**GUIDING PRINCIPLES FOR SURVEILLANCE**

# **USING THIS GUIDE**

The Guiding Principles for Surveillance (**Guiding Principles**) and accompanying Checklist and Case Studies should be used by any Victorian public sector organisation that monitors or analyses personal information or data.

Surveillance can include, but is not limited to, the use of CCTV, remote invigilator software, analytics software, user management and monitoring tools, artificial intelligence, or tracking employee logins and activity, irrespective of the purpose of the data collection or analysis.

Using the Guiding Principles and Checklist will support organisations to identify and evaluate surveillance practices and take a privacy and human rights enhancing approach to its use.

The Guiding Principles must be interpreted alongside legislative frameworks applicable to organisations, such as legislation permitting or prohibiting surveillance generally, or in specific instances.

# **SURVEILLANCE AND THE RIGHT TO PRIVACY**

Organisations that use surveillance to collect personal information have various obligations under the *Privacy and Data Protection Act 2014* (**PDP Act**) and the Information Privacy Principles (**IPPs**). These obligations require organisations to undertake surveillance in a privacy enhancing way, which involves protecting the privacy of individuals that the information is about, and collecting and handling personal information in a transparent and responsible manner.[[1]](#endnote-1)

The sophistication of surveillance technologies is improving exponentially. These advancements increase the risk that unlawful or arbitrary surveillance will interfere with the right to privacy. This highlights the importance of organisations adopting a privacy enhancing approach to surveillance that respects the human rights of Victorians.

Surveillance that is not undertaken with a privacy enhancing approach has the potential to interfere with various civil liberties that are fundamental to Victoria’s democracy. International human rights law[[2]](#endnote-2) and the Victorian Charter of Human Rights and Responsibilities[[3]](#endnote-3) codify and preserve these civil liberties, while the PDP Act and the IPPs both complement and enhance these rights.

The Guiding Principles provide organisations with an ethical framework for the use of surveillance that respects and protects privacy and human rights, and assists organisations to meet their duties and obligations. Using a human rights lens, the Guiding Principles apply the obligations under the IPPs to how they would generally operate when organisations use surveillance to collect and analyse personal information.

This guidance should be read alongside the PDP Act and the IPPs, as well as OVIC’s [*Artificial Intelligence resources*](https://ovic.vic.gov.au/privacy/privacy-resources-for-organisations/) and the [*Technology Systems and Solutions resources*](https://ovic.vic.gov.au/privacy/privacy-resources-for-organisations/). Together, these resources form a framework that is designed to guide organisations on complying with the PDP Act and IPPs, and upholding individual human rights when using surveillance.

# **DEFINITION OF SURVEILLANCE**

Surveillance is the monitoring and analysis of data to collect information about persons, groups, and contexts, often through the use of technology.[[4]](#endnote-4) Surveillance technologies are tools used to conduct surveillance activities. These range from devices, such as cameras and microphones, to automated software processes that incorporate algorithmic analysis, artificial intelligence, and quantum computing.

The surveillance described in these Guiding Principles includes actions and practices of surveillance that are either intentional or incidental, and overt or covert. Moreover, these Guiding Principles acknowledge that aggregation and analysis of metadata can reveal a wide range of personal and sensitive information about an individual.[[5]](#endnote-5) As such, the surveillance described in these Guiding Principles encompasses acts and practices of surveillance that result in the monitoring and analysis of an individual’s personal information and/or metadata.

# **THE GUIDING PRINCIPLES FOR SURVEILLANCE**

These seven Guiding Principles are designed to assist organisations that use surveillance to meet their privacy obligations under the PDP Act. Respecting privacy in the use of surveillance protects the human rights of Victorians and Victoria’s democracy.

* Principle 1: Legality
* Principle 2: Legitimate aim
* Principle 3: Necessity
* Principle 4: Proportionality
* Principle 5: Safeguards
* Principle 6: Non-discrimination
* Principle 7: Complaints and remedy

## ***PRINCIPLE 1: LEGALITY***

1. An organisation ensures all surveillance is lawful.[[6]](#endnote-6)
2. An organisation undertakes a [privacy impact assessment](https://ovic.vic.gov.au/privacy/privacy-officer-toolkit/privacy-impact-assessments/?highlight=privacy%20impact%20assessment) when considering surveillance.
3. An organisation complies with the [IPPs](https://ovic.vic.gov.au/privacy/information-privacy-principles-full-text/) when collecting personal information and [sensitive information](https://ovic.vic.gov.au/privacy/information-privacy-principles-full-text/#schedule-1-the-information-privacy-principles) through surveillance.
4. An organisation periodically reviews its surveillance practices to ensure they remain lawful.

## ***PRINCIPLE 2: LEGITIMATE AIM***

1. An organisation only collects personal information by surveillance when that surveillance is connected to a legitimate aim that directly corresponds to the organisation’s functions or activities.[[7]](#endnote-7)
2. An organisation limits the use of personal information collected through surveillance to the primary purpose for the surveillance or a permitted secondary purpose.[[8]](#endnote-8)

## ***PRINCIPLE 3: NECESSITY***

1. An organisation limits personal information collected through surveillance to that which is demonstrably necessary to achieve a legitimate and lawful aim.[[9]](#endnote-9)
2. An organisation does not use surveillance to collect personal information about an individual, where it is reasonable and practicable to collect the personal information directly from that individual without using surveillance.[[10]](#endnote-10)

## ***PRINCIPLE 4: PROPORTIONALITY***

1. An organisation assesses the proportionality of the surveillance required in the particular circumstances of an individual case, to ensure the surveillance is carried out in a way that is least likely to impact on privacy and human rights.[[11]](#endnote-11)
2. An organisation limits surveillance to the least intrusive acts, practices, or methods that are necessary to achieve a legitimate and lawful aim.[[12]](#endnote-12)
3. An organisation limits surveillance to relevant individuals only.

## ***PRINCIPLE 5: SAFEGUARDS***

1. An organisation implements procedural safeguards when using surveillance and ensures these safeguards are effective and adequately resourced.

### **Transparency**

#### Notifications

1. At or before the time (or, if that is not practicable, as soon as practicable after) an organisation uses surveillance to collect personal information about an individual, an organisation takes reasonable steps to ensure that the individual is aware of:
	1. the identity of the organisation using surveillance and how to contact it; and
	2. the fact that the individual can gain access to the information collected through surveillance; and
	3. the purposes for which the surveillance is being used; and
	4. to whom the organisation usually discloses information collected through surveillance; and
	5. any law that enables the surveillance to be used.[[13]](#endnote-13)

#### Openness

1. An organisation makes available a document setting out the sorts of personal information it collects through surveillance, its purposes for using surveillance, the specific surveillance practices it uses for collection, and how collected personal information is used and disclosed.[[14]](#endnote-14)
2. An organisation considers proactively publishing policies and records in relation to its use of surveillance.[[15]](#endnote-15)

#### Access to personal information

1. An organisation provides individuals whose personal information has been collected through surveillance with the ability to request access to that information.[[16]](#endnote-16)

### **De-identification**

1. An organisation takes reasonable steps to destroy or permanently de-identify personal information collected through surveillance if it is no longer needed.[[17]](#endnote-17)
2. An organisation considers the risks of re-identification when de-identifying personal information, and destroys personal information collected through surveillance where the risk of re-identification cannot be reduced to very low.

### **Anonymity**

1. An organisation only collects anonymous information through surveillance, rather than personal information, wherever it is reasonably practicable.[[18]](#endnote-18)

### **Information sharing**

1. An organisation limits the sharing and disclosure of personal information collected though surveillance to the primary purpose of the surveillance or a permitted secondary purpose.[[19]](#endnote-19)
2. An organisation does not transfer personal information collected about an individual through surveillance to someone (other than the collecting organisation or the individual) who is outside of Victoria, unless permitted by the IPPs.[[20]](#endnote-20)

**Information security**

1. An organisation takes reasonable steps to protect personal information collected through surveillance from being misused, lost, or accessed, modified, or disclosed by unauthorised persons.[[21]](#endnote-21)

## ***PRINCIPLE 6: NON-DISCRIMINATION***

1. An organisation does not use surveillance in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

## ***PRINCIPLE 7: COMPLAINTS AND REMEDY***

1. An organisation provides information and pathways for individuals to complain directly to the organisation where they believe their privacy has been interfered with.
2. An organisation works constructively to remedy privacy complaints involving surveillance where they are escalated to the Information Commissioner.[[22]](#endnote-22)
1. See, section 5 and section 8C(1)(g) of the PDP Act. [↑](#endnote-ref-1)
2. Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including African Charter on the Rights and Welfare of the Child Article 10, American Convention on Human Rights Article 11, African Union Principles on Freedom of Expression Article 4, American Declaration of the Rights and Duties of Man Article 5, Arab Charter on Human Rights Article 21, ASEAN Human Rights Declaration Article 21, European Convention for the Protection of Human Rights and Fundamental Freedoms Article 8; Organisation for Economic Cooperation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data Part 1: General Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality. [↑](#endnote-ref-2)
3. Charter of Human Rights and Responsibilities Act 2006 (VIC) section 13, the right not to have one’s privacy, family, home or correspondence arbitrarily interfered with. [↑](#endnote-ref-3)
4. Marx, G. T. (2015). Surveillance studies. *International encyclopaedia of the social & behavioural sciences*, *23*(2), 733-741. [↑](#endnote-ref-4)
5. In the context of surveillance, metadata is information about a person that, unaggregated, would not form personal information about an individual, such as geolocation or communications data. [↑](#endnote-ref-5)
6. IPP 1.2, PDP Act. [↑](#endnote-ref-6)
7. IPP 1.1, PDP Act. [↑](#endnote-ref-7)
8. IPP 2, PDP Act. [↑](#endnote-ref-8)
9. IPP 1.1, PDP Act. [↑](#endnote-ref-9)
10. IPP 1.4, PDP Act. [↑](#endnote-ref-10)
11. IPP 1.2, PDP Act. [↑](#endnote-ref-11)
12. IPP 1.2, PDP Act. [↑](#endnote-ref-12)
13. IPP 1.3, PDP Act. [↑](#endnote-ref-13)
14. IPP 5, PDP Act. [↑](#endnote-ref-14)
15. Part II of the *Freedom of Information Act 1982* (Vic). [↑](#endnote-ref-15)
16. Under the *Freedom of Information Act 1982* (Vic), section 17 allows individuals to request access to documents and section 39 allows correction of records containing personal information. Under the PDP Act, IPP 6 equally allows access and correction if the FOI Act does not apply to an organisation. [↑](#endnote-ref-16)
17. IPP 4.2, PDP Act. [↑](#endnote-ref-17)
18. IPP 8, PDP Act. [↑](#endnote-ref-18)
19. IPP 8, PDP Act. [↑](#endnote-ref-19)
20. IPP 9.1, PDP Act. [↑](#endnote-ref-20)
21. IPP 4.1, PDP Act. Certain Victorian organisations have information security obligations under the Victorian Protective Data Security Framework and Standards. See OVIC’s website for further information - <https://ovic.vic.gov.au/data-protection/framework-vpdsf/>. [↑](#endnote-ref-21)
22. See *Privacy Complaints at OVIC – Guide for Individuals*, at <https://ovic.vic.gov.au/privacy/privacy-complaints-at-ovic-guide-for-individuals/>. [↑](#endnote-ref-22)