Office of the Victorian Information Commissioner

IPP 8 – Anonymity

IPP 8 – Anonymity

On this page

> IPP 8 states:
>
> *Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.*
>
> The underlying objective of the anonymity principle is to maximise the individual's control in their interactions with government and to minimise government's intrusion into the life of the individual.

8.1 IPP 8 is intended to preserve and protect the ability of individuals to remain anonymous in transactions with government organisations.[1] It makes clear that, by default, people should be able to transact anonymously or pseudonymously.

8.2 Organisations should regularly look out for opportunities to introduce or reinstate the ability for individuals to engage in anonymous transactions. Reviewing information flows and why the organisation collects and needs certain personal information may highlight areas where an individual could transact anonymously. Allowing individuals to be anonymous when interacting with an organisation can minimise the risk of data loss in the case of a data security breach, as no personal information is collected in an anonymous transaction.

Transactions

8.3 'Transactions' should be interpreted broadly to include the interactions and dealings between the individual and the organisation, whether or not they involve an exchange in a commercial sense.

8.4 Examples of transactions where anonymity could be offered include:

- paying for goods and services – can individuals pay anonymously using cash? Do individuals need to provide identifying information when buying certain goods or services, such as a ticket to an event?
- using a computer for internet browsing – does the organisation need to know what websites users visit?
- travelling on public transport – how can members of the public travel anonymously, especially where valid tickets are held?
- walking along streets, through parks and attending other places open to the public – to what extent can individuals remain anonymous in a crowd when CCTV is installed?
- accessing and obtaining copies of publicly available government records – can the organisation allow individuals to anonymously access to government policies and procedures, including where these are made available online over the internet?
- making enquiries to government organisations – is it necessary to record a name or use CCTV

[1] See the note to IPP 8 in the Explanatory Memorandum, Privacy and Data Protection Bill 2014 (Vic) 35.

to monitor who attends your office to request general information about accessing government services or exercising their rights?
- interacting with government organisations online – can individuals interact with government organisations anonymously, or does the organisation require individuals to provide personal information before they are able to interact with, or contact, the organisation?
- expressing views and concerns at public meetings – is it necessary to record every speaker's identity in the minutes? Is it necessary to collect personal information about someone who complains about a general issue?
- use of monitoring or location-based tracking technology – if GPS is used to track the organisation's vehicles, can an employee turn off the GPS at certain times, for example, on their lunch break?

8.5 Whether the option of anonymity should or can be offered depends on the context. Under IPP 8, the option for transacting anonymously must be made available wherever it is lawful and practicable to do so. In certain circumstances, anonymity may be impracticable, for example, where justice centres have CCTV for the safety of staff. Organisations should also consider their obligation under IPP 1 (Collection) to only collect personal information that is necessary for their functions or activities.

Lawful and practicable

8.6 An organisation may be unable to offer an anonymous option if a law requires the organisation to identify an individual. In this case, allowing individuals to transact anonymously or pseudonymously would not be 'lawful'. For example, some laws require individuals to provide identifying information to transact with an organisation, for example, when individuals register for a profession or apply for a licence.

8.7 'Practicable' has been considered in these Guidelines in the Key Concepts chapter. Determining whether it is practicable to offer the option of anonymity involves consideration of matters such as the cost that may be involved in allowing an anonymous option and whether there is a public interest in requiring individuals to identify themselves.

8.8 Other factors that affect whether it is practicable to provide the option of anonymity include the functions of the organisation, the purpose of the interaction and the role of identifying information in the interaction. For example, it may not be practicable for a complaint handling body to provide an individual with the option of remaining anonymous if the complaint specifically concerns the treatment of that individual.[2] Similarly, it may not be practicable for an individual to remain anonymous where their identity is needed in order to provide them with a good or service.

8.9 Providing an anonymous option will not always be appropriate. Determining when anonymity is inappropriate requires organisations to carefully balance what can be done within existing legal and technological constraints and what should be done to promote and protect privacy and other fundamental rights and public interests. Any restrictions on the ability to transact anonymously should be limited to what is necessary and proportionate to protect the various interests at stake, while always considering possible less restrictive means.

8.10 Some examples where anonymity may not be appropriate include:

- The investigation of incidents involving serious criminal activity;

[2] *Complainant AW v Statutory Authority* [2012] VPrivCmr 1.

- Combating money laundering through financial institutions; and
- Ensuring the transparency of donations to political campaigns.

8.11 It may be necessary to collect some information to, for example, determine the quality of, or need for, services. Organisations should consider carefully what information is needed and whether it needs to be collected in an identified way. For example, when conducting a survey, it may be sufficient to ask a person for their suburb or postcode, or to survey individuals anonymously.

8.12 Where identification is needed to establish eligibility for a service or benefit, it might be sufficient to sight a document and record that the particular document was sighted, rather than to record or copy the personal information contained in the document.

Waiving anonymity

8.13 In some cases, individuals may decide to waive the option of anonymity and provide identifying information. This is consistent with the importance of control in privacy – individuals should be allowed to control what happens with their personal information – and the role of consent in other IPPs.

8.14 When individuals waive the option of anonymity, the collection still needs to be necessary to the organisation's functions or activities. An individual providing their personal information voluntarily with consent does *not* mean the organisation no longer needs to comply with IPP 1 (Collection). The important thing is that organisations provide the option of anonymity where practicable and lawful and, where individuals choose to identify themselves, ensure any identifying information is appropriately handled in accordance with the IPPs.

Case Study 8A: Mishandling of identifying information after anonymity option declined[3]

A woman residing in a small rural community contacted the customer service officer of a local council to report a leaking tap in the public toilets and the fact that her son had tripped and hit his head on the wet floor. The woman was asked at the outset whether she wanted to make her report anonymously. She decided to identify herself, saying later that she did so because she wanted a record of the incident concerning her son, but that she did not expect that in doing so, an employee of the council without a 'need to know' would have access to it.

The customer service officer forwarded a report, including the woman's name, to the relevant business unit supervisor. The supervisor then forwarded the report to an employee who was asked to coordinate the repairs. This employee in turn allegedly disclosed the woman's name to his spouse.

The woman heard about the disclosure when the employee's spouse allegedly accused the woman of complaining about her husband's work. The woman was concerned that, as a result of the disclosure, another member of the small community wrongly believed that the complaint had been about a particular person's work, rather than about a public facility.

[3] *Complainant N v Local Council* [2004] VPrivCmr 8.

The Privacy Commissioner commented that, in circumstances such as this, in which a council is required to respond to a report of a fault in a public facility, it is not necessary to the efficient repair of the fault for the identity of the person who reported the fault to be so widely circulated among council employees. In other circumstances, such as where the fault relates to the property of the person making the report, it is likely to be necessary (and often expected) that identifying information will be circulated to a wider range of employees or contractors so repairs can be undertaken efficiently and with consultation.

The Commissioner noted the impact of wide circulation of personal information within organisations and unauthorised disclosure outside them can be greater in small communities where people are more likely to know each other, and names are more easily recognised.

The council agreed to amend its incident reporting procedures to limit who has access to personally identifying incident reports, and to provide appropriate training for relevant employees. The council also undertook to continue its policy of allowing members of the public to anonymously report public health and safety matters.

Pseudonymity

8.15 Organisations may consider other means of promoting the intention underpinning IPP 8, such as by using pseudonymity. The use of pseudonyms, where lawful and practicable, can enable individuals to transact with organisations using a fictitious name instead of revealing their true identity. For example, where an organisation handles calls from the public, such as inquiries, that organisation may make records of the phone calls. In this example, pseudonymity can be used to allow the caller to not identify themselves and transact with the organisation anonymously. Where an individual's identity needs to be ascertained, for example, to send correspondence in the mail, pseudonymity is unlikely to be practicable.

8.16 Where pseudonymity is being considered, consider whether the information needs to be collected at all. Data quality issues under IPP 3 might also be relevant where the organisation is collecting information that may not necessarily be accurate. Please also refer to the Pseudonymisation and anonymised data in the Key Concepts chapter.

Case Study 8B: Pseudonymity when conducting a survey

An organisation might conduct a survey and receive responses from the public which contain unsolicited and unnecessary personal information. Because the personal information is not needed for the activity of the organisation (conducting a survey), the organisation could consider using pseudonyms to remove the personal information of respondents to the survey. This links to IPP 1 (Collection). Using pseudonymity might reduce the personal information collected by an organisation.

IPP 8 in practice

Complaint handling

8.17 IPP 8 is particularly relevant for the complaint handling functions of organisations. Many complaints can be resolved without collecting identifying information about complainants. For example, if a person complained about the state of a public facility, it is unlikely collection of their personal information would be necessary to fairly and appropriately respond to the complaint. See Case Study 8A, above.

8.18 In some instances, anonymity can encourage individuals to make complaints where they would otherwise fear the potential consequences of identifying themselves. In *Case Note 256145* [2015] NZ PrivCmr 2,[4] the complainant made a complaint to a government agency regarding their employer. The complainant requested their identity remain confidential, however, their name was inadvertently disclosed to the employer by the government agency, leading to a breakdown in the relationship between the complainant and their employer. The NZ Privacy Commissioner found it is important to allow individuals to remain anonymous when they make a complaint in certain circumstances, as individuals may be otherwise discouraged from expressing their concerns if they knew their identity would be disclosed to the party they had complained about.

8.19 In other contexts, it may not be practicable for individuals making a complaint to remain anonymous. Procedural fairness may require that a complainant's identity be disclosed so the party subject to the complaint can fairly respond to the allegations. For example, in *Complainant AW v Statutory Authority* [2012] VPrivCmr 1, the Privacy Commissioner found it was not practicable for the Statutory Authority to keep the Complainant's identity anonymous from the service provider for the purpose of the complaints process, as the Complainant's identifying information needed to be provided to the service provider to be able to provide a proper response to the Complainant's allegations.

Relationship between anonymity and other IPPs

8.20 Both organisations and individuals can benefit from anonymous transactions. The individual is able to deal with the organisation without giving up control over their personal information and the organisation does not incur any of the obligations under the other IPPs that follow from collection of personal information.

8.21 Where organisations intend to collect and use anonymous data, they should ensure the information is not reasonably identifiable or reasonably capable of being re-identified through, for example, matching the information to other datasets. See 'De-identification in practice' in Key Concepts.

8.22 Providing an anonymity option is also consistent with IPP 1.1, which states that organisations should not collect personal information unless it is necessary for one or more of their functions or activities. If an organisation can achieve its function or activity without collecting personal information and allow an individual to remain anonymous, it should do so.

8.23 IPP 8 is also relevant to the conduct of human research under IPP 2.1(c). Limitations around use and disclosure under IPP 2.1(c) are not an issue where researchers collect information anonymously – whether this is directly from the individuals concerned, or indirectly using existing datasets held by other organisations.

8.24 IPP 8 should also be read in conjunction with IPP 5 and IPP 1.3(f). The concepts of openness and

[4] Available on the NZ Privacy Commissioner's website.

transparency in IPP 5, and the requirement to take reasonable steps to notify individuals under IPP 1.3 when collecting information, suggest that if an organisation has an anonymity option, it should be offered at the appropriate time to allow the individual to make an informed decision.

Case Study 8C: Communicating when anonymity is not practicable

The Complainant had an anonymous account with Organisation A, and after some time, the card for the account became faulty and required replacement. The Complainant was advised by Organisation A that in order to obtain a replacement card, they would have to provide their personal information.

The Complainant asked Organisation A whether they could purchase a new anonymous card and have the balance of their old account transferred to their new card. Organisation A replied that this was not possible and confirmed there was no way for the Complainant to maintain their anonymity without losing the account balance.

The Complainant complained that Organisation A had failed to give the Complainant the option of not identifying themselves when entering into the transaction (the exchange of the balance on their anonymous card to another card), when it was lawful and practicable to do so.

Organisation A argued it was not practicable for the Complainant to remain anonymous in these circumstances as the balance transfer could not be performed in person. Organisation A explained to the Complainant that their personal information would be kept for a strictly limited purpose and time (to perform the transfer), and securely destroyed once it was no longer required for recordkeeping purposes. The Complainant's personal information would not be linked to the new key.

The Complainant accepted this explanation and the complaint was conciliated. Organisation A agreed to improve the notice it provided to individuals seeking to transfer a balance between anonymous accounts.

This is a good example of:

- an organisation generally offering an anonymous option;
- an organisation demonstrating why, in limited circumstances, anonymity is not practicable; and
- the relationship between IPPs 1 and 8. Better notice about why anonymity was not practicable in these circumstances may have prevented the complaint.

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.

Version control table

Version	Description	Date published
IPP 8 – Anonymity 2019.B	Edits following consultation.	14 November 2019
IPP 8: Anonymity 2019.A	Consultation draft.	16 May 2019
IPP 8: Anonymity (2011)	2011 pdf version.	2011