providing guidance, general training and tailored advice.
- **Preliminary inquiries** — When responding to privacy concerns, OVIC usually starts with preliminary inquiries with the relevant regulated body to gather information and resolve issues promptly, to minimise the impact on affected individuals. In this stage, OVIC may make non-binding recommendations to improve practice or suggest actions to remediate a breach.
- **Examination and audit** — OVIC may examine the practices or audit the records of a regulated body to assess compliance with the IPPs. OVIC may conduct an examination or audit as a periodic assurance tool, to assess a potential privacy breach or to better understand an issue.
- **Investigations and Compliance Notices —** Where OVIC identifies serious, flagrant or repeated breaches of the IPPs, OVIC may investigate and issue a Compliance Notice. A Compliance Notice is a notice requiring the regulated body to take specified action within a specified time to remedy breaches and comply with IPPs and the PDP Act.
- **Penalties and prosecution** — Where a regulated body does not comply with a Compliance Notice, OVIC can prosecute and seek penalties from that regulated body.

Figure 1: Levels of Privacy Regulatory

[10] References to OVIC include the Information Commissioner, the Public Access Deputy Commissioner and the Privacy and Data Protection Deputy Commissioner, as appropriate. Some regulatory functions and powers are vested only in the Information Commissioner, or in the Information Commissioner and the relevant Deputy Commissioner.

Factors that we take into account

In deciding what regulatory action to take in response to an issue, OVIC considers the regulatory objectives of the PDP Act, the statutory purpose of the powers in the PDP Act and factors including:

- How serious the issue is based on:
  - the type of information involved, for example sensitive or delicate information;
  - the amount of information involved, and the number of people affected;
  - whether particularly vulnerable or disadvantaged groups are affected;
  - the extent of possible harm to people; and
  - community concern about the issue and the impact on public trust.
- Whether the issue arose from inadvertent, deliberate or reckless conduct.
- Whether the regulated body self-reported the incident to OVIC.
- Whether the issue is systemic, ongoing or isolated.
- How the regulated body has already addressed the issue, including steps taken to redress harm, improve practices and prevent recurrence.
- Whether regulatory action would have educational, deterrent or precedent value.
- Whether the regulated body was the subject of prior regulatory action and whether the current breach is related to prior regulatory action.

Advice, education and guidance

OVIC provides a range of advice, education and guidance to regulated bodies through:

- The OVIC website: https://ovic.vic.gov.au/
- Information sheets and other resources: https://ovic.vic.gov.au/privacy/for-agencies/
- IPP Guidelines: https://ovic.vic.gov.au/resource/guidelines-to-the-information-privacy-principles/
- A telephone enquiry line: 1300 006 842.
- An email enquiry address: enquiries@ovic.vic.gov.au
- Training and public forums: https://ovic.vic.gov.au/privacy/training-and-events/
- A blog: https://ovic.vic.gov.au/category/blog/
- Submissions to public consultations: https://ovic.vic.gov.au/privacy/submissions-and-reports/
- Reviewing Privacy Impact Assessments (**PIAs**) submitted by regulated bodies.
- Privacy Awareness Week annual activities
- Consulting with regulated bodies when they develop legislation and policy.

OVIC positively engages with regulated bodies to help them achieve privacy best practice and address privacy issues as they arise. OVIC also engages with regulated bodies to understand the issues they face which in turn highlights issues for OVIC to proactively target.

OVIC encourages regulated bodies to proactively engage with OVIC for advice, education and guidance. Engaging with OVIC early helps regulated bodies avoid formal regulatory action later.

Intervening in VCAT proceedings

OVIC can intervene in privacy proceedings at the Victorian Civil and Administrative Tribunal (**VCAT**) at any time.[11] When intervening, OVIC does not represent or advocate for any party. Rather, OVIC makes submissions to assist VCAT in interpreting the PDP Act.

In deciding whether to intervene, OVIC will consider:

- Whether there are **significant legal questions** that arise under the PDP Act. For example, if the case involves a new or unsettled area of law, or would it clarify a disputed interpretation of the PDP Act.
- Whether there are **broader privacy implications**. For example, where the privacy of third parties not in VCAT, or where a strategic function of OVIC is affected.
- The **impact to VCAT and the parties** to the proceeding. For example, whether OVIC's issue is central or peripheral to the proceeding, whether OVIC can help VCAT make a decision by making new or informed submissions, and whether the parties want OVIC to intervene.

Preliminary inquiries

OVIC identifies privacy issues in many ways including privacy complaints, reports from the public, press or social media reports, referrals from other regulators and when engaging with regulated bodies. When OVIC identifies an issue, it starts by making preliminary inquiries of the regulated body.

OVIC usually starts preliminary inquiries with a telephone call or email to the regulated body's nominated privacy officer. Depending on how serious the issue is and the risks involved, OVIC may also ask to be briefed by senior management in the regulated body. OVIC also asks for details of the regulated body's privacy policy and practices. OVIC expects regulated bodies to constructively assist and be transparent.

At the preliminary inquiry stage, OVIC tries to resolve privacy issues promptly and amicably. This reduces the adverse impact on individuals and avoids the need for OVIC to use compulsive powers.

During this stage, OVIC may offer non-binding recommendations to improve practice or suggest actions to remediate a breach. OVIC will subsequently check recommendations are implemented.

Preliminary inquiries also help OVIC to decide whether to take more formal regulatory action.

Audits and examinations

The PDP Act authorises OVIC to conduct examinations or audits.

- **Examinations** – In an examination, OVIC reviews the policies and procedures of a regulated body to ascertain if policies reflect all relevant requirements in IPPs and the PDP Act.
- **Audits** – In an audit, OVIC reviews records of personal information held by the regulated body to ascertain if records are maintained in accordance with IPPs and the PDP Act.

OVIC may use an examination or audit:

- To investigate a potential breach of the PDP Act brought to OVIC's attention.
- As a proactive, periodic assurance tool.
- To target a particular privacy issue. OVIC may conduct examinations or audits proactively as a

[11] Section 66AB of the *Victorian Civil and Administrative Tribunal Act 1998* (Vic).

periodic assurance activity, or to target a systematic privacy issue.

The examination or audit process in each matter depends on the privacy issue but may involve:

- Requests for documents, including copies of policies, procedures or privacy impact assessments;
- Requests for answers to specific questions; or
- Site visits including interviews of key personnel, and review of records and databases.

OVIC may publish a report of the examination or audit after it is concluded.

Investigations

The PDP Act authorises OVIC to serve a Compliance Notice on a regulated body.[12] Under the PDP Act, OVIC can investigate to decide if a Compliance Notice should be served.[13] OVIC can start an investigation on its initiative, or based on a complaint.[14]

OVIC can investigate to decide whether to serve a Compliance Notice. To serve a Compliance Notice, OVIC must be satisfied that:

The regulated body has breached an IPP, codes of practice or information usage arrangement.

AND

The breach is serious or flagrant, or similar breaches occurred at least 5 times in the last 2 years.

"Serious" and "flagrant" are distinct concepts. A contravention that is either serious or flagrant may result in OVIC issuing a Compliance Notice.

Is there a serious breach?

Whether a privacy breach is serious depends on a range of factors, including:

- The type of information involved, for example whether sensitive information is involved.
- The amount of information involved and the number of people that it relates to.
- Whether particularly vulnerable or disadvantaged groups are affected.
- The extent of harm to individuals and the likelihood of that harm eventuating.
- Whether the breach arose from inadvertent, deliberate or reckless conduct.
- The impact the breach has on public trust.
- Whether the issue is systemic, ongoing or isolated.

Is there a flagrant breach?

A flagrant privacy breach involves a conspicuous or obvious failure to comply with an IPP, applicable code of practice or an Information Usage Arrangement (IUA). Examples of flagrant breaches include:

- A regulated body knew it was failing to comply with an IPP because of past complaints, but continued to breach the IPP.
- A regulated body engaged in an act or practice substantially at odds with well-established standards or community expectations

[12] Section 78 of the PDP Act.
[13] Section 8(C)(2)(e) of the PDP Act.
[14] Section 78(5) of the PDP Act.

How OVIC investigates

OVIC's approach to an investigation depends on each case. OVIC usually starts investigations by contacting the regulated body and affected individuals to gather information.

OVIC expects regulated bodies to fully cooperate in any investigation. However, where necessary for an investigation, OVIC can compel a person to produce relevant documents at a specified time and place or compel a person to give evidence under oath.[15] It is an offence not to comply with a notice to produce or to attend.[16]

During an investigation, OVIC continues to work with regulated bodies to remedy the privacy breach and mitigate harm to individuals. This action may negate the need to serve a Compliance Notice.

After gathering sufficient information to form a preliminary view, OVIC will give a regulated body a reasonable opportunity to respond to potential adverse findings about that body. OVIC will take into account any response, before developing and issuing a final investigation report.

When an investigation is concluded, OVIC may report its findings. In the interests of transparency and of promoting compliance with the PDP Act, OVIC will publish completed investigation reports, unless there are compelling reasons not to.

After an investigation, OVIC will monitor, and liaise with, the regulated body to ensure recommended action is implemented.

Compliance Notices

A Compliance Notice can be served once OVIC is satisfied that a serious or flagrant breach occurred, or where similar breaches occurred at least 5 times over the last 2 years.

- A Compliance Notice requires the regulated body to take specified action within a specified time to remedy breaches and comply with IPPs and the PDP Act.[17]
- A regulated body that disagrees with a Compliance Notice can apply to VCAT for review.[18]
- A regulated body can ask OVIC to extend the specified time, if they apply before that time expires. OVIC may extend the specified time if satisfied it is not reasonably possible to take the specified action in the specified time.
- A Compliance Notice may be served on one or more regulated bodies, depending on the regulated body responsible for a breach and the action required by a Compliance Notice.
- It is an offence not to comply with a Compliance Notice.[19] The offence attracts a penalty of up to 600 penalty units for individuals and 3000 penalty units for other regulated bodies.[20]

Ordinarily, a Compliance Notice is served after an investigation to address outstanding actions, where breaches are not remedied during the investigation. Nevertheless, a Compliance Notice may be served immediately, or during an investigation, depending on risk factors including whether:

- The breach is serious based on the type or volume of the information affected, or the harm caused

[15] Section 79 of the PDP Act. See the Information Commissioner's *Policy and Procedure for Exercising Coercive and Other Powers* for further information on how the Information Commissioner exercises this and other coercive powers.
[16] Section 83H of the PDP Act.
[17] Section 78(1) and (2) of the PDP Act.
[18] Section 83 of the PDP Act.
[19] Section 82 of the PDP Act.
[20] The value of one penalty unit from 1 July 2018 to 30 June 2019 is $161.19.

by the breach.

- The breach was reckless or deliberate.
- The breach, or the harm from the breach, is ongoing.
- The regulated body has not cooperated with OVIC about the issue or was previously the subject of related regulatory action by OVIC.
- OVIC considers that follow up with the organisation is desirable.

After a Compliance Notice is served, OVIC will monitor the regulated body's progress in taking the action specified in the Compliance Notice in the specified time. Regulated bodies should keep OVIC informed about the action they take in response to the Compliance Notice. OVIC will continue to liaise with the organisation to ensure that steps are taken to comply with the PDP Act and IPPs.

Once OVIC is satisfied that the action specified in the Compliance Notice is complete, it will write to the regulated body to confirm the regulated body has satisfied the Compliance Notice.

OVIC may publish the issue of compliance notices and whether they have been satisfied on its website.

Prosecutable offences under the PDP Act

It is an offence to obstruct, hinder or resist OVIC officers when they perform their duties. It is also an offence to mislead or provide false information to OVIC.[21]

Ministerial Investigations

At the request of the Minister, OVIC must investigate and report to the Minister on any matter relating to information privacy under the PDP Act. On receipt of such a report, the Minster may table a copy of the report before each House of Parliament.[22]

[21] Sections 122 of the PDP Act.
[22] Section 111(1) of the PDP Act.

SCHEDULE 2 - FREEDOM OF INFORMATION REGULATORY ACTIVITIES

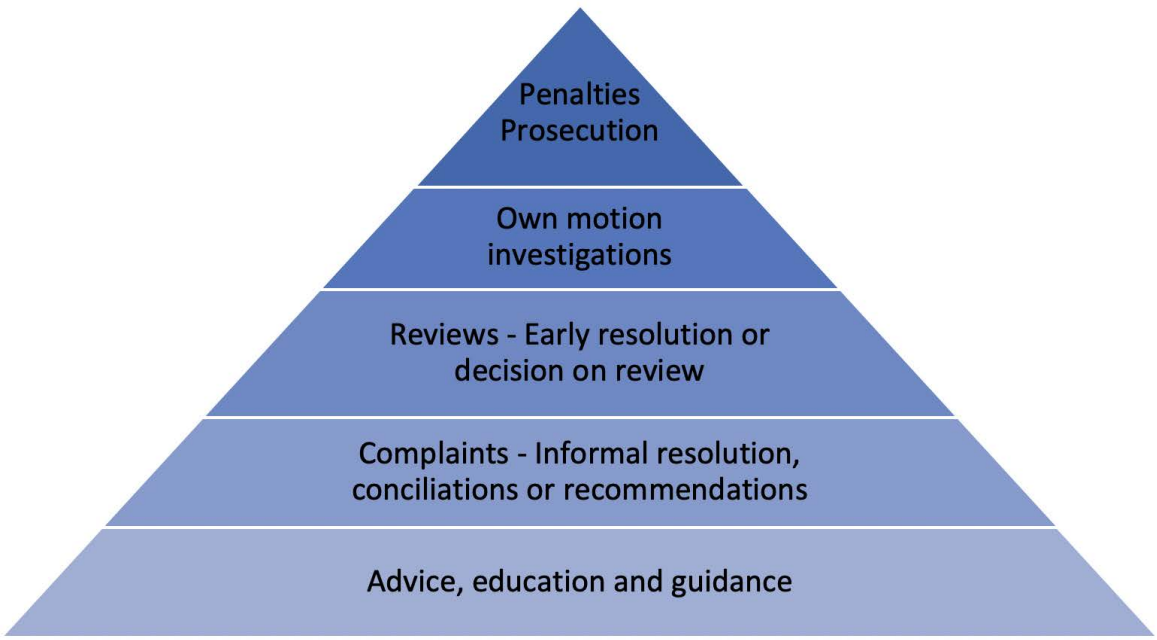
This schedule sets out how OVIC[23] takes regulatory action to ensure regulated bodies understand and comply with the FOI Act.

Role of OVIC in regulating freedom of information

OVIC has different roles in enforcing the FOI Act:

- **Advice, education and guidance** – OVIC helps regulated bodies comply with the FOI Act through advice, training and guidance delivered across different platforms. OVIC will also issue binding professional standards to give clear guidance to regulated bodies and the public.
- **Review of decisions** – To deliver timely and efficient outcomes, OVIC starts by trying to resolve reviews at an early stage by agreement, or through a conciliation where appropriate. If unable to do so, OVIC independently conducts a review of the regulated body's decision, asking both the applicant and regulated body for submissions. During reviews, OVIC has coercive powers, but prefers to work collaboratively with regulated bodies.
- **Complaints** – OVIC accepts and deals with complaints about whether or not a regulated body complied with the FOI Act. Where it can, OVIC resolves complaints informally. If unable to do so, OVIC may make formal recommendations to the regulated body how to improve its policies, procedures and systems to comply with the FOI Act.
- **Investigation** – OVIC can investigate how regulated bodies comply with the FOI Act and has coercive powers in conducting investigations.
- **Penalties and prosecution** – Where a regulated body does not comply with a notice to produce or to attend and give evidence, OVIC can prosecute and seek penalties from that regulated body.

Figure 2: Levels of Freedom of Information Regulatory Action



[23] References to OVIC include the Information Commissioner, the Public Access Deputy Commissioner and the Privacy and Data Protection Deputy Commissioner, as appropriate. Some regulatory functions and powers are vested only in the Information Commissioner, or in the Information Commissioner and the relevant Deputy Commissioner.

Advice, education and guidance

OVIC promotes the objects of the FOI Act by providing advice, education and guidance to regulated bodies and the public in the following ways:

- The OVIC website: https://ovic.vic.gov.au/
- Information sheets: https://ovic.vic.gov.au/freedom-of-information/guidance-and-resources/
- A telephone enquiry line: 1300 006 842
- An email enquiry address: enquiries@ovic.vic.gov.au
- Training and presentations: https://ovic.vic.gov.au/freedom-of-information/training-and-events/
- Stakeholder engagement: https://ovic.vic.gov.au/freedom-of-information/for-agencies/public-access-agency-reference-group/
- A blog: https://ovic.vic.gov.au/category/blog/
- Right to Know Day annual activities: https://ovic.vic.gov.au/rtk/

OVIC's advice, education and guidance aims to ensure that both regulated bodies and the public understand and accept the purpose of the FOI Act – to give a general right of access to information limited only by exceptions and exemptions in the FOI Act.

OVIC will also develop and issue Professional Standards under Part 1B of the FOI Act to ensure regulated bodies are accountable, meet their FOI obligations and carry out their functions in accordance with the FOI Act.

Reviews

A person has 28 days from receiving a regulated body's FOI decision to apply to OVIC in writing for review of that decision.[24] OVIC can review:

- Decisions to refuse, or defer, access to a document sought under an FOI request.
- Decisions not to waive or reduce an application fee.
- Decisions not to amend a document.

OVIC may refuse or dismiss a review application if satisfied that:

- The review is frivolous, vexatious, misconceived, lacks substance or is not made in good faith.
- The review applicant fails to cooperate with OVIC without reasonable excuse or OVIC is unable to contact the applicant after reasonable attempts.
- The review is more appropriately dealt with by VCAT.
- The review is not appropriate in the circumstances.
- The review applicant agrees to OVIC dismissing the review application.

Preliminary inquiries and early resolution

The FOI Act requires OVIC to conduct reviews in a timely, efficient and fair manner, with as little formality and technicality as possible. Consequently, OVIC starts its reviews with a preliminary inquiry to identify issues and try to resolve some, or all, disputed issues by:[25]

[24] Unless the Information Commissioner is satisfied that the delay was caused by an act or omission of the regulated body.
[25] Sections 49H and 49K of the FOI Act.

- **Releasing documents administratively outside of FOI** – Documents can sometimes be released by the regulated body administratively outside of the FOI Act to limit or resolve the FOI request.
- **Narrowing the scope of the review** – OVIC works with applicants to pinpoint the information they seek to narrow the scope of the FOI request and review that OVIC conducts.
- **Reducing the extent of exemptions** – OVIC shares its preliminary view about how exemptions apply to documents with regulated bodies and applicants to try to resolve a matter early.
- **Withdrawing a review** – An applicant may agree to withdraw the review at any time during a review. For example, the applicant accepts OVIC's preliminary view that the regulated body made the correct decision.
- **Negotiating an agreement** – OVIC can facilitate an agreement between the applicant and the regulated body, then make a review decision based on that agreement.[26]
- **A new decision by the regulated body** – If disputes about documents are reduced or a regulated body accepts OVIC's preliminary view, a regulated body can make a new decision on its own initiative or with the applicant's consent.[27]

Conciliation

If a review is not resolved or dismissed, OVIC will try to conciliate the complaint between the complainant and the regulated body. A successful conciliation will be recorded in a written agreement.

Formal reviews If a review is not resolved or dismissed, OVIC will review the regulated body's decision and the documents in the review including documents the regulated body exempted. OVIC will then independently decide whether more information should be released.[28] OVIC publishes its decisions in deidentified form to guide regulated bodies and the public about how OVIC applies the FOI Act.

OVIC expects regulated bodies to assist OVIC in its review,[29] but has powers to:

- Require the regulated body to make a further search for documents, including specifying the method for conducting that search.
- Compel the regulated body to produce relevant documents at a specified time and place.
- Compel a person to give evidence under oath.[30]
- Compel a regulated body to provide a reasonable sample of documents for OVIC to assess.[31]

Assisting in VCAT reviews

Where the Information Commissioner's decision is appealed to the Victorian Civil and Administrative Tribunal (**VCAT**), the Information Commissioner is not, and cannot, be a party to that proceeding. Nevertheless, VCAT may call on OVIC to assist VCAT either on its own motion or if OVIC applies. In deciding whether to apply to assist VCAT, OVIC considers:

- Whether there are **significant legal questions** that arise under the FOI Act. For example, if the case

[26] Section 49N of the FOI Act.
[27] Sections 49M and 49L of the FOI Act – A regulated body can make one fresh decision once on its own initiative but needs the applicant's consent afterward.
[28] Sections 49F and 49P of the FOI Act.
[29] Section 49I of the FOI Act.
[30] Sections 49KA and 49KB of the FOI Act.
[31] For 25A(1) and 25A(5) decisions pursuant to section 49KA(2)(b) of the FOI Act.

involves a new or unsettled area of law, or it would clarify a disputed interpretation of the FOI Act.

- Whether there are **broader implications for FOI policy and practice.** For example, where the information rights of third parties not in VCAT or a strategic function of OVIC is affected.
- The **impact to VCAT and the parties** to the proceeding. For example, whether OVIC's issue is central or peripheral to the proceeding, whether OVIC can help VCAT make its decision by making new or informed submissions, and whether the parties want OVIC to intervene.

Complaints

As well as applying for review, a person can also complain to OVIC about:

- A delay by a regulated body in handling a request.
- A decision by a regulated body that a document does not exist or cannot be located.
- A decision by a regulated body to release personal or business affairs information.
- Decisions by regulated bodies about publishing information about their functions.[32]

Complaints must be in writing, identify the decision-maker, set out the nature of the complaint and be made within 60 days of the action complained about.

OVIC may refuse or dismiss a complaint if satisfied that:

- The complaint does not relate to a decision under the FOI Act, or should be dealt with by another process under the FOI Act.
- The complaint is frivolous, vexatious, misconceived, lacks substance or is not made in good faith.
- It is more appropriate for another body to deal with the complaint.
- The complainant does not have sufficient interest in the complaint.
- The complainant fails to cooperate with OVIC without reasonable excuse or OVIC is unable to contact the applicant after reasonable attempts.
- The complaint is not appropriate in the circumstances.

Preliminary inquiries and informal resolution

On receiving a complaint, OVIC may consult with the complainant and the regulated body to identify issues, and try to resolve the complaint by agreement. OVIC must resolve complaints informally if possible, for example, the regulated body could apologise, acknowledge delay or explain its actions.[33]

Deciding a complaint

Where informal resolution and conciliation do not resolve a matter, OVIC will decide the complaint. OVIC must deal with the complaint in private, but will give the complainant and regulated body a chance to make a written submission, and respond to each other's submissions.

OVIC expects regulated bodies to assist OVIC in determining complaints, but has powers to:

- Require the regulated body to make a further search for documents, including specifying the method for conducting that search.

[32] The types of information captured is set out in Part II of the FOI Act.
[33] Sections 61G and 61GB of the FOI Act.

- Compel the regulated body to provide a reasonable sample of documents for OVIC to assess.
- Compel the regulated body to produce relevant documents at a specified time and place.
- Compel a person to give evidence under oath.

OVIC's complaint decision will be given in a written notice to the complainant and the regulated body.

OVIC can either decide to dismiss a complaint, or recommend that the regulated body make changes to their policies, procedures and systems to comply with the FOI Act. Where appropriate, OVIC will publish its recommendations.

Investigations

OVIC can investigate how a regulated body performs, fails to perform or purports to meet obligations under the FOI Act. OVIC can unilaterally decide to investigate a regulated body and does not require a complaint or report to prompt an investigation. Nevertheless, OVIC usually starts by trying to assist regulated bodies to resolve issues informally.

When OVIC will investigate

OVIC starts an investigation where it cannot resolve the issue informally, or if a formal regulatory response is needed for other reasons. In deciding whether to investigate, OVIC considers:

- The impact of the practice on the object of the FOI Act.
- Whether the practice is inadvertent, deliberate or reckless.
- Whether the practice indicates a systemic or ongoing issue, or appears to be isolated.
- Whether an investigation would have educational, deterrent or precedential value.
- Whether the practice is contrary to law or published guidance such as VCAT decisions, OVIC decisions or professional standards issued under the FOI Act.
- Whether the practice was previously subject to an OVIC review or complaint.
- Community concern about the practice, as indicated by public discussion or by direct contact to OVIC from community members or their representatives.

How OVIC investigates

OVIC's investigation approach depends on each case. OVIC usually starts investigations by contacting affected parties and the regulated body's principal officer to gather information.

OVIC expects regulated bodies to fully cooperate in any investigation. However, where necessary, OVIC can compel a regulated body or other person to produce relevant documents at a specified time and place, or compel a person to give evidence under oath. It is an offence:

- Not to comply with a notice to produce or to attend.
- To obstruct, hinder or resist OVIC officers when they perform their duties.
- To mislead or provide false information to OVIC.

After gathering sufficient information to form a preliminary view, OVIC will give the regulated body or person a reasonable opportunity to respond to potential adverse findings about them. OVIC will take into account any response, before developing and issuing a final investigation report.[34]

[34] See sections 61R(2), 61R(4) and 61Q of the FOI Act. The Commissioner must allow the person or regulated body to respond and must fairly set out each element of the response in the final investigation report.

When an investigation is concluded, OVIC reports its findings.[35] Although investigations are conducted in private,[36] OVIC may publish the investigation report by tabling it in Parliament.[37] In the interests of transparency and of promoting compliance with the FOI Act, OVIC will table completed investigation reports, unless there are compelling reasons not to.

After an investigation, OVIC will monitor, and liaise with, the regulated body to ensure recommended action is implemented.

[35] Section 61Q of the FOI ACt. Section 61R of the FOI Act sets out restrictions and required procedures about the content of investigation reports

[36] Section 61P(1) of the FOI Act.

[37] Section 61T of the FOI Act.

SCHEDULE 3 – INFORMATION SECURITY REGULATORY ACTIVITIES

This schedule sets out how OVIC[38] regulates regulated bodies captured by Part 4 and Part 5 of the PDP Act to ensure they protect the security of Victorian government information under the Victorian Protective Data Security Framework (**VPDSF**) and PDP Act.

OVIC prefers to work collaboratively with regulated bodies to resolve issues before taking formal action. Nevertheless, where the risk associated with an information security issue is high, OVIC may take formal action immediately.

Victorian Protective Data Security Framework, Standards and Assurance Model

OVIC developed the VPDSF to monitor and assure the security of Victorian government information. To support the VPDSF, OVIC issued protective data security standards (**Standards**) as high level mandatory requirements to help protect Victorian government information across five areas - governance, information security, personnel security, ICT security and physical security.[39]

The PDP Act required captured regulated body Heads to undertake a security risk profile assessment and a protective data security plan. The PDP Act also requires regulated body Heads to ensure the protective data security plan is reviewed every two years, or when there is a significant change in the regulated body's operating environment or security risks.[40]

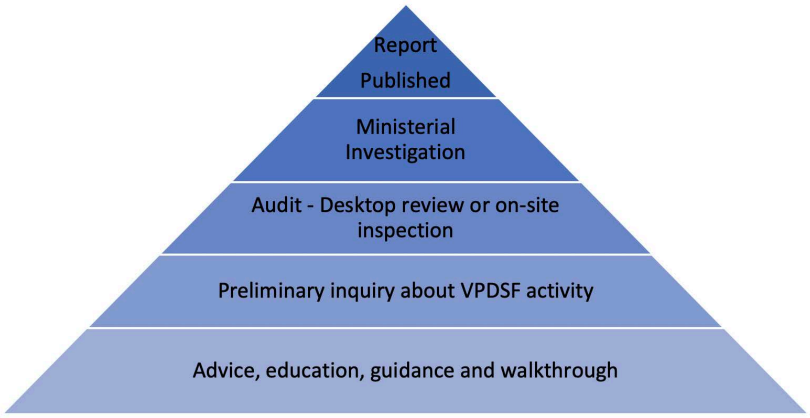
Role of OVIC in regulating information security

The PDP Act requires OVIC to promote, monitor and assure information security under the PDP Act by:

- **Guidance, training, advice or a walkthrough** – OVIC works with regulated bodies to develop policies and practices to protect Victorian government information. This includes providing guidance, general training, tailored advice or, walking through their policies and practices.
- **Preliminary inquiry about VPDSF activity** – Where OVIC identifies a theme or issue, including an information security breach or inadequate information security practice, OVIC may make inquiries about issues identified through the regulated body head.[41]
- **Audit** – Where OVIC identifies a potential breach of the VPDSF, OVIC may conduct an audit of the regulated body including either a desktop or onsite review of their policies and practices.[42] Audits can also be used as a periodic assurance tool, or to target a particular information security issue.
- **Report for Minister** – The responsible Minister can ask OVIC to investigate and report on matters relating to data security or law enforcement data security.[43]
- **Report published** – OVIC can, in the public interest, publish reports or recommendations dealing with information security. Where a report is prepared for the Minister, the Minister can also lay the report before each House of the Parliament.[44]

[38] References to OVIC include the Information Commissioner, the Public Access Deputy Commissioner and the Privacy and Data Protection Deputy Commissioner, as appropriate. Some regulatory functions and powers are vested only in the Information Commissioner, or in the Information Commissioner and the relevant Deputy Commissioner.
[39] Sections 85, 86 and 87 of the PDP Act.
[40] Section 89 of the PDP Act.
[41] Section 8D(2)(b) and section 110 of the PDP Act.
[42] Section 8D(2)(b) and section 110 of the PDP Act.
[43] Section 89 of the PDP Act.
[44] Section 111 of the PDP Act.

Figure 3: Levels of Information Security Regulatory Action



Factors that we take into account

In deciding what regulatory action to take in response to an issue, OVIC considers the regulatory objectives of the PDP Act, the statutory purpose of the powers in the PDP Act and factors including:

- How serious the issue is based on:
  - the type of information involved, for example sensitive or high value information;
  - the amount of information involved, and the nature and extent of likely harm including the effect on government, organisations or individuals;
  - the length of time that information is accessible when it should not be;
  - how it affects government service delivery including law enforcement.
- How the issue arose based on:
  - the identity of the recipients and instigator of an information security breach;
  - the security measures in place and the likelihood of circumvention;
  - whether the incident or conduct was inadvertent, deliberate or reckless;
  - whether the issue indicates a systemic or ongoing issue, or appears to be isolated.
- How the regulated body responded to the issue based on:
  - whether there was voluntary notification and how soon OVIC was notified after the issue was identified;
  - the types of remedial action already taken including steps taken to redress any possible harm and reduce the likelihood of recurrence;
  - the willingness of the organisation to improve its practices proactively without intervention by OVIC.
- Whether regulatory action would have educational, deterrent or precedential value.
- Whether the organisation was the subject of prior regulatory action and whether the current breach is related to prior regulatory action.
- Any other relevant factors.

Advice, Education, Guidance and Walkthroughs

OVIC works collaboratively with regulated bodies to help them maintain the confidentiality, integrity and availability of Victorian government information. Regulated bodies are encouraged to proactively engage with OVIC to seek advice, education and guidance. Engaging with OVIC early makes it less likely that the

regulated body attracts formal regulatory action later. It also allows OVIC to identify and help regulated bodies deal with emerging issues.

OVIC provides a range of advice, guidance, tools and other resources online including video guidance, FAQs, business impact level apps, templates and specific guidance about topics such as information security by contracted service providers.

- The OVIC website: https://ovic.vic.gov.au/
- Information guides/videos, interactive aids, templates and other resources: https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/
- A telephone enquiry line: 1300 006 842
- An email enquiry address: security@ovic.vic.gov.au
- Training: https://ovic.vic.gov.au/data-protection/training-and-events/
- Stakeholder engagement like the Victorian Information Security Network: https://ovic.vic.gov.au/data-protection/for-agencies/victorian-information-security-network/
- Submissions to public consultations: https://ovic.vic.gov.au/privacy/submissions-and-reports/

Walkthroughs

When asked by a regulated body, OVIC may walkthrough a regulated body's information security policies, governance arrangements and practices. A walkthrough will be arranged by appointment. In deciding whether or not to conduct a walkthrough, OVIC will consider the issues that the regulated body faces and information security resources that it has.

Preliminary inquiries

OVIC identifies information security issues in many ways including reviews of protective data security plans, voluntary incident reports, reports from the public, press or social media reports, referrals from other regulators and when engaging with regulated bodies.

When OVIC identifies an issue, it starts by making preliminary inquiries of the regulated body. The form of preliminary inquiries depends on each case based on the seriousness of the case and risks involved. However, preliminary inquiries generally start by email or telephone call to the regulated body's nominated security officer asking for information about their information security policies, governance arrangements and practices, or details of a particular incident. OVIC expects regulated bodies to constructively assist and be transparent.

OVIC promotes best practice and compliance with the VPDSF and PDP Act through an assurance model, working cooperatively with regulated bodies. Consequently, OVIC collaborates with regulated bodies at the preliminary inquiry stage to try to resolve information security issues at an early stage.

Early resolution reduces the adverse impact on individuals and avoids the need for OVIC to use compulsive powers. During this collaborative phase, OVIC may offer non-binding recommendations to improve practice or suggest actions to remediate a breach, then confirm if the recommendations were implemented. Preliminary inquiries also allow the Information Commissioner to decide whether to conduct more formal regulatory activity.

Audit

OVIC audits regulated bodies to ensure compliance with the VPDSF and PDP Act.[45] Audits can be used:

- To investigate a potential breach of the VPDSF or PDP Act brought to OVIC's attention.
- As a proactive, periodic assurance tool.
- To target a particular information security issue.

In an audit, OVIC reviews regulated body's information security policies, governance arrangements and practices. This may either occur as desktop review at OVIC, or onsite at the regulated body's premises. OVIC may also interview key personnel responsible for information security.

Ministerial investigations

At the request of the Minister, OVIC must investigate and report to the Minister on any matter relating to protective data security under the PDP Act. On receipt of such a report, the Minster may table a copy of the report before each House of Parliament.[46]

Publication of Reports or Recommendations

The PDP Act authorises OVIC to, in the public interest, publish reports or recommendations made relating to OVIC's functions under the Act. In considering whether publication is in the public interest, OVIC will take into account matters including:

- Whether the issues are of significant public concern.
- Whether the issues are already in the public domain.
- The educational value regarding the issue and the potential to encourage reform.
- The potential deterrent to other government regulated bodies in relation to the issue.
- Whether publication will demonstrate public accountability in OVIC's regulatory action.
- Any negative impact on public security, personal privacy, the welfare of impacted individuals or the right of any person to a fair trial.

OVIC's powers

When OVIC conducts any information security monitoring or assurance activities, the regulated body is obliged to assist OVIC. OVIC also has power to require free and full access at all reasonable times to a government body's data or data system and to take copies of that data.[47] It is an offence to obstruct, hinder or resist OVIC officers when they perform their duties. It is also an offence to mislead or provide false information to OVIC.[48] Information obtained can be referred to responsible agencies for urgent investigation or attention.[49]

---

[45] Section 8D(2)(b) and section 110 of the PDP Act.

[46] Sections 111(1) and 8D(1)(d) of the PDP Act.

[47] Sections 106, 109 and 110 of the PDP Act.

[48] Section 122 of the PDP Act.

[49] Section 112 of the PDP Act allows referral to IBAC, the Victorian Inspectorate, the Victorian Ombudsman Victoria, the Chief Commissioner for Police, the Director of Public Prosecutions or any other prescribed person or body. When referring under this section, OVIC must advise the Premier, the responsible Minister for the affected government body. Section 113 of the PDP Act also allows referral to IBAC notifying where OVIC only needs to also notify only the head of the affected government body of the referral.

Feedback

OVIC's Regulatory Action Policy will continue to be reviewed and updated in response to feedback or any significant changes to legislation, government policy or our regulatory practice. We welcome feedback about OVIC's Regulatory Action Performance or the performance of OVIC.

Version Information

Version	Date	Details
1.0	__/__/____	Initial Release

Authorised by the Victorian Information Commissioner

PO Box 24274 Melbourne, Victoria, 3001 Australia

Tel: 1300 006 842

Email: enquiries@ovic.vic.gov.au

Website: ovic.vic.gov.au