Office of the Victorian Information Commissioner

IPP 10 – Sensitive Information

IPP 10 – Sensitive Information

On this page

10.1 IPP 10 regulates the collection of personal information that falls within one of the categories contained in the definition of 'sensitive information' under Schedule 1 of the PDP Act. IPP 10 prohibits the collection of sensitive information, subject to a number of exceptions in IPP 10.1 and 10.2.

10.2 The PDP Act imposes restrictions on the collection and handling of sensitive information. There are additional restrictions because certain types of personal information carry inherent risks to individuals' privacy and other rights.[1] One of the most obvious risks associated with the collection and handling of sensitive information is discrimination, for example, discrimination on the basis of racial or ethnic origin, sexual practices, or political opinions. Unnecessary or unlawful collection or use of these types of sensitive information may give rise to parallel rights under both privacy and anti-discrimination laws.

10.3 Organisations should handle sensitive information carefully. A breach of sensitive information may be more damaging to individuals than other personal information breaches and may lead to further encroachments on an individual's rights.

10.4 Sensitive information can often be confused with other types of information that are widely regarded as requiring additional protection. For example, details of a person's finances are widely regarded as requiring a high degree of protection, but do not fall under the definition of sensitive information in the PDP Act. Likewise, biometric information does not fall under the definition of sensitive information in the PDP Act, however, given such information relates to individuals' unique physiological and behavioural characteristics, it should also be afforded a higher degree of protection.[2] This sort of information is sometimes referred to as 'delicate information'. For more information about delicate information, refer to 'Sensitive and Delicate Information' in the Key Concepts chapter.

Categories of 'sensitive information'

10.5 The definition of 'sensitive information' is in Schedule 1 of the PDP Act. Sensitive information means information or an opinion that relates to an individual's –

- racial or ethnic origin; or
- political opinions; or
- membership of a political association; or
- religious beliefs or affiliations; or
- philosophical beliefs; or
- membership of a professional or trade association; or
- membership of a trade union; or
- sexual preferences or practices; or
- criminal record—

[1] Council of Europe, *Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108)*, explanatory note to Article 6 (Special categories of data), para 43, available here.
[2] Refer to OVIC's *Biometrics and privacy* information sheet.

that is also personal information.

10.6 Sensitive information is a subset of personal information. Sensitive information is therefore subject to all the other IPPs just like all other personal information. IPP 10 simply adds restrictions on the collection of sensitive information. For more information about personal information, refer to Personal Information in the Key Concepts chapter.

10.7 Like other provisions of the PDP Act, IPP 10 will be interpreted and applied in a manner that is compatible with human rights so far as it is possible to do so, consistent with the PDP Act's purpose.[3]

Racial or ethnic origin

10.8 Racial or ethnic origin is not defined in the PDP Act.

10.9 The Macquarie Dictionary relevantly defines race as meaning 'a group of people sharing genetically determined characteristics such as skin pigmentation or hair texture', or 'a group of people sharing a language or culture or traditional beliefs or practices'.[4] In the *Racial and Religious Tolerance Act 2001* (Vic) and the *Equal Opportunity Act 2010* (Vic) (**EO Act**), 'race' is defined as including:

- colour;
- descent or ancestry;
- nationality or national origin;
- ethnicity or ethnic origin;
- if 2 or more distinct races are collectively referred as a race –
    - each of those distinct races;
    - that collective race'.[5]

10.10 According to a federal case *Yang v Langs Building Suppliers Pty Ltd* [2018] FCCA 3203, 'language may be but is not necessarily a racial attribute'. In the NSW Supreme Court, citizenship has not been regarded as an element of 'race'.[6]

10.11 From these definitions, it is apparent that 'race' is a broad concept, encompassing groups that share genetic characteristics, and also groups that share language, culture, or traditional beliefs or practices.

10.12 The term 'ethnic origin' has been regarded by the courts as having a wider meaning than 'racial origin'. The UK House of Lords considered the meaning under UK legislation in *Mandla v Dowell Lee*.[7] This case was a complaint of racial discrimination involving the refusal by a school headmaster to admit a Sikh boy, unless he removed his turban and cut his hair. The House of Lords found Sikhs were an 'ethnic group' for the purposes of the legislation, and the meaning of 'ethnic' should not be restricted to biological characteristics. This case indicated that characteristics used to identify an ethnic group included:

- a shared history;

---

[3] The Information Commissioner, like other Victorian public authorities, is obliged to give proper consideration to a relevant human right when making a decision (*Charter of Human Rights and Responsibilities Act 2006* (Vic) s 38).
[4] *Macquarie Dictionary* (2017, 7th ed) Macquarie Dictionary Publishers, Sydney.
[5] *Racial and Religious Tolerance Act 2001* (Vic), s 3; *Equal Opportunity Act 2010* (Vic) s 4.
[6] *Re Carl* [2003] NSWSC 756. This is a case involving a complaint about a decision refusing the plaintiff entry to a selective high school because he was not an Australian or New Zealand citizen or a permanent resident of Australia.
[7] *Mandla v Dowell Lee* [1983] 2 AC 548.

- its own cultural tradition;
- a common geographical origin or descent from a small number of ancestors;
- a common language;
- a common literature peculiar to the group; and
- a common religion differing from neighbouring groups or the surrounding community.[8]

10.13 This approach has been adopted in Australia, for example, in the Federal Court case of *Jones v Scully* [2002] FCA 1080, a racial vilification case brought under the *Racial Discrimination Act 1975* (Cth).

10.14 Information can be regarded as relating to 'racial or ethnic origin', and therefore sensitive information, if it discloses someone's race or ethnicity, as those concepts are described above. It may also relate to their racial or ethnic origin if it concerns the characteristics of particular races or ethnicities, such as those identified above.

Political opinion

10.15 Political opinion is not defined in the PDP Act. The term 'political' has been interpreted in Victoria as a 'matter or activity that involves that state and "bears on government"'.[9] However, in *Australian Anti-Discrimination and Equal Opportunity Law* (Rees et al 2018), the idea of political belief is discussed in an anti-discrimination context. It states:

> 'What is political must be determined objectively, taking into account the nature of the activity or belief. In most cases, the perceptions of the parties will be irrelevant.[10] A belief is not political because a person says or thinks it is. However, there may be cases where a person considers that belief is political because the society in general, and other people who hold that belief, also consider it so. This may well be evidence that the belief is in fact political.'[11]

10.16 Political opinion was raised in the Federal Court of Australia in *Sayed v Construction, Forestry, Mining and Energy Union* [2015] FCA 27. Judge Mortimer concluded that regardless of the complete meaning of 'political opinion', he was certain that:

> 'the applicant's membership of, and involvement in the activities of, the Socialist Alliance constituted the holding and manifestation of a political opinion within the meaning of that phrase in s 351 of the Fair Work Act.'

10.17 Individuals involved in a group protesting about a government project might be considered as conveying a political opinion, or, in some circumstances, showing membership in a political association. This means information about a person's involvement in a protest would likely fall within the definition of sensitive information.

Membership of a political association

10.18 In *Complainants R, S, T, U and V v Local Council* [2005] VPrivCmr 4, the Privacy Commissioner considered the meaning of the third category of sensitive information: membership of a political

---

[8] *Mandla v Dowell Lee* [1983] 2 AC 548, 562 (Lord Fraser), referring to *King-Ansell v Police* (1979) 2 NZLR 531.
[9] Victorian Equal Opportunity and Human Rights Commissioner, *Victorian Discrimination Law*, *Chapter 3 Protected Attributes,* p.26. See also *Hein v Jacques Ltd* (1987) EOC 92-188; followed in this respect *Nestle Australia Ltd v Equal Opportunity Board* [1990] VR 805; (1990) EOC 92-281); *CPS Management Pty Ltd v President and Members of the Equal Opportunity Board* [1991] 2 VR 107; (1991) EOC 92-332 at 78, 290.
[10] *Duggan v South Yarra Constructions Pty Ltd* (1987) EOC 92-220.
[11] Rees, Neil, Rice, Simon, Allen, Dominique, *Australian Anti-Discrimination and Equal Opportunity Law*, 3rd edition, The Federation Press,2 7 February 2018, 541.

association. The Privacy Commissioner found that information about the complainants' membership of a local ratepayers association fell within the category 'membership of a political association'. In that case, the Privacy Commissioner noted that 'political' is not defined in the PDP Act, but has been interpreted by the Victorian Supreme Court in anti-discrimination cases as being a matter or activity which has a bearing on government.

Religious beliefs or affiliations

10.19 'Religious belief or activity' is defined in the EO Act to mean holding or not holding a lawful religious belief or view; or engaging or not engaging in a lawful religious activity.[12] Although the term 'religious belief' is not defined in the PDP Act, OVIC considers that it includes both the holding of a religious belief, and the absence of religious belief.

Membership of a trade union

10.20 Information about trade union membership is also considered sensitive information under the PDP Act. Trade union membership information can include information about:

- whether or not an individual is a trade union member;
- an individual's type of trade union membership; and
- the length of time the individual has been a member of the trade union.

10.21 Information collected from employees will include sensitive information if it is information about membership of a trade union. In *Seven Network (Operations) Limited v Media Entertainment and Arts Alliance* [2004] FCA 637, the Federal Court of Australia accepted that information collected from Seven Network employees included sensitive information. The information was collected during a telephone poll carried out by a call centre on behalf of a union (MEAA). The call centre's polling script asked questions, including whether:

- the employee was a member of the union;
- he or she would be willing to take part in various forms of industrial action; and
- he or she wanted further contact with the union.

Criminal record

10.22 'Criminal record' is not defined in the PDP Act, and there is very little case law that explains what the term means. OVIC suggests that 'criminal record' should be broadly interpreted to mean any information associating an identifiable individual with criminal behaviour, either alleged or proven. VCAT has suggested that a person's 'criminal record' is likely more than just 'findings of guilt and the sentences or other dispositions in which those findings result', and may include information such as booking forms, or legal advice that relates to an individual's criminal defence.[13] Another example of information that may relate to a person's criminal record is a photograph taken by police of that person while in custody.[14]

When may sensitive information be collected?

10.23 IPP 10 states organisations must not collect sensitive information unless one of the grounds in IPP 10.1 or IPP 10.2 applies. In addition to identifying a valid ground for collection under IPP 10,

[12] *Equal Opportunity Act 2010* (Vic) s 4.
[13] *Gao v Victoria Legal Aid* (Health and Privacy) [2012] VCAT 523.
[14] *Smith v Victoria Police* (General) [2005] VCAT 654.

organisations should consider the usual requirements for the collection of personal information in IPP 1. Relevantly, IPP 1 (Collection) specifies that personal information may only be collected if:

- the information is necessary for the organisation's functions or activities (IPP 1.1);
- the information is collected by lawful and fair means, and in a manner that is not unreasonably intrusive (IPP 1.2);
- the information is collected directly from the individual, where it is reasonable and practicable to do so (IPP 1.4); and
- proper notice is provided about who is collecting the information and why, to whom the information is usually disclosed, any legal basis for requiring the information, any usual disclosures, the individual's right of access and consequences for the individual if they do not provide any or all of the information (IPP 1.3).

10.24 When collecting personal information, organisations should be mindful of inadvertent collection of sensitive information. For example, the collection of an individual's photos (such as a driver's licence) or location data may inadvertently reveal information about their racial or ethnic origin, or religious beliefs. Where there is a real likelihood that organisations will collect sensitive information inadvertently, they should ensure the collection is authorised under IPP 10, while also considering the requirements under IPP 1.

10.25 The handling of sensitive information is also subject to greater restrictions under IPP 2.1(a). IPP 2.1(a) requires reasonably expected secondary uses and disclosures of sensitive information to be directly related to the primary purpose for collecting the sensitive information. See the discussion on 'Reasonably expected related secondary purposes' in the IPP 2 chapter of these Guidelines.

10.26 Other legislation may contain provisions permitting the use and disclosure of sensitive information. For example, the *Family Violence Protection Act 2008* (**FVP Act**) allows certain agencies (known as information sharing entities) to share sensitive information under the Family Violence Information Sharing Scheme.[15] The provisions under the FVP Act override the requirements under IPP 10 to the extent of the inconsistency of the relevant IPPs.[16]

10.27 The discussion below explains each of the exceptions of IPP 10.1 that permit the collection of sensitive information.

IPP 10.1(a): Individual gives consent

10.28 Organisations can collect sensitive information under IPP 10.1(a) where the individual gives consent. Consent must be informed, current, specific, voluntary and given by someone with capacity. For example, consent may not be valid if an individual has no real choice but to agree to the collection of sensitive information (for example, the collection of criminal record histories for job applicants).

10.29 The validity of consent may be affected if an organisation fails to comply with the notice obligations under IPP 1.3. This is particularly the case where individuals may not have provided their information had they known the reason for the collection or how the organisation would later use their information. Collecting sensitive information without telling individuals why it is being collected, to whom it is usually disclosed and whether they have a choice in providing the information will likely affect whether the consent given was informed and voluntary. Additionally,

[15] See OVIC's *Family violence information sharing scheme and privacy law FAQs* for more information.
[16] PDP Act, s 6.

if individuals are misled into believing they are required to provide their information when this is not actually the case, any resulting collection may also be regarded as unfair. For more information, see the discussion of 'fair' in the IPP 1 chapter.

10.30 Consent is the most common basis for collection of sensitive information. When organisations rely on consent, individuals know who is collecting sensitive details such as their racial or ethnic origin, criminal records, sexual preferences or practices, religious beliefs or affiliations, or political opinions. If organisations are unable to seek consent, or where valid consent cannot be given, organisations should consider whether they are permitted to collect sensitive information under one of the other grounds set out in IPP 10.1 or IPP 10.2.

IPP 10.1(b): Required or authorised under law

10.31 IPP 10.1(b) permits organisations to collect sensitive information where the collection is required or authorised under law.[17] See the discussion on 'required or authorised by law' in the IPP 2 chapter.

10.32 In the absence of a legislative mandate, organisations seeking to collect sensitive information should obtain the individual's consent or look to one of the other grounds specified under IPPs 10.1 or 10.2.

IPP 10.1(c): Necessary to lessen or prevent a serious threat to the life or health of any individual

10.33 IPP 10.1(c) allows sensitive information to be collected where the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual to whom the sensitive information relates cannot provide consent because that individual is either physically or legally incapable of consenting, or physically cannot communicate their consent.

10.34 This exception is similar to the exception for use and disclosure under IPP 2.1(d), which is discussed in the IPP 2 chapter of these Guidelines.

IPP 10.1(d): Necessary for legal or equitable claims

10.35 Organisations are permitted to collect sensitive information where the collection is necessary for the establishment, exercise or defence of a legal or equitable claim. The meaning of 'necessary' is discussed in the Key Concepts chapter of these Guidelines.

10.36 IPP 10.1(d) may be relevant to situations where, for example, an organisation is defending itself against a claim of unlawful discrimination or unfair dismissal.

10.37 The establishment, exercise or defence of legal or equitable claims includes situations where it is necessary to collect sensitive information for the purpose of obtaining legal advice in connection with an existing or potential legal proceeding in a court or tribunal. There should either be a legal proceeding on foot or a real possibility the organisation will need to exercise or defend its legal or equitable rights in the near future. In other words, sensitive information should not be collected 'just in case' there is a future legal claim or defence.

10.38 As noted earlier, IPP 10 should be read in conjunction with IPP 1. IPP 10.1(d) will not permit the collection of sensitive information for use in legal proceedings where that information is unlawfully or unfairly obtained, or collected in an unreasonably intrusive way. See the discussion

[17] The *Victorian Data Sharing Act 2017* amended IPP 10.1(b) to include 'or authorised' under law.

of 'lawful' and 'fair' in the IPP 1 chapter of these Guidelines.

IPP 10.2: Use of sensitive information for research or statistical purposes

10.39 Organisations may also collect sensitive information if it meets one of the exceptions under IPP 10.2, where the collection:

- is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
- is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; *and*
- there is no reasonably practicable alternative to collecting the information for that purpose; and
- it is impracticable for the organisation to seek the individual's consent to the collection.

'Government funded targeted welfare or educational services'

10.40 The authority in IPP 10.2 is limited to 'welfare or educational services' that are 'targeted' and 'funded' by government.

10.41 'Welfare or educational services' are likely to include schooling and educational support services, and programs aimed at promoting physical and social wellbeing, especially for those in financial or social need. For example, welfare services might include the provision of health, counselling and support services, and assistance programs in obtaining employment and housing.

10.42 The funded service must be 'targeted'. This may mean the service is aimed at a particular group of persons, for example, referral and support services for victims of crime. 'Targeted' may also mean the service is carried out with a particular objective or result in mind, for example, reducing homelessness or unemployment in Victoria.

10.43 'Government funded' services can include services funded by any combination of local, state or federal governments. This can occur through government grants or more direct funding arrangements, for example a service agreement or contract. It is not necessary under IPP 10.2 for the government to have any control over the service provider or the delivery of the funded services.[18] Also, IPP 10.2 does not require the funded services to be related to the particular functions of the funding organisation,[19] although the services must be of an educational or welfare kind.

IPP 10.2(a)(i): Sensitive information necessary for research or statistics about government services

10.44 IPP 10.2(a)(i) allows Victorian government organisations (and, where relevant, their contracted service providers) to collect sensitive information necessary to carry out research, or compile and

[18] This is in contrast to the application of the *Freedom of Information Act 1982* (Vic), which extends to prescribed authorities defined in s 5 of that Act to include 'an incorporated company or association or unincorporated body **which is supported directly or indirectly by government funds or other assistance or over which the State is in a position to exercise control'** (emphasis added).

[19] IPP 10.2 does not require a 'State contract' to be on foot where an outsourcing organisation engages the service provider to provide a service 'in connection with the performance of functions of the outsourcing state or local government organisation'. Where the service is carried out under a 'State contract', organisations would be expected to consider binding the service provider to the PDP Act through the use of a clause under s 17(2) of the PDP Act. For further guidance on outsourcing, see OVIC's *Guidelines for outsourcing accompanying guide and checklist*.

analyse statistics, about government funded educational or welfare services. This has the obvious benefit of enabling government to assess whether public funds are being spent effectively.

10.45 The collection of sensitive information must be 'necessary' for the research or statistics to be carried out. See the discussion on the meaning of 'necessary' in the Key Concepts chapter.

IPP 10.2(a)(ii): Information about racial or ethnic origin to deliver government services

10.46 IPP 10.2(a)(ii) authorises the collection of information about an individual's racial or ethnic origin where this is collected for the purpose of providing a government funded targeted welfare or educational service. It does not, however, authorise the collection of other types of sensitive information for the purpose of service delivery.

10.47 Collection of information about individuals' racial and ethnic origin without their consent through this exception should only occur where it is necessary for the effective delivery of government welfare programs.[20]

IPP 10.2(b): No reasonably practicable alternative to proposed collection

10.48 IPP 10.2(b) emphasises the need to keep non-consensual collection of sensitive information to a minimum by directing organisations to consider all practicable alternatives. For example, organisations might consider whether the research, statistics or service delivery can be conducted by using information that is not sensitive information or, where it is necessary to collect sensitive information, doing so by consent. Organisations should routinely consider whether they can use anonymous or de-identified information. This is consistent with their obligations under IPP 1.1 and IPP 8.

IPP 10.2(c): Impracticable to seek consent

10.49 Impracticability should not be confused with undesirability. IPP 10.2(c) does not permit consent to be waived where the organisation can readily seek consent but would prefer not to, for example because a high rate of participation is desired and the organisation fears individuals would refuse their consent if asked.

10.50 For more information on the meaning of 'practicable' please refer to the Key Concepts chapter. The discussion on 'Impracticable to seek consent' in the research context is discussed in IPP 2 chapter.

> Please send any queries or suggested changes to privacy@ovic.vic.gov.au. We will respond to privacy enquiries and consider your suggestions when we next update the Guidelines to the Information Privacy Principles.

[20] See the clause note to IPP 10 in the Explanatory Memorandum to the Privacy and Data Protection Bill 2014.

Version control table

Version	Description	Date published
IPP 10 – Sensitive Information 2019.B	Edits following consultation.	14 November 2019
IPP 10: Sensitive Information 2019.A	Consultation draft.	1 August 2019
IPP 10: Sensitive Information (2011)	2011 pdf version.	2011