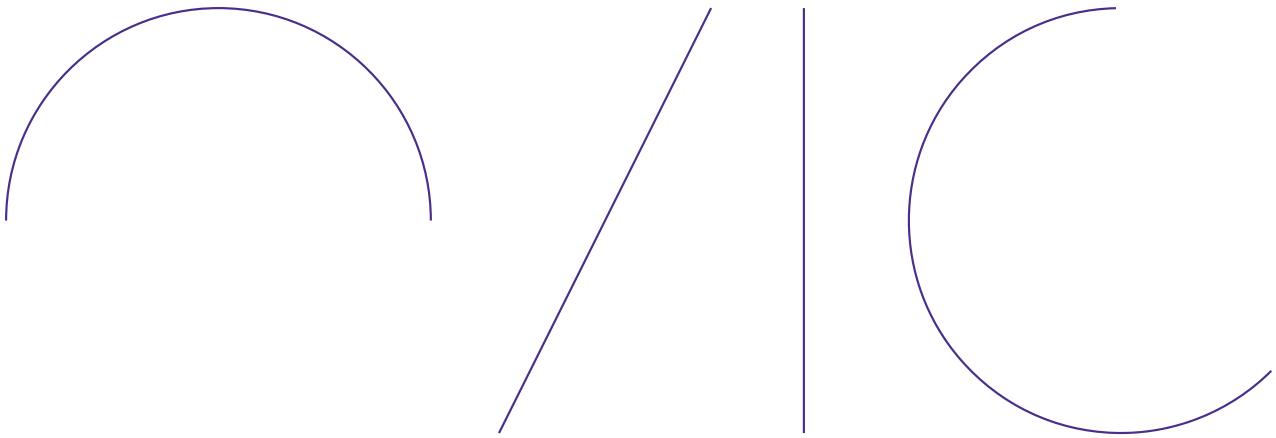
OVIC
Office of the Victorian
Information Commissioner

Regulatory Action Policy 2022-25



Version	Author	Date	Additions/changes
1.0	Office of the Victorian Information Commissioner	2019/05/27	Initial Release
2.0	Office of the Victorian Information Commissioner	2022/10/12	Updated Release

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 Policy or the performance of OVIC.

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

Disclaimer

The information in this document is general in nature and does not constitute legal advice.

Copyright

Table of Contents

Commissioner's Foreword

The Office of the Victorian Information Commissioner (**OVIC**) was established in 2017 to ensure the information rights of Victorians are upheld.

Since then, OVIC has used its regulatory powers under the *Freedom of Information Act 1982* (Vic) (**FOI Act**) and the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) to promote, assure and enforce those rights.

It has been three years since I published the first iteration of our Regulatory Action Policy detailing how OVIC will use its regulatory powers.

Since then, we have seen technological developments that have had implications across the freedom of information, privacy, and information security landscapes.

We also experienced the COVID-19 pandemic which had significant impacts on the operations of the Victorian public sector. Government collected more personal information than ever before, which led to more members of the public rightly being interested and concerned about their privacy and the protection of their data.

The pandemic also tested the resilience of the FOI system in Victoria. As noted in reports by my office, the public's right to access government information suffered during this time.

Since 2019, my office has undertaken a range of regulatory action including conducting preliminary inquiries, audits, examinations, and investigations, and issuing compliance notices. We published reports detailing our regulatory action to improve understanding of obligations under the FOI Act and PDP Act. We established regulatory priorities that reflect existing and emerging issues affecting the information rights of Victorians to guide our regulatory action.

OVIC has a renewed focus on engaging directly with members of the public. This Policy is an important tool in helping citizens to better understand their information rights and how they will be enforced under the FOI Act and the PDP Act.

This updated Regulatory Action policy reflects OVIC's increasing maturity as a regulator and provides agencies and the public with important information about how OVIC undertakes regulatory action.

We aim to build public trust by committing to Victorians that strong action will be taken to ensure their information rights are respected and upheld by government.

Sven Bluemmel
Victorian Information Commissioner

October 2022

About this policy

This policy describes the Office of the Victorian Information Commissioner's (**OVIC**) regulatory approach. In this policy, 'regulatory action' means OVIC[1] 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; and

- The second part consists of three schedules related to 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 exercising them.

[1] Reference to OVIC includes the Information Commissioner, the Public Access Deputy Commissioner and the Privacy and Data Protections 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.

PART 1 - OVIC's approach to regulatory action

What does OVIC do?

OVIC is an independent regulator that protects and upholds the information rights of Victorians. OVIC is headed by the Victorian Information Commissioner, who is supported by the Public Access Deputy Commissioner and the Privacy and Data Protection Deputy Commissioner, along with OVIC staff.

OVIC is the primary regulator and source of independent guidance to the community and Victorian government about how the public sector collects, uses and discloses information. OVIC's legislative functions and powers are set out in the FOI and PDP Acts.

What OVIC regulates

As an independent regulator, OVIC has three functional areas: privacy and information security, which relate to the PDP Act, and freedom of information, which relates to the FOI Act.

The key functions of these areas are:

Privacy

- Promote awareness and understanding of the Information Privacy Principles (**IPPs**);
- Handle complaints and conciliate disputes about possible breaches of the IPPs by the Victorian public sector;
- Examine the practices of regulated bodies regarding personal information they hold and the IPPs;
- Conduct audits to assess compliance with the IPPs;
- Provide guidance to regulated bodies and the public about the PDP Act and the IPPs;
- Undertake research, issue reports, guidelines and other materials with regard to information privacy.; and
- Investigate alleged breaches of the IPPs and the PDP Act by regulated bodies.

Freedom of information

- Promote understanding and acceptance by agencies and the public of the FOI Act and its object;
- Conduct reviews of decisions made by agencies and Ministers under the FOI Act;

- Handle complaints about an action taken, or failed to be taken, by an agency or Minister when performing their functions or meeting obligations under the FOI Act;
- Provide education, and guidance to agencies and the public in relation to OVIC's functions;
- Monitor compliance with the Professional Standards;
- Provide education and guidance to agencies and the public in relation to compliance with the Professional Standards;
- Investigate how a regulated body performed, or failed to perform, its FOI functions and obligations under the FOI Act and the Professional Standards; and
- Investigate public interest complaints related to the Information Commissioner's functions referred to OVIC by the Independent Broad-based Anti-corruption Commission (**IBAC**).

Information security

- Promote continuous improvement through guidance about information security;
- Monitor and promote compliance with the Victorian Protective Data Security Framework (**VPDSF**) and the PDP Act by review of protective data security plans (**PDSPs**) and audits;
- Conduct monitoring and assurance activities to assess compliance with the Victorian Protective Data Security Standards (**VPDSS**); and
- Undertake research, issuing reports, guidelines and other materials with regard to information security.

The Information Commissioner's functions and powers extend to all of these matters, while the Public Access Deputy Commissioner is responsible specifically for FOI matters and the Privacy and Data Protection Deputy Commissioner for information privacy and information security matters.

The Information Commissioner can also delegate functions and powers to the Deputy Commissioners and OVIC staff. OVIC may use information gathered during reviews, complaints and other sources in conducting regulatory action.

Who OVIC regulates

OVIC's jurisdiction relates to public sector bodies, organisations or agencies as defined 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 include departments, councils, Victoria Police, public entities,[2] courts and tribunals;[3]

- **Freedom of information** – 'agencies' defined in section 5 of the FOI Act and include departments, councils and prescribed authorities such as TAFES, public hospitals and public schools; and

- **Information security** – 'public sector bodies'[4] include departments, public entities, and Victoria Police.[5] Councils[6], universities, ambulance services, public hospitals, public health services and multipurpose services under the *Health Services Act 1988* (Vic) are excluded from the definition of 'public sector body'.

Aims of regulatory action

OVIC has a range of functions and powers supporting its regulatory action. These include powers that allow OVIC to engage and work with regulated bodies to facilitate compliance and best practice, as well as investigation and enforcement powers directed to redress any regulated body's failure to perform their functions and obligations or breaches of relevant laws and standards.

The Information Commissioner, the Public Access Deputy Commissioner and the Privacy and Data Protection Deputy Commissioner use the powers conferred on them under 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;

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

[3] 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.

[4] As defined by section 84 of the PDP Act and section 5 of the *Public Administration Act 2004*.

[5] Other bodies are Victorian Civil and Administrative Tribunal, Independent Broad-based Anti-corruption Commission, Victorian Auditor-General's Office, Victorian Electoral Commission, 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.

[6] Councils may have obligations under the PDP Act if they are appointed as a Committee of Management under the *Crown Land Reserves Act 1978* (Vic) or if they are a trustee of a cemetery trust under the *Cemeteries and Crematoria Act 2003* (Vic) (note that the reporting entity is the Committee of Management or the Trust as the case may be).

- **Foster public trust and awareness** of the Victorian public sector's responsibility, ability and commitment to handling information in a responsible and accountable manner;
- **Influence government to consider information rights** in developing new policies or programs; and
- **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;
- **Effective and targeted** – OVIC uses its powers to protect the Victorian community from harm caused by infringements of their information rights and responds to possible contraventions of the PDP Act and FOI Act based on their likelihood and severity. OVIC's regulatory action leads to changed behaviour on the part of regulated bodies;
- **Proportional** – OVIC takes action that is proportionate to the issue being addressed. The scale of OVIC's regulatory response is based on the risk of harm the issue creates for the community or for individuals and whether the issue is systemic; and
- **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.

How does OVIC undertake regulatory action?

OVIC takes a risk-based approach in deciding when and how to take regulatory action. OVIC is not able to take regulatory action in all matters that are brought to its attention. As such, 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. These factors are outlined in further detail below.

Types of regulatory action

- **Education and guidance** —Under both the PDP and FOI Acts, OVIC works with regulated bodies to encourage and support best practice. This includes providing tailored guidance and general training;
- **Preliminary inquiries** — Under both the PDP and FOI Acts, OVIC conducts preliminary inquiries with regulated bodies to gather information and resolve issues promptly, or to decide whether to take further regulatory action;

- **Examination and audit** — Under the PDP Act, OVIC may examine the practices or audit the records of a regulated body to assess compliance with the IPPs or compliance to the VPDSS;

- **Investigations** — Under the FOI Act, OVIC can undertake an own motion investigation. Under the PDP Act, OVIC may conduct an investigation for the purpose of issuing a compliance notice in response to serious, flagrant or repeated breaches of the IPPs; and

- **Penalties and prosecution** — Where a regulated body does not comply with a compliance notice or a notice to produce or attend, OVIC can prosecute the regulated body for committing an offence.

Responding to issues, allegations, and referrals

OVIC may become aware of issues or allegations of non-compliance with the FOI and PDP Acts and the Professional Standards in a number of ways, including:

- complaints, FOI reviews, or enquiries from members of the public;

- complaints or enquiries from members of Parliament;

- information provided by an informant;

- open-source publicly available information (e.g. media, website monitoring);

- internal referrals from OVIC's business units;

- Information Security Incident Notification Scheme (**ISINS**) under the provisions of the VPDSS or OVIC's voluntary privacy breach notification scheme;

- referrals from integrity and oversight agencies, regulatory agencies, law enforcement, or parliamentary committees; and

- Public Interest Complaint (**PIC**) referrals from IBAC.

OVIC is not authorised to investigate Public Interest Disclosures (**PIDs**). These complaints are referred to IBAC.

OVIC has limited resources and is not able to respond to every referral or issue it becomes aware of. In deciding how to respond to any particular issue or referral, OVIC is guided by the principles and factors described below.

Factors OVIC considers in deciding on a regulatory response

The key considerations when deciding whether to respond to an allegation are the likelihood that the allegation is accurate, the seriousness of the alleged conduct and the value of the public sector information.

OVIC also considers factors including the following:

- The seriousness of the issue based on:
  - the number of people affected;
  - the people affected, for example, whether particularly vulnerable or disadvantaged groups are affected;
  - the extent of possible harm to people;
  - community concern about the issue and the impact on public trust; and
  - the sensitivity/value of public sector information that was compromised (affecting its confidentiality, integrity, or availability).
- Actions taken by the regulated body in relation to the issue including:
  - whether the issue arose from inadvertent, reckless or deliberate conduct;
  - whether the regulated body self-reported the incident to OVIC;
  - whether the issue is systemic, ongoing or isolated; and
  - how the regulated body has addressed or proposes to address the issue, including steps taken to redress harm, improve practices and prevent recurrence.
- Actions taken or planned by OVIC such as:
  - whether the regulated body was the subject of prior regulatory action and whether the current breach is related to prior regulatory action;
  - whether the practice was previously subject to an OVIC review or complaint;
  - whether regulatory action would have educational, deterrent or precedent value;
  - whether the issue relates to one of OVIC's regulatory priorities; and
  - the resource implications for OVIC on taking regulatory action, including impacts on ongoing and planned regulatory matters.
- Broader implications including:
  - the impact of the practice on the objects of the FOI or PDP Acts; and
  - whether the practice is contrary to law or published guidance such as Victorian Civil and Administrative Tribunal (VCAT) decisions, OVIC decisions or Professional Standards issued under the FOI Act.

Compulsive powers

OVIC has powers under both the PDP and FOI Acts that can require action by a regulated body or individual. These include powers to issue notices to produce and/or attend. A notice may require a person to appear before the Information Commissioner to provide information as a witness or to provide documentation. It is an offence under the FOI Act and the PDP Act for a person to refuse or fail to comply with a notice without reasonable excuse.

Communication of regulatory action

When an issue is identified, OVIC usually seeks a response from the affected regulated body before deciding whether to take regulatory action. Where appropriate, OVIC usually seeks to resolve issues by agreement before resorting to formal regulatory action, as this is usually a more efficient use of OVIC's limited resources.

Regulatory priorities

OVIC publishes regulatory priorities to inform the community and regulated agencies of its areas of focus. These priorities are published in the annual report and on the website.

Working with other regulators

OVIC is part of a broader integrity framework and works with other regulators to limit duplication of investigations. OVIC works with other regulators formally through referral provisions, and informally through research and education.

Regulators that OVIC works with include:

- Independent Broad-based Anti-corruption Commission;
- Victorian Ombudsman;
- Health Complaints Commissioner;
- Mental Health Complaints Commissioner;
- Disability Services Commissioner;
- Commission for Children and Young People;
- Victorian Auditor General's Office; and
- Office of the Australian Information Commissioner.

Active investigations

OVIC generally does not comment on active regulatory matters. However, if a particular matter is subject to significant public discussion or concern, OVIC may confirm that it is taking regulatory action. OVIC aims for its public statements to be accurate, fair and balanced.

Communicating at the start of regulatory action

In some circumstances, OVIC may announce the start of an investigation or other regulatory action by publishing a statement on its website. This will usually only happen in circumstances where the topic has been of significant public discussion, or where OVIC requires the assistance of the public in the conduct of the regulatory action.

Publishing the results of regulatory action

Unless there is good reason not to, OVIC publicly communicates the outcome of its work to:

- encourage adherence to the PDP Act and FOI Act by increasing awareness and understanding 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; and
- ensure OVIC's use of regulatory powers is transparent and consistent.

The Information Commissioner is empowered to publish reports of regulatory action under both the PDP and FOI Acts. How regulatory action will be made public will depend on the type of regulatory action undertaken and the legislation (FOI Act or the PDP Act) that applies.

Under the FOI Act a report of investigation may be tabled in Parliament.[7]

The PDP Act authorises OVIC to publish a report or recommendations made in relation to its functions when doing so would be in the public interest. [8] It is ordinarily in the public interest to publish reports of regulatory action, so in most cases this will occur, unless there is a compelling reason not to.

When deciding whether publication is in the public interest, OVIC will consider:

- 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; and

[7] Section 61T(1), *Freedom of Information Act 1982* (Vic).

[8] Section 111(3), *Privacy and Data Protection Act 2014* (Vic).

- any negative impact on public security, personal privacy, the welfare of impacted individuals or the right of any person to a fair trial.

In most cases, public reporting on formal regulatory action (investigations, audits, and examinations) achieves one or more of these objectives. Therefore, OVIC usually publishes a report at the conclusion of these categories of regulatory action.

However, a report may not be published, or publication may be deferred, if publishing the report will cause harm to particular individuals or groups – for example, if publishing a report may compromise criminal proceedings.

Progress reporting following the conclusion of regulatory activity

Once regulatory action is finalised, OVIC will engage with the regulated body to discuss any proposed findings, recommendations or specified actions.

Once a matter has been finalised, OVIC may seek regular updates from regulated bodies about progress to meeting the recommendations or specified actions. The ongoing reporting requirements will be determined on a case-by-case basis.

Monitoring our performance

OVIC monitors and evaluates its performance including the impact of its regulatory action on regulated bodies and the public. OVIC monitors the impact of its regulatory action by monitoring the implementation of our recommendations made to agencies. OVIC reports on its functions to Parliament through its annual report and also reports to the Integrity and Oversight Committee.

PART 2 – Functional areas approach to regulatory action

SCHEDULE 1 - Privacy regulatory activities

This schedule sets out how OVIC takes regulatory action to ensure that regulated bodies understand and comply with the PDP Act including the IPPs.

Where it is practicable and appropriate, OVIC seeks to work collaboratively with regulated bodies and any affected person to try to resolve issues before taking formal action through investigations, compliance notices or penalties.

OVIC may take formal action where the risk associated with a privacy issue is high, or where a breach of the PDP Act is flagrant, systemic or has other aggravating factors.

OVIC's role in regulating information privacy

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

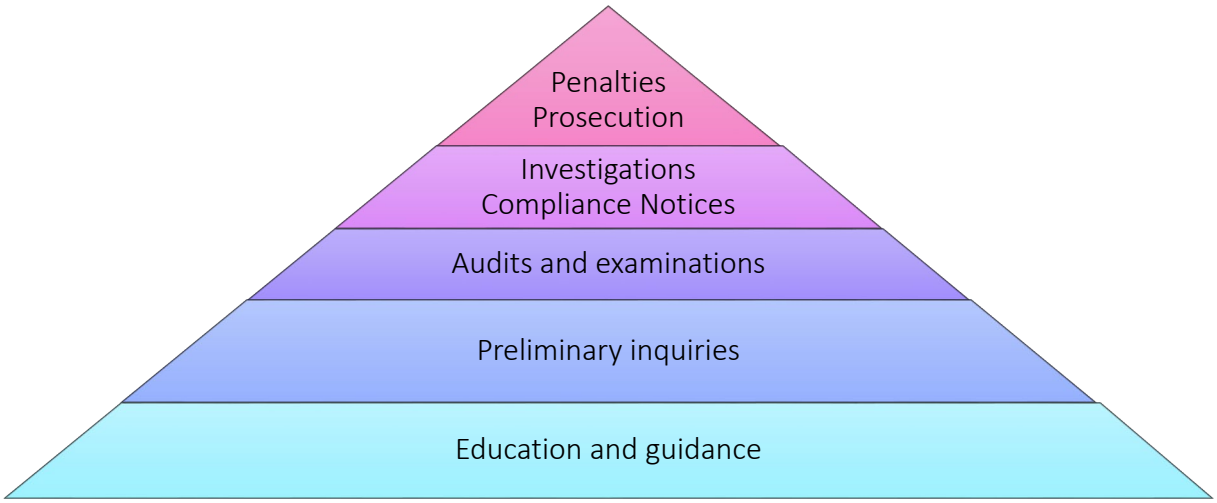


Figure 1 – Levels of privacy regulatory action

Education and guidance

OVIC publishes and provides a range of education and guidance to regulated bodies on its website.

OVIC 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 and assist them to comply with their obligations. This can also highlight issues for OVIC to proactively target.

OVIC encourages regulated bodies to proactively engage with OVIC for education and guidance as it can help regulated bodies avoid formal regulatory action later.

Preliminary inquiries

When OVIC identifies an issue that may involve a contravention of the IPPs warranting regulatory action, it starts by making preliminary inquiries of the regulated body, to better understand the issue in question.

This usually involves a telephone call or email to the regulated body's nominated privacy officer. Depending on the seriousness of the issue and the risks involved, OVIC may also ask to be briefed by senior management in the regulated body. OVIC expects regulated bodies to constructively assist and be transparent.

Where OVIC commences preliminary inquiries, it will attempt to resolve privacy issues promptly without progressing to more formal regulatory action, where appropriate. This may involve offering non-binding suggestions to improve practice or propose actions to remediate a contravention of the IPPs.

However, OVIC's preliminary inquiries may lead to a decision that more formal regulatory action – like an investigation, audit or examination – is required, taking into account the factors listed above.

Audits and examinations

The PDP Act authorises OVIC to conduct examinations[9] or audits:[10]

- Examinations – OVIC examines the practices of a regulated body to determine whether the regulated body manages personal information in accordance with the IPPs and the PDP Act; and
- Audits –OVIC reviews records of personal information held by the regulated body to ascertain if records are maintained in accordance with the 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;

[9] Section 8C(2)(b) of the PDP Act.

[10] Section 8C(2)(f) of the PDP Act.

- as a proactive, periodic assurance tool; or
- to target a particular 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; and
- site visits including interviews of key personnel, and review of records and databases.

At the conclusion of an examination or audit, OVIC may publish a report of its findings and recommendations to improve privacy practices.

Investigations

The PDP Act authorises OVIC to serve a compliance notice on a regulated body.[11] Under the PDP Act, OVIC can investigate a regulated body to decide if a compliance notice should be served.[12] OVIC can start an investigation on its own initiative or based on a complaint.[13]

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, code 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:

[11] Section 78 of the PDP Act.

[12] Section 8C(2)(e) of the PDP Act.

[13] Section 78(5) of the PDP Act.

- The type of information involved, for example whether sensitive or delicate 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, reckless or deliberate conduct;
- The impact the breach has on public trust; and/or
- 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.

Examples of flagrant breaches include:

- A regulated body knew it was failing to comply with an IPP because of past complaints, but failed to take appropriate action to prevent further breaches of the IPP; and/or
- A regulated body engaged in an act or practice substantially at odds with well-established standards or community expectations.

Is there a repeated breach?

Consistent with the terms of the PDP Act, OVIC will consider a contravention of the IPPs as a repeated breach where the same or similar breaches have occurred at least five times in the last two years.

How OVIC investigates

OVIC's approach to an investigation depends on each case. OVIC usually starts investigations by contacting the regulated body to notify it of the investigation. OVIC may also contact any individuals affected by a potential breach of the IPPs or other relevant persons 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 or affirmation.[14] It is an offence not to comply with a notice to produce or to attend without a reasonable excuse.[15]

During an investigation, OVIC continues to work with regulated bodies to remedy any privacy breaches 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 potentially adverse findings about that body. OVIC will take into account any response before finalising and issuing an 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 liaise with the regulated body to monitor the implementation of any recommendations made.

Compliance notices

Where OVIC is satisfied that a regulated body has committed a serious, flagrant or repeated breach, it may serve a compliance notice.

A compliance notice requires the regulated body to take specified action within a specified time to remedy breaches and comply with the IPPs and the PDP Act.[16] A compliance notice may be served on one or more regulated bodies, depending on the regulated bodies responsible for a breach and the remediation action required.

A regulated body that disagrees with a compliance notice can apply to VCAT for review.[17]A regulated body can also ask OVIC to extend the specified time to comply with the compliance notice if it applies 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.

It is an offence not to comply with a compliance notice.[18] The offence attracts a penalty of up to 600 penalty units for individuals and 3000 penalty units for other regulated bodies.[19]

---

[14] Section 79 of the PDP Act.

[15] Section 83H of the PDP Act.

[16] Section 78(1) and (2) of the PDP Act.

[17] Section 83 of the PDP Act.

[18] Section 82 of the PDP Act.

[19] Penalty unit value available at https://www.dtf.vic.gov.au/financial-management-government/indexation-fees-and-penalties.

Ordinarily, a compliance notice is served after an investigation where OVIC is not satisfied that breaches have been remedied or that the regulated body has adopted practices that comply with the IPPs 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;[20]
- 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; and
- OVIC considers that follow up with the regulated body 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 regulated body 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 it 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:

- not comply with a compliance notice;
- fail to comply with a notice to produce or attend without reasonable excuse;
- mislead or attempt to mislead OVIC; and

[20] See section '*Factors OVIC considers when deciding on a regulatory response*' for relevant factors relating to the seriousness of an issue/breach.

- to provide information or make a statement to OVIC knowing that it is false or misleading in a material particular.[21]

These are summary offences which carry penalties, and which OVIC can prosecute in the Magistrates' Court. OVIC will only take this action in the most serious cases.

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 Minister 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 takes regulatory action to ensure regulated bodies understand and comply with the FOI Act.

Where it is practicable and appropriate, OVIC seeks to work collaboratively with regulated bodies and any affected person to try to resolve issues before taking formal action through investigations or penalties.

OVIC may take formal action where the risk associated with an FOI issue is high, or where a breach is serious or has other aggravating factors.

Role of OVIC in regulating freedom of information

OVIC has different roles in enforcing the FOI Act.

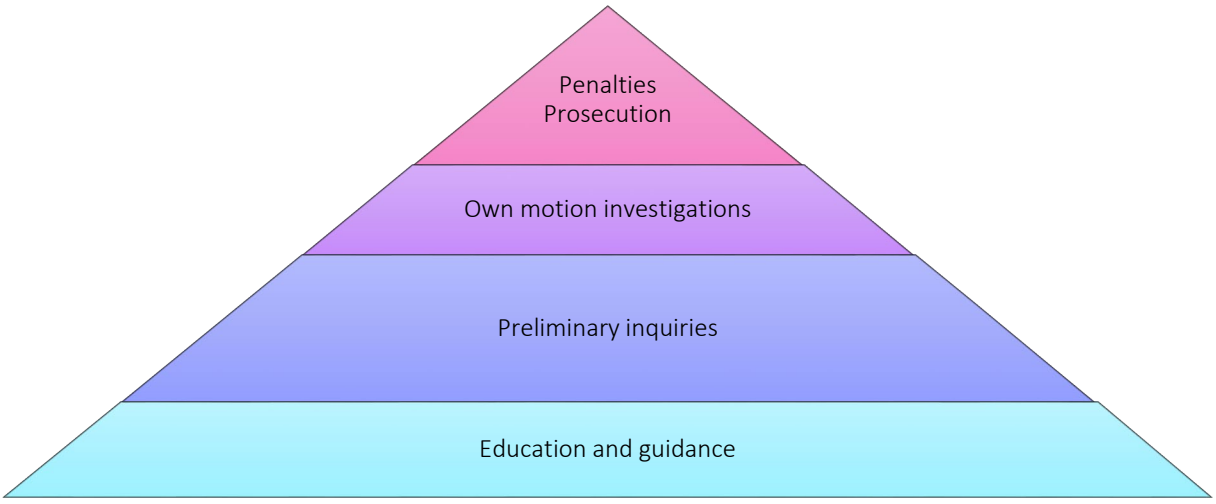


Figure 2 Levels of freedom of information regulatory action

Education and guidance

OVIC promotes the objects of the FOI Act by providing education and guidance to regulated bodies and the public. Educational and supporting materials can be found on OVIC's website.

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

The Professional Standards, issued under Part 1B of the FOI Act, aim to ensure regulated bodies are accountable, meet their FOI obligations and carry out their functions in accordance with the FOI Act.

Preliminary inquiries

OVIC's Public Access Branch generally commences preliminary inquiries in relation to new reviews, complaints and Professional Standards engagements.

Reviews

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 informally resolve some, or all, disputed issues by:[23]

- Releasing documents administratively outside of FOI[24] – Where appropriate, OVIC encourages the regulated body to administratively release documents outside of the FOI Act to limit or resolve the FOI request;
- Narrowing the scope of the review – OVIC works with applicants to determine the key information they seek and where possible, seeks to narrow the scope of the review that OVIC conducts;
- Reducing the extent of exemptions – Where appropriate, OVIC provides preliminary views on the likely outcome of a review application and how exemptions apply to documents to regulated bodies and applicants to try to informally resolve a matter;
- Withdrawing a review – An applicant may agree to withdraw the review at any time during a review. For example, where an applicant accepts OVIC's preliminary view that the regulated body made the correct decision, they may agree to withdraw their application for a review;

[23] Sections 49H and 49K of the FOI Act.

[24] For further information regarding proactive and informal release see the following links: https://ovic.vic.gov.au/freedom-of-information/resources-for-agencies/practice-notes/proactive-release-of-information/; https://ovic.vic.gov.au/freedom-of-information/resources-for-agencies/practice-notes/informal-release-of-information/.

- **Negotiating an agreement** – OVIC can facilitate an agreement between the applicant and the regulated body, then make a review decision based on that agreement;[25] and

- **A new decision by the regulated body** – A regulated body can make a new decision on its own initiative or with the applicant's consent at any stage during a review.[26] This may occur where the regulated body accepts OVIC's preliminary view about the likely outcome of the review, or where the regulated body may have located additional documents relevant to an applicant's FOI request terms following OVIC inquiries on the adequacy of its original search.

Complaints

When receiving a complaint, OVIC may undertake preliminary inquiries to determine the material facts in dispute and to obtain further details about the grounds of complaint.[27]

OVIC aims to resolve complaints informally and by agreement. This involves consulting with the complainant and the regulated body. Where a complaint is unable to be resolved informally, OVIC may conciliate the complaint or dismiss a complaint where it is considered to have been pursued to its fullest extent.

Professional Standards engagements

In accordance with the Professional Standards Framework[28], OVIC assesses each review and complaint application it accepts for any Professional Standards engagements.

Where a potential or actual instance of non-compliance is identified, it is recorded in OVIC's case management system.

In some instances, non-compliance will be apparent based on the information OVIC already has, and further inquiries will not be required to confirm if a breach has occurred.

Where OVIC needs more information about the Professional Standards engagement, OVIC staff will make preliminary inquiries with the regulated body and/or an applicant/complainant about potential non-compliance with the Professional Standards.

Where non-compliance is established, OVIC will consider the nature and extent of the breach, and determine what action, if any, to take. This may involve educational and informal action or formal action.

---

[25] Section 49N of the FOI Act.

[26] 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.

[27] Sections 61G and 61GB of the FOI Act.

[28] See https://ovic.vic.gov.au/freedom-of-information/resources-for-agencies/professional-standards/the-foi-professional-standards-framework/.

OVIC's approach will depend on the nature and seriousness of the conduct, the impact of the non-compliance, and the circumstances of each case. OVIC adopts a graduated approach to compliance and enforcement. This means that, generally, the more serious the breach, the more interventionist the response.

OVIC classifies Professional Standards breaches into two categories:

- Minor or technical breaches - where an agency's action or inaction results in a minimal risk of detriment to members of the public or OVIC (such as a minor delay in providing information where an agency must provide it in a specified period of time); and
- Substantial, persistent or systemic breaches - where an agency's action or inaction result in a moderate to high risk of detriment to members of the public or OVIC (such as significant and ongoing delays, repeated and persistent breaches, or the identification of wider systemic concerns).

OVIC most often uses educational and informal tools to resolve issues. In the case of significant, persistent or systemic Professional Standards breaches, the matter will be escalated to a senior member of OVIC's Public Access Branch for consideration of formal action.

Where appropriate, OVIC may consider investigating a Professional Standards breach through an own-motion investigation.

Investigations

OVIC can investigate how a regulated body performs, fails to perform or purports to meet obligations under the FOI Act.[29]

OVIC can decide to investigate a regulated body on its own motion and does not require a complaint or report to prompt an investigation. OVIC will consider an own motion investigation where, for example, there appears to be a significant, persistent or systemic contravention of the FOI Act.

OVIC is also required to undertake an investigation of a public interest complaint referred by IBAC.[30]

How OVIC investigates

OVIC identifies issues of non-compliance in many ways including through:

- FOI reviews and complaints;

[29] Section 61O(1) of the FOI Act.

[30] Section 61TA(1) of the FOI Act.

- stakeholder engagement;
- engaging with regulated bodies including through their reports of FOI statistics; and
- reports from members of the public, including the media.

OVIC uses this information in the exercise of its regulatory activities. For example, there may be instances where it is considered appropriate to conduct both a review and an investigation into an FOI complaint, where the outcome sought is both access to documents and a remedy to address procedural or processing issues, including non-compliance with statutory obligations.

OVIC's investigation approach will be made on a case-by-case basis. OVIC usually commences investigations by contacting affected parties and the regulated body's principal officer to gather information and make preliminary inquiries.

OVIC's powers and prosecutable offences under the FOI Act

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 within a specified timeframe or compel a person to give evidence under oath or affirmation.

It is an offence:

- not to comply with a notice to produce or to attend;[31]
- to obstruct, hinder or resist OVIC officers in the performance of their duties;[32] and
- to mislead or provide false information to OVIC.[33]

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

[31] Section 61X of the FOI Act.

[32] Section 63F(1) of the FOI Act.

[33] Section 63F(2) of the FOI Act.

[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 will generally report 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 and the Professional Standards, OVIC will table completed investigation reports, unless there are compelling reasons not to.

After an investigation, OVIC will liaise with the regulated body to monitor the implementation of any recommendations made.

[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 public sector information under the VPDSS and PDP Act.

Where appropriate, OVIC will work with regulated bodies to resolve issues before taking formal action. Where the risk associated with an information security issue is significant, OVIC may take formal regulatory action.

Victorian Protective Data Security Framework and Standards

OVIC developed the VPDSF to monitor and assure the security of public sector information.[39]

To support the VPDSF, OVIC issued the VPDSS as mandatory requirements to help protect Victorian government information across five areas – governance, information security, personnel security, information and communications technology (**ICT**) security and physical security.[40]

The PDP Act requires regulated body Heads to undertake a Security Risk Profile Assessment (**SRPA**) and a Protective Data Security Plan (**PDSP**).[41]

The PDP Act also requires regulated body Heads to ensure the PDSP is reviewed every two years, or when there is a significant change in the regulated body's operating environment or security risks.[42]

[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] Section 85 of the PDP Act.

[40] Sections 86 and 87 of the PDP Act.

[41] Section 89(1)(a) and (b) of the PDP Act.

[42] Section 89 of the PDP Act.

Role of OVIC in regulating information security

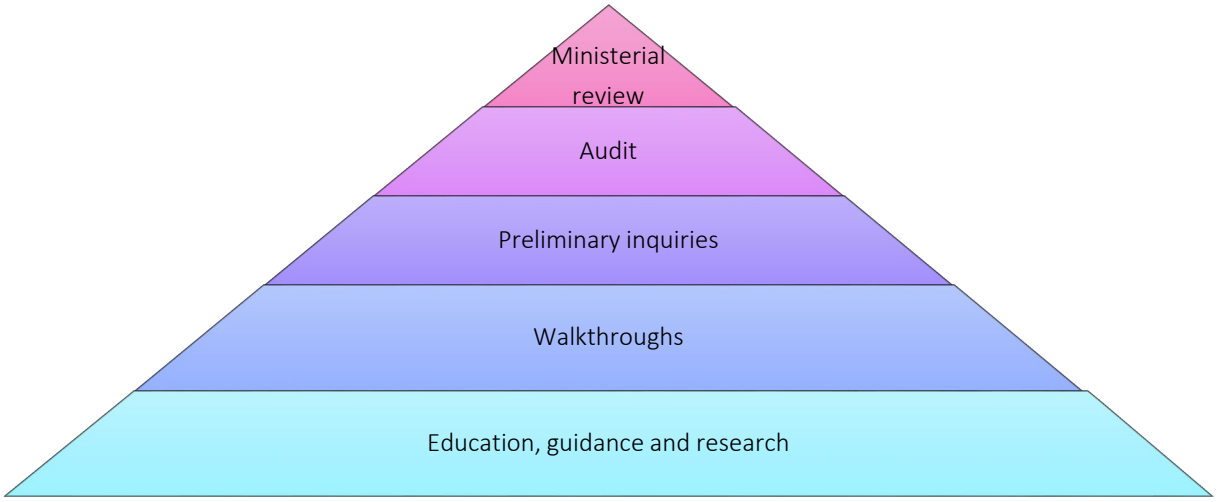


Figure 3 Levels of information security regulatory action

The PDP Act requires OVIC to research, promote, monitor and assure information security under the PDP Act.

Education, guidance and research

OVIC works collaboratively with regulated bodies to help them maintain the confidentiality, integrity and availability of Victorian public sector information. Regulated bodies are encouraged to proactively engage with OVIC to seek education, and guidance of the VPDSF and VPDSS.

OVIC provides a range of guidance tools and other resources online including video guidance, FAQs, business impact level apps, templates and specific guidance about information security topics.

OVIC may also undertake research in relation to protective data security and law enforcement data security matters relevant to the public sector, particularly on ICT.[43]

Walkthroughs

OVIC may conduct a walkthrough of a regulated body's information environment.

A walkthrough provides OVIC with the opportunity to discuss the information security policies, governance arrangements and practices. A walkthrough will be arranged by appointment. When

[43] Section 8D(1)(d) of the PDP Act.

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 trends, themes and issues through a variety of channels including reviews of PDSPs, incident notifications, reports from the public, media or social media reports, referrals from other regulators and insights from outreach and engagement activities.

When OVIC becomes aware of an information security issue, it generally starts by making preliminary inquiries of the regulated body.

Preliminary inquiries often start with an email or telephone call to the regulated body asking for further information. Regulated body Heads are required to provide assistance[44] and direct their staff to constructively assist and be transparent in their dealings with OVIC.

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

During this phase, OVIC may offer non-binding suggestions to improve practice or suggest actions to address non-compliance with the VPDSS. Preliminary inquiries also allow the Information Commissioner to decide whether to conduct further regulatory activity.

Audit

OVIC audits regulated bodies to ensure compliance with the VPDSS and PDP Act.[45]

Audits can be used:

- to investigate non-compliance with the VPDSS or PDP Act;
- as a proactive, periodic assurance tool;
- inform research activities; and
- to target a particular information security issue.

[44] Section 110 of the PDP Act.

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

In an audit, OVIC may review the regulated body's information security environment, governance arrangements, policies, procedures 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.

Ministerial reviews

At the request of the Minister, the Information Commissioner must undertake reviews of information security matters and report to the Minister.[46]

On receipt of a report, the Minister may table a copy of the report before each House of Parliament.[47]

OVIC's powers and prosecutable offences under the PDP Act

When OVIC conducts any information security monitoring or assurance activities, the regulated body is obliged to assist OVIC.[48]

OVIC may also require free and full access at all reasonable times to a government body's data or data system and to take copies of that information.[49]

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.[50] Information obtained can be referred to responsible agencies for urgent investigation or attention.[51]

[46] Section 8D(2)(d) of the PDP Act.

[47] Sections 111(2) and 8D(1)(d) of the PDP Act.

[48] Section 110 of the PDP Act.

[49] Sections 106, 107, 109 and 110 of the PDP Act.

[50] Section 122 of the PDP Act.

[51] 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.

www.ovic.vic.gov.au