Office of the Victorian Information Commissioner

IPP 3 – Data Quality

IPP 3 – Data Quality

On this page

3.1 IPP 3 provides that 'an organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.' Its aim is to keep the quality of personal information high. These Guidelines use 'quality' to mean being accurate, complete and up to date.

3.2 Data quality is important because the personal information collected by government informs decisions which affect the lives of individuals and the community. Government decision-making will be better if it is based on accurate, complete and up to date information. This is an important part of protecting individuals' privacy.

Information that an organisation 'collects, uses or discloses'

3.3 IPP 3 requires organisations to take reasonable steps to ensure the quality of personal information at three distinct points in the information lifecycle:

- when personal information is collected;
- when it is used; and
- when it is disclosed.

3.4 Historical information held by an organisation, which is not currently being used or disclosed, does not require constant reasonable steps to ensure its accuracy. However, if the information is used or disclosed at a later point in time, reasonable steps need to be taken at that time to ensure its quality. This is discussed in more detail below, in 'Reasonable steps under IPP 3 throughout the information lifecycle'.

'Accurate', 'complete' and 'up to date'

Accurate

3.5 'Accurate' is not defined in the PDP Act. The ordinary meaning of the word 'accurate' is 'free from error or defect' or 'in exact conformity to truth, to a standard or rule'.[1] Organisations must take reasonable steps to ensure personal information is accurate when it is collected, used and disclosed.

3.6 Inaccuracy for the purposes of IPP 3 includes factually incorrect personal information. For example, misspelt names, wrongly addressed personal correspondence and information attributed to the wrong person will be regarded as inaccurate.

> **Case Study 3A: Surveillance records created about the wrong person[2]**
>
> A Department received a claim for compensation from Person Y. To assess the claim, the Department engaged a Contracted Service Provider (**CSP**) to undertake surveillance of Person Y. The Department gave the CSP a physical description of Person Y. However, the CSP undertook surveillance of the wrong individual, Person X (Person Y's same sex partner).
>
> The surveillance report included detailed personal information about Person X's

[1] Macquarie Dictionary, *Australian Online Dictionary*, http://www.macquariedictionary.com.au.
[2] *Complainant X v Contracted Service Provider to a Department* [2005] VPrivCmr 6.

movements, activities with their children and other activities over a 48-hour period.

The information collected by the CSP was not accurate as the information was about Person X, instead of Person Y.

Inaccurate opinions

3.7 The definition of 'personal information' in s 3 states opinions 'whether true or not' fall within the ambit of the PDP Act. This makes clear the PDP Act applies to inaccurate or untrue information and opinions.

3.8 Opinions are not inaccurate under IPP 3 simply because someone else holds a different opinion. However, opinions may be inaccurate for the purpose of IPP 3 if they are based on bias, ill will or erroneous facts. Incomplete or inaccurate opinions often demonstrate a 'total inadequacy of underlying factual information'.[3] It can be dangerous to rely on opinions based on inaccurate information because they are likely to result in error.

3.9 Organisations can take steps to determine if an opinion is 'inaccurate' or 'incomplete' under IPP 3. Taking into account competing facts or views of relevant parties before reaching a final opinion will usually be enough for the organisation to demonstrate the opinion should be considered 'accurate' or 'complete' under IPP 3. For example, a professional opinion formed on a reasonable basis does not become inaccurate when later information proves the opinion to be false. The opinion was accurate when it was formed and recorded. If it is later relied upon, the organisations must again take steps to ensure accuracy and quality.

Considerations in ensuring accuracy

3.10 Firstly, organisations should ensure information is accurately recorded. Accurate records of opinions should clearly state it is an opinion. If possible, organisations should also record the name of the person holding that opinion.

3.11 When the factual basis of the opinion is found to be flawed, an opinion may need to be updated, as the record might be 'incomplete'. If it is impracticable or inappropriate for the opinion to be updated, it may be reasonable for an organisation to add a note to the record that indicates the opinion is flawed or out of date. If organisations disclose a flawed opinion, the organisation should also point out the flawed basis to recipients.

3.12 Part V of the *Freedom of Information Act 1982* (Vic) (**FOI Act**) provides for the addition of a note to a disputed opinion so that, while the integrity of a file is maintained, the contrary view, perhaps now based on better or more complete factual information, is also available to future decision makers. This is a way to deal with situations in which two appropriately qualified persons give conflicting opinions on the same matter.

3.13 For more guidance on the relationship between IPP 3 and IPP 6 (Access and Correction), see the discussion under 'Data quality and freedom of information (FOI)' below, and IPP 6.

[3] *Leverett and Australian Telecommunications Commission* (1985) 8 ALN N135.

Practical tips to ensure accuracy

Names: Organisations should take care with individual's names and avoid making assumptions about spelling. Names can have varied spellings. When an individual provides their name to an organisation, the organisation should spell it back to the individual to check the record is correct.

Precision: Organisations should be precise when recording information and distinguish fact from opinion. For example, when making notes about a phone call with an individual, the organisation should make the relevant details clear to others who might use the information later. Vagueness and ambiguity will be problematic later.

Check: It is always best to get personal information from individuals themselves. Second hand information should be checked for accuracy. It may have been collected for a different purpose or be less precise than necessary for your purpose.

Warn: If an organisation can't check the quality of the personal information, they should make a note of this to warn the next user that the information still needs checking. This is especially important if the information may be used in a way that could adversely affect the person it is about.

Addresses: Accurate addresses are important to ensure information reaches only the appropriate recipients. A misspelt street name or a wrong house number can result in a letter never reaching its recipient, or someone else might open the letter making the privacy breach worse.

Complete

3.14 'Complete' means 'having all its parts or elements; whole; entire; full'.[4] What is complete depends on the specific information and the context and purpose of collection, use or disclosure. Where incomplete information would be misleading or lead to incorrect decisions, organisations have an obligation to hold, use and disclose complete information.

Case Study 3B: Incomplete address information[5]

The complainant's account fell behind with direct debit payments. The respondent – a finance company - listed the default on their credit rating. The complainant claimed they were unaware they were in default and that the default would be listed on their consumer credit file.

The respondent said it had sent a letter to the complainant at his last known address.

[4] Macquarie Dictionary, *Australian Online Dictionary*, http://www.macquariedictionary.com.au.
[5] *D v Finance Company* [2009] PrivCmrA 4.

However, the respondent company left out enough information from the address it was unlikely the letter would ever reach the complainant. The Australian Privacy Commissioner decided this address was incomplete.

3.15 The purpose and context of a record or database of information will affect what is considered complete or incomplete. Even when an organisation's information is true and correct, it may be incomplete because it leaves out subsequent events or important information. This might also make the information out of date. For example, if a record of parking fines issued by a local council does not also record whether the fines have been paid and the information is used to demand payment or deny other council services, the information might be incomplete. However, if the purpose of this database of internal statistics is about the issuing of parking fines, it may not be necessary to include payment information.

'Up to date'

3.16 'Up to date' for IPP 3 means extending to the present time including the latest facts. Information may be considered out of date where subsequent information becomes available, which renders the earlier information erroneous or out of date. Ensuring records are up to date is largely about ensuring they are not likely to convey a misleading impression to others who view the information.

3.17 Personal information is not out of date simply because it is old. Information about a past event can be an accurate record of the facts known at the time. For example, a birth record stating the weight of a newborn is not out of date simply because time has passed. Other information that never becomes out of date is an individual's birthplace or the fact that they obtained an academic qualification. Time does not change these facts.

3.18 Information becomes out of date when relevant changes mean information no longer accurately represents the present.

3.19 To ensure information is fit for its intended use, organisations may need to replace or delete out of date information, for example, when updating mailing addresses. The need to update old information due to subsequent events or the availability of new information depends on the purpose for which the information is used or disclosed and 'the context in which that information appears'.[6] When organisations are required to retain old information due to recordkeeping obligations, organisations may archive or store the information with a note which says it is out of date.

Case Study 3C: Use of old address information[7]

The complainant moved to a new house and gave their new address to the Agency. The Agency used out of date information and sent correspondence to the old address. The complainant again informed the Agency of their new address and complained to the Australian Privacy Commissioner because they were not satisfied with the Agency's

[6] *Re Hinds and Australian National University* [2012] AATA 495 [51].
[7] *M v Body Corporate* [2010] PrivCmrA 15 (24 December 2010).

response.

Despite the use of out of date information, no breach of the data quality principle was proven because the Agency demonstrated reasonable steps had been taken. These reasonable steps included an organisational policy, regular training for staff on amending personal information and other procedures and the practice of regularly sending forms to individuals to update their details.

'Reasonable steps' to ensure quality

What are 'reasonable steps'?

3.20 IPP 3 requires organisations to take 'reasonable steps' to ensure data quality at multiple stages of the information lifecycle. This is different from a strict requirement to achieve data quality itself. Organisations are not required to take every possible step to ensure quality. An organisation must comply with IPP 3 when it collects, uses and discloses personal information. There are also additional duties under IPP 3 if an organisation keeps a record of the information. Organisations have a duty to consider the quality of the data when and if the information is subsequently used or disclosed.

3.21 The reasonable steps required to ensure data quality will vary in different circumstances. When considering what is reasonable in a specific context, organisations should keep in mind the underlying principle that personal information should be fit for its purpose. Other factors which affect what is reasonable include:

- the nature of the information;
- how recently the information was collected;
- how quickly the information can go out of date;
- who provided the information;
- the purpose for which the organisation uses the information;
- to whom the organisation discloses the information;
- how, and for what purpose, the information will be used by the recipient; and
- the consequences for the individuals concerned if the data is not sufficiently accurate, complete and up to date.

3.22 The nature or type of personal information and the consequences of poor data quality are particularly important when organisations are considering what steps to ensure data quality are 'reasonable'. The incorrect use or disclosure of some information will merely annoy the data subject until it is corrected, for example, misspelling a name or using an incorrect title. Small inaccuracies will normally not cause harm but in some circumstances they may. For example, recording the wrong age may impact on someone's concession entitlements. Other categories of personal information could inconvenience the data subject if the information is incomplete or out of date when it is used, for example a wrong or old address. The potential for harm when there is a delay in receiving wrongly addressed correspondence is small, however, a wrong address could cause the intended recipient missing a crucial deadline due to the delay.

3.23 Certain categories of information may cause serious harm to an individual, if the information is of poor quality. For example, information about an investigation into any allegation of improper behaviour needs to be accurate, complete and up to date. Where an organisation publishes identifying information about disciplinary matters, publications should note the date the information

was ‘accurate at’ or ‘last revised’.

3.24 Where information can have adverse consequences for an individual, greater ‘reasonable steps’ are required of an organisation to meet the requirements of IPP 3. For example, organisations should take appropriate steps to confirm the accuracy of the information they use or the accuracy of facts from which opinions are drawn before making a decision or taking action which will deprive individuals of benefits or result in serious adverse consequences. These consequences can include financial losses, reputational harm and emotional distress (including damage to relationships).

Case Study 3D: Complainant loses membership due to Organisation’s failure to keep data accurate

The Complainant was an employee of Organisation A. The Complainant applied to become an Organisation B member and completed all the relevant training and assessments to become an eligible member.

The Complainant received a call from an Organisation B representative. They informed the Complainant that an Organisation A employee had contacted Organisation B to discuss concerns about the Complainant’s suitability for Organisation B membership. The Organisation A employee had made a range of allegations about the Complainant’s conduct while employed at Organisation A. The Complainant’s application for Organisation B membership was rejected as a result of the disclosure.

Organisation A stated its employee had disclosed information that was provided by a third party (an individual). Organisation A’s employee had not asserted that the information about the Complainant was true but had not checked the basis for the allegations before passing them on to Organisation B.

Organisation A agreed to change its procedures, whereby any individual expressing concerns about an employee’s application to Organisation B would be referred to report them directly instead of via Organisation A.

3.25 For further examples of data quality errors leading to serious harm for individuals, see:

- *Beneficiary complains ACC acted on inaccurate information in cancelling compensation* (Case Note 17749) [1999] NZPrivCmr 13.
- *CYF wrongly noted father had sexual abuse convictions* (Case Note 277483) [2017] NZPrivCmr 3.
- *Sensible Sentencing Trust falsely labels man as paedophile* (Case Note 294302) [2018] NZPrivCmr 6.[8]

3.26 Sometimes a step taken to improve data quality can create new risks. For example, data matching techniques are sometimes used to compare two datasets to improve their accuracy. Mismatches and mistaken identities present a privacy risk. Similarities between names or addresses can lead to cases of mistaken matches and mistaken identity. As a result, it will not always be ‘reasonable’ to engage in data matching exercise for the purposes of updating personal information. Organisations should

[8] Case notes published by the New Zealand Privacy Commissioner are accessible here.

consider whether the privacy risks associated with a proposed 'reasonable step' outweigh the benefits. If they do, it is unlikely to be a reasonable step the agency is obliged to take under IPP 3.

When do reasonable steps need to be taken?

3.27 Reasonable steps to ensure data quality must be taken at multiple points of the information lifecycle. Key times to take reasonable steps to check data quality are collection, use, re-use and disclosure. How often an organisation must reasonably monitor data quality depends on the potential for that type of information to lose quality over time, whether the information is used regularly or constantly and the potential harm if the information is inaccurate, incomplete or out of date.

3.28 When personal information is collected, used immediately for a purpose and subsequently archived it will be less likely the information will need to be thoroughly checked for accuracy. Organisations do not need to constantly check accuracy or monitor data quality when information is effectively dormant.

3.29 When personal information is disclosed, both the disclosing and receiving organisations should check accuracy. Recipient organisations should ask about the quality of the information received as they will usually be in a weaker position to judge data quality. If the recipient organisation is bound by the PDP Act, they will have data quality responsibilities as soon as they receive the information.

3.30 If either a disclosing or recipient organisation later become aware of (significant) data quality issues, it is good practice (although not required by IPP 3) to tell other organisations who have that information. IPP 3 requires organisations to take reasonable steps to ensure data accuracy both when collecting and using and disclosing personal information.

3.31 Different stages of the information lifecycle might require reasonable steps to check quality include collection, recording and transcription, storage and dissemination. Data quality can be especially vulnerable at times of data entry because mistakes can be made when typing. Or, for example, pages can be lost when photocopying. Also, digital data is susceptible to change or loss in ways that paper documents are not. This is partly because technology allows large amounts of digital data to be handled in relatively automated ways.

3.32 Steps that can help organisations maintain data quality include regular checks to assess accuracy of data entry, publishing documents in a read-only format, using encryption to securely transmit data and adopting technologies which record when information is altered or deleted and by whom. Reasonable steps to protect data from unauthorised modification or premature disposal are discussed further under IPP 4 (Data Security). One effective way to check data quality is to ask subjects of information to point out whether any information needs correcting or updating. Collection requirements under IPP 1 can improve data quality for IPP 3.

> **Case Study 3E: Reasonable steps includes educating staff as to data quality responsibilities**[9]
>
> The complainant sent an employee of a government agency their CV and covering letter. That employee then uploaded some of this information to a personal blog and made unfavourable remarks about the complainant's qualifications. The website was public and

[9] *Complainant AY v Public Sector Employer* [2013] VPrivCmr 2.

the complainant only became aware of it five years later.

The actions of the employee were attributed to the agency. Because the agency did not provide evidence of what steps they had taken to educate the employee on their responsibilities under the *Information Privacy Act 2000* (Vic) (the predecessor of the PDP Act), reasonable steps were assumed to not have been taken.

In conciliation, the complainant received a financial offer of compensation from the agency.

Case Study 3F: Reasonable steps includes taking steps to check information accuracy[10]

A couple with young children made a data quality complaint when a childcare centre referred a debt to a collection agency. The couple withdrew their children from the centre because they were concerned about the way it was being run. The centre billed the couple for four weeks of fees and the couple disputed the debt. Eventually the centre listed the debt with a debt collection agency.

The NZ Privacy Commissioner found the child care centre had taken reasonable steps to check the information about the outstanding payment was accurate. Its enrolments terms stated that four weeks' notice was required when removing a child from the centre. The financial management policy said that unpaid fees would be followed up, and if they were not paid within a month, action would be taken – including the use of debt collection agencies.

The centre also advised the couple it would take action to recover the money owed and gave them an opportunity to respond. The couple said they did not think they should pay, based on their safety concerns. The centre considered the couple's reasons for not paying and decided the reasons were not valid. After the couple refused to pay the fees, the centre contacted the debt collector.

IPP 3 in practice

Public registers and online information

3.33 Because personal information on the internet can be easily stored and reproduced elsewhere, more may be required of an organisation to take reasonable steps to ensure data quality. For example, search engines can cache or store information even after it is removed from the public register. To take reasonable steps to ensure data quality, an organisation may need to correct information on websites other than their own.

[10] *Couple says they were wrongly billed for childcare* (Case note 273665) [2017] NZPrivCmr 10.

3.34 To ensure data quality it may be best to only allow online information to be accessed from the organisation's website – the 'official source'. This may involve excluding search engine 'spiders' or 'robots' from indexing the site.

3.35 When organisations regulate particular trades and professions administer information on public registers, they should make sure the information accurately reflects an individual's registration status. For example, the phrases 'de-registered' or 'cancelled' next to a professional's name may have a more negative effect than the phrases 'not current' or 'not currently practising'.

Case Study 3G: Inaccurate public register information retained in search engine and archive's database despite being removed from the 'official source'[11]

The complainant held a licence for a sensitive trade activity. This licence was registered on a public register regulated by a Statutory Entity. Google searches gave results which associated her name with a related sensitive trade activity also regulated by the Statutory Entity. The complainant felt humiliated about being wrongly identified with the incorrect sensitive trade. Further, the public register made it possible for any person to locate the Complainant's phone number and address. The complainant was concerned about the risk of harm that may result from being identified and then located.

Shortly after receiving the complaint, the Statutory Entity removed its register from the internet. However, the complainant advised the Statutory Entity that even though the register had been removed, the old copy of the webpage was still accessible through Google.

The Statutory Entity then contacted the Australian and overseas controllers of Google.com.au to disable the link to the register and have the information removed. The complainant complained to the Privacy Commissioner to request the manner be resolved more quickly.

The Privacy Commissioner declined to resolve the complaint because the Statutory Entity demonstrated they were taking steps to remove the information and the Privacy Commissioner was satisfied these steps were reasonable.

Reasonable steps to ensure quality and law enforcement

3.36 In Victoria, law enforcement agencies are exempt from certain IPPs under s 15 of the PDP Act. However, it is important to remember that s 15 does not exempt law enforcement agencies from their obligations under IPP 3. Data quality of information in the hands of law enforcement agencies is important to ensure profiling and investigations are appropriate and rely on information that is true and correct. This is illustrated in the case of *Zegaj v Victoria Police* (Human Rights) [2018] VCAT 1733.

[11] *Complainant E v Statutory Entity* [2003] VPrivCmr 5.

Case Study 3H: Examples of reasonable steps in a law enforcement context[12]

Victoria Police told the Australian Taxation Office (**ATO**) they were investigating the complainant who was allegedly involved in the cultivation, distribution and sale of cannabis in two disclosures in 2011 and 2012.

VCAT said it was apparent the information was an opinion and that there were only allegations against the complainant.

VCAT accepted the Respondent's statements about investigation and suspicions it held about the Complainant from 2011 and 2012 stating that it 'might fairly be regarded as accurate at that time' and accordingly it did not find that the Respondent had breached IPP 3.1.

VCAT also accepted that Victoria Police records capture information at particular points in time and that 'it would not be appropriate to remove or delete information which records historical events, including when allegations come to nothing and no action is taken. I accept that historical material might be relevant to POI [person of interest] risk assessments and the like so it must be retained, subject of course to the review and updating mentioned…'.

Victoria Police told a member of the Complainant's family (Individual A) that Victoria Police considered the Complainant a 'known criminal identity'. This disclosure was a breach of IPP 3 because Victoria Police could not prove the Complainant was known (as opposed to suspected) to be involved in criminal activity.

It was not reasonable to label the Complainant a 'known criminal identity' because the Complainant had no convictions. Victoria Police stated that its Manual and privacy policies demonstrated that it took reasonable steps to comply with IPP 3. However, VCAT found that the obligation applies to whether the required reasonable steps are taken in relation to individual pieces of personal information. Victoria Police had not checked the basis for or reliability of the intelligence linking the Complainant to Individual A.

Contracted service providers

3.37 Where an organisation outsources functions to a contracted service provider (**CSP**), both parties should work together to ensure data quality. In an outsourcing arrangement, obligations for ensuring data quality should be clearly communicated to both parties and set out in the binding contract underpinning the arrangement. At a minimum, organisations should consider:

- which organisation will control the data;
- which organisation will be responsible for updating it; and
- what obligations will arise where information is found to be out of date, inaccurate or incomplete.

3.38 Importantly, organisations should check the CSP is adequately equipped to meet the obligations

[12] *Zeqaj v Victoria Police* (Human Rights) [2018] VCAT 1733 (20 November 2018).

under IPP 3 and have appropriate procedures in place. For example, this may involve putting in place measures to ensure that data is accurately collected, verified and reviewed and having clear policies in place for the destruction of out of date data (where recordkeeping obligations permit).

3.39 The obligations for organisations and CSPs to ensure data quality in an outsourcing arrangement will differ depending on whether the CSP has assumed direct liability for their obligations under the IPPs, under a State contract in accordance with s 17(2) of the PDP Act. Where a CSP has assumed direct liability for the obligations under the IPPs, they must take reasonable steps to ensure the quality of any data they collect, use and disclose (when performing functions under the State contract). Where the CSP doesn't assume direct liability for the obligations under the IPPs, the outsourcing party (the organisation) will need to take reasonable steps to ensure data quality. This may involve prescribing processes or minimum standards to ensure information is accurately recorded, unreliable data is identified and old data is destroyed in accordance with recordkeeping requirements.

3.40 More detailed guidance on the obligations of CSPs and organisations in an outsourcing arrangement is available in the *Guidelines for outsourcing in the Victorian public sector*, available on OVIC's website.[13]

Data quality and freedom of information (FOI)

3.41 Access to personal information, whether under the FOI Act or under IPP 6 (Access and Correction), can help an organisation comply with IPP 3. Data quality is likely to be higher where individuals can get access to the information which relates to them and seek correction where appropriate.

3.42 Individuals should seek access and correction to personal information under the FOI Act wherever possible, rather than via IPP 6. Section 14(1) of the PDP Act provides that, where a document containing personal information is a document of an agency within the meaning of the FOI Act, then access or correction to the document may only be granted in accordance with the FOI Act.

3.43 The Explanatory Memorandum for the PDP Act states the FOI Act operates in Victoria to provide rights of access or correction for documents held by government. It says that 'in the case of documents held by public sector agencies, the FOI Act will continue to be the only enforceable method of access. This arrangement is affected by clause 14 of the Bill.' This is because it is not the intention of the PDP Act to 'disrupt established systems of access (under the FOI Act) by supplanting them or creating a concurrent system'. Instead, the rights of access and correction under IPP 6 are intended to have limited operation to organisations which are not agencies within the meaning of the FOI Act, for example, CSPs acting under a State contract.

3.44 Section 39 of the FOI Act provides that where a document is released and contains personal affairs information, an individual can request a correction on or amendment to that document, where the individual believes that the document is:

- inaccurate;
- incomplete;
- out of date; or
- would give a misleading impression.

3.45 OVIC has published information about access and correction under the FOI Act.

3.46 Where a CSP holds personal information that is inaccurate, incomplete or out of date, individuals may seek access or correction under IPP 6. IPPs 6.5 and 6.6 require a CSP to take reasonable steps to

[13] See in particular, pages 8-9 and 25-26.

address the data quality issues by amending, correcting, or associating a statement with the record.

3.47 IPP 3 (Data Quality) is different to the FOI Act and IPP 6 (Access and Correction) because it does not place an obligation on an organisation to correct inaccurate personal information. IPP 3 considers if the steps an organisation to ensure data quality were adequate. IPP 3 focuses on whether an organisation has done all it reasonably should to ensure the accuracy of personal information.

> 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 3 – Data Quality 2019.B	Edits following consultation.	14 November 2019
IPP 3: Data Quality 2019.A	Consultation draft.	28 February 2019
IPP 3: Data Quality (2011)	2011 pdf version.	2011