



PRIVATE SECTOR INFORMATION SHEET 28 - NPP 3 Data Quality

Key Messages

This information sheet will assist private sector organisations covered by the *Privacy Act 1988* (Cth) ('Privacy Act') to comply with their obligations under National Privacy Principle 3 ('NPP 3'). NPP 3 requires organisations to take reasonable steps to make sure the personal information they collect, use or disclose is accurate, complete and up-to-date.

Using personal information that is inaccurate, incomplete or out-of-date raises compliance and operational risks for businesses, and can result in adverse consequences for individuals.

At the same time, organisations need to take a balanced approach to data accuracy. For example, data accuracy should not involve unnecessary intrusion on an individual's privacy.

Assessing what are reasonable steps

Organisations that don't take reasonable steps to maintain data quality risk breaching the NPPs and receiving privacy complaints from individuals.

Organisations should consider the following factors when assessing what are reasonable steps in terms of complying with NPP 3:

1. The type of personal information they hold and how it is going to be used and disclosed
2. Whether the information was collected directly from the individual or from a third party
3. Whether certain 'trigger points' provide an appropriate opportunity to recheck the accuracy of information
4. Using internal common sense protocols to audit, identify and correct obvious errors
5. The age of the information
6. Whether it is easy for individuals to correct and update personal information held by the organisation
7. Whether it would impose an inappropriate intrusion on individuals or an unnecessary burden on the organisation
8. What adverse impacts individuals could suffer as a result of inaccurate, incomplete or out-of-date information being used for business activities

In some limited circumstances, where an appropriate balancing of the above factors has been undertaken, reasonable steps may mean taking no steps at all. Organisations would need to determine this on a case by case basis.

NPP 3 and its relationship to other NPPs

The obligations that exist under NPP 3 closely interact with other NPPs. NPP 1 requires organisations not to collect information unless it is necessary for its purposes. NPP 6 provides a mechanism for individuals to obtain access to information held about them and correct that information; and NPP 8 allows individuals to interact anonymously with an organisation where it is lawful and practicable to do so.

There are some things that an organisation can do to make it easier to comply with NPP 3. Firstly, transacting anonymously with individuals where it is lawful and practicable to do so, can reduce the amount of personal information that is collected. Secondly, limiting the collection of personal information to the minimum necessary to complete a transaction. Thirdly, making it as easy as possible for individuals to access and correct their own information.

Background

What is this information sheet about?

This information sheet outlines what reasonable steps in NPP 3 might be in a range of contexts and circumstances. It also explains how NPP 3 interacts with other NPP obligations.

NPP 3 – Data Quality

NPP 3 says that an organisation must take reasonable steps to make sure that the personal information it collects, uses and discloses is accurate, complete and up-to-date.

This information sheet is intended to assist organisations by:

- providing advice about NPP 3 obligations
- listing the key factors that organisations can consider in planning how to manage data quality
- illustrating how the key factors can be applied by using examples
- emphasising the need for a balanced approach to data quality management that takes account of context and circumstances.

Who is this information sheet for?

This information sheet is for private sector organisations that are covered by the Privacy Act. These organisations must comply with the 10 National Privacy Principles ('NPPs') in the Privacy Act when handling personal information.

'Organisations' are defined in section 6 of the Privacy Act to include:

- all businesses with an annual turnover greater than \$3 million
- all private sector health service providers, regardless of turnover
- some small businesses¹

What is personal information?

'Personal information' is defined as information or an opinion, whether true or not, about an individual whose identity is apparent or can be reasonably ascertained from that information.²

¹ For a more detailed explanation refer to the [Private Sector Information Sheet 12](#).

² The full definition is in s6(1) of the Privacy Act 1988.

When does an organisation check that information is accurate, complete and up-to-date?

Organisations are required to take reasonable steps to make sure that personal information is accurate, complete and up-to-date *at the time* of collecting, using or disclosing the information.

How does the Privacy Commissioner determine what are reasonable steps?

The aim of NPP 3 is to prevent adverse consequences for individuals arising from an organisation collecting, using or disclosing inaccurate, incomplete or out-of-date information.

The reasonable steps an organisation takes to comply with NPP 3 will depend on the circumstances.

When considering a complaint about an alleged breach of NPP 3, the Privacy Commissioner will consider what reasonable steps the organisation could have taken in the particular circumstances and what steps they did take.

The Office of the Privacy Commissioner has identified a number of key factors that organisations should consider when assessing what reasonable steps they need to take to comply with NPP 3.

The factors listed below, are not in order of importance, nor do they stand alone.

Rather, organisations should consider together all the issues identified below before deciding what reasonable steps they need to take. In doing this, organisations may need to balance differing factors to determine the most appropriate approach to take in particular circumstances.

1. Type of information held and how it is going to be used and disclosed

The type of information is important when assessing the privacy risks that could arise from inaccurate, incomplete and out-of-date information. For example, higher risks might arise in relation to collecting, using or disclosing

financial information or sensitive information³ such as health information.

Sometimes the context in which information is going to be used or disclosed as well as the type of information is important.

Example: reasonable steps may differ for sensitive information and in different contexts

A general medical practice might need to have a proactive system for checking and updating its clients' address and contact details on a regular basis. There could be serious consequences for individuals if the practice could not contact them to organise and remind them about follow up appointments and treatment, or inform them about test results. In contrast, an online florist might only need to make sure a client's address and contact details are up-to-date when the client places an order.

Inaccurate, incomplete or out-of-date information can lead to unauthorised disclosures or result in uninformed decisions being made by an organisation or by the individual themselves.

2. What was the source of the personal information?

Personal information collected from a third party may be less reliable than if it was collected directly from the individual.

³ Sensitive information is a subset of personal information. Sensitive information is defined in s6 of the Privacy Act to mean:

information or an opinion about an individual's:

- racial or ethnic origin
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual preferences or practices
- criminal record
- health information about an individual
- genetic information about an individual that is not otherwise health information.

It may be necessary to contact the individual to check the accuracy of the information if it was collected from a third party.

Example: checking with the individual about information received from third parties

Tom Smith has an account with the XYZ Gas Company. The company has decided to promote new 'green' customer plans which include wherever possible the issuing of electronic accounts. As part of the marketing campaign for these new 'green' plans XYZ is sending sales representatives out to visit every existing customer.

A sales representative working in Tom's local area calls him to organise a home visit to discuss the new customer plans. They agree on a suitable time but on the day the sales representative visits Tom's house he is not home. The only person at home is Tom's cousin, Amelia, who is staying with Tom while on holidays. The sales representative asks Amelia to provide Tom's email address. Amelia inadvertently gives the sales representative an old address which Tom no longer regularly uses.

XYZ send Tom's next bill to this email address and, as a consequence, Tom misses the payment and has his service disconnected. Tom rings up the Customer Service Manager at XYZ and demands to know why their staff did not check with him before changing the delivery of his billing information. The Customer Service Manager admits the sales representative should have made another time to visit Tom when he was at home.

3. 'Trigger points' for checking accuracy

The best opportunity to obtain accurate, complete and up-to-date personal information is at the initial point of collection. However information could also be checked and updated at the following trigger points: when additional information is collected and before existing information is to be used or disclosed.

Organisations should determine when these trigger points occur and align their processes accordingly. In most cases, this can be achieved without imposing a burden on an organisation or being unnecessarily intrusive for the individual.

Example: selecting an appropriate trigger point to check data accuracy

For many internet businesses an appropriate trigger point to confirm the accuracy of personal information held in their records is when a customer places an order.

By giving customers the ability to change, and prompting them to update their name and contact details whenever they place an order, businesses are making it easy to keep information up-to-date and accurate in a way that is neither intrusive nor burdensome.

4. Using internal common sense protocols for checking accuracy

Internal protocols and processes can assist organisations in keeping personal information accurate, complete and up-to-date.

Systems programs that identify potential anomalies (such as likely spelling mistakes or incomplete address fields) when personal information is entered or regular data audits are ways in which an organisation can identify and correct obvious errors relatively easily.

Other measures organisations can take include adequately training staff about the privacy obligations of the business and implementing internal procedures which verify the accuracy of data collected, used or disclosed.

Adopting appropriate internal protocols and processes assists businesses in actively minimising their privacy risks and preventing adverse consequences for individuals arising from inaccurate, incomplete or out-of-date information.

Example: internal common sense protocols

Susan and Barry have moved house and ask their bank to change their address. The bank changes their residential address but not their postal address. As a result bank statements for their credit card account are still sent to their old postal address.

This error could have been avoided if the bank's customer system prompted staff at the same time to check whether the postal address for Susan and Barry's accounts should also be changed.

5. How old is the information?

The quality of some personal information is likely to be compromised over time.

If the personal information was collected a long time ago and has not been used since, it may be inaccurate, incomplete or out-of-date.

If the information will be used some time in the future it should be checked prior to using or disclosing it. If it is unlikely that the information will be used again, the organisation should consider whether to delete it, after first checking whether any legal retention periods apply.⁴

Example: risks using old information

Jim rented a property through real estate agency A in 1996. In early 1997 the Residential Tenancy Tribunal issued an order against Jim relating to his rental agreement with real estate agency A. Several years later management of the property Jim was renting was transferred to real estate agency B.

Without checking the currency or accuracy of the tribunal order, real estate agency B listed Jim on a tenancy database in 2002. Jim made a complaint to the Privacy Commissioner, claiming the default listing on the tenancy database was not current or accurate.

When the Office assessed Jim's complaint, the Privacy Commissioner found that the information recorded on the database related to conduct that had occurred a long time ago. Due to the passage of time, the information on the database no longer accurately reflected the risk Jim posed as a tenant.

As such, the tenancy database company before making the listing should have taken additional steps to find out if the tribunal order was still current and accurately reflected the risk Jim posed as a tenant. Instead, it just relied on the fact that the tribunal order was still enforceable.

⁴ Under NPP 4.2 an organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP 2 – see the [NPP Guidelines](#) for further information.

6. How easy is it for individuals to correct and up-date personal information held by organisations?

Organisations should consider whether there are mechanisms in place that allow individuals to correct their own information. For example, many organisations have online programs that allow individuals to update their own personal information.

These programs may give the organisation a greater level of confidence about how accurate, complete and up-to-date client information is. However, organisations should not rely solely on these mechanisms.

It is also important that organisations have appropriate security measures in place to prevent unauthorised access and changes.

7. Balancing privacy risks

Organisations should take a balanced approach to complying with NPP 3. In meeting their data quality requirements there may be limits on the type of information an organisation should collect. Practically, this means organisations should balance the privacy risks that might arise for individuals with other factors including the compliance burden.

Unnecessary collection and intrusion

Organisations should not consider their obligations under NPP 3 in isolation to other NPP obligations. NPP 1 requires that organisations only collect personal information that is necessary for one or more of their functions or activities.

Collecting personal information to update existing records when those records are no longer being used may be an unnecessary collection. In this circumstance, an organisation's request to update its records could intrude on an individual's privacy.

Example: identifying reasonable limits to collecting information

Matthew visits a large electrical and whitegoods retailer to purchase new kitchen appliances. Matthew is not a regular customer of the store and has only made one other purchase - a new washing machine which he bought about 18 months ago.

Matthew decides to have the new kitchen appliances he has chosen delivered. The salesperson at the store asks Matthew to confirm the delivery details that they already

have for him on their customer service system are up-to-date.

Matthew confirms his address and a contact telephone number but the salesperson then asks him for further details such as his age, marital status, number of dependents and annual income.

When Matthew queries why it is necessary for him to supply this information for a simple delivery, the sales person tells him the information helps the store build up a profile of its customers so it can offer them more targeted special offers. Matthew feels this is intrusive given he is not a regular customer and cancels the sale.

Managing any compliance burden

Spending considerable resources on data quality systems might not be justified in some circumstances if the organisation, for example, holds personal information that is not sensitive and the privacy risks to the individual are minimal.

However, if an organisation's business activity relates to sensitive information then a more thorough data quality management plan is justified – despite the compliance burden this may incur.

Example: not having an effective data quality management plan

Sarah had surgery for an aggressive form of cancer. The private hospital she used arranged to send reminders to her for check-ups. This worked well for the first year.

When Sarah moved house she rang the hospital's clinic to advise them of her new contact details. The clinic did not have any procedures in place to easily forward this new information to the hospital administration for updating. As a consequence the changes were not passed on to administration.

Sarah did not receive any more reminders at her new address and lost track of when her last visit was. After six months she called the clinic to check. On her next visit the oncologist finds her cancer has returned and is inoperable.

An effective data quality management plan would most likely not have placed too onerous a compliance burden on the hospital and may have led to a better outcome for Sarah.

8. Adverse impacts

Inaccurate, incomplete and out-of-date personal information can cause unnecessary inconvenience or result in more serious consequences for individuals.

Poor quality data can often be misleading and unreliable. The kind of systems needed to maintain the integrity of data quality will depend on the nature of the personal information being collected and the context in which it is being used and disclosed.

Example: Adverse impacts from poor quality information

Keith starts to receive letters and telephone calls at home and work from a debt collection agency. This debt collection agency, acting on behalf of 3X Company (an internet service provider), is requesting payment for an overdue account with 3X Company.

Keith does not have an account with 3X Company. The overdue account related to an individual with the same surname and birth date but with a different first name. Keith tells 3X that their records are wrong and why. He asks 3X to check their records and asks that they stop contacting him until they investigate his claim. However, the debt collector continues to call Keith at work and at home.

Keith feels increasingly harassed and is embarrassed because all his work colleagues are talking about the debt collection calls. Plus he has spent a lot of time trying to resolve this matter, which has impacted on his work and his home life.

Eventually, 3X investigates the matter and discovers that Keith's claim regarding the records is correct. Keith has now made a complaint to the Privacy Commissioner and is seeking compensation.

When will taking reasonable steps mean taking no steps at all?

In certain limited circumstances reasonable steps may mean an organisation does not have to take any steps at all. However, this would need to be determined on a case by case basis.

An organisation in assessing whether or not reasonable steps are necessary to comply with NPP 3 should have regard to the particular circumstances surrounding the collection, use or disclosure of the personal information; the likely consequences to the individual that might result

from an organisation collecting, using or disclosing inaccurate, incomplete and out-of-date information; and the balancing of the key factors identified above.

In some cases the individual would not suffer any adverse outcome if their information was not accurate, complete or up-to-date because they no longer have any active ongoing relationship with the organisation. Further, it may be unduly intrusive for an organisation to verify an individual's personal information with a third party data source when no active ongoing relationship exists.

However, organisations may have other legal obligations to keep the individual's information accurate, complete or up-to-date even though they have no active ongoing relationship.

Example: When taking no steps may be appropriate

Two years ago Jason purchased an electronic navigation device from EEE Ltd, a large electronics retailer. At the time of the purchase Jason decided to join EEE's customer club so he provided the company with his name, address and telephone number.

Since that time, EEE Ltd has sent Jason their monthly customer newsletter. Jason has made no other purchases from EEE Ltd and when Jason changes his address he decides not to inform EEE Ltd.

It may not be necessary, and in some cases it may be inappropriate, for EEE Ltd to take any steps to make sure Jason's personal information is accurate, correct and up-to-date.

This is because there are no serious consequences for Jason if he does not receive EEE's monthly customer newsletter. If EEE Ltd did seek to update Jason's personal information it may be unnecessarily intrusive.

However when Jason decides to open up an account with a new industry superannuation fund and discontinue making contributions to his old fund, the old fund manager requests that he confirms his current address details.

This is appropriate in the circumstances because the old fund manager has an obligation to provide Jason with regular statements about the status of his superannuation account even though he is no longer actively contributing to it.

How does NPP 3 interact with other NPPs?

The balance between NPP 3 Data Quality and NPP 1.1 - Collection must be necessary

NPP 3 needs to be balanced with NPP 1.1 that requires organisations to only collect information that is necessary for their functions and activities.

Generally, an organisation should not collect information on the off chance that it may become useful in the future. By limiting the unnecessary collection of information organisations will reduce the compliance burden associated with keeping information accurate, complete and up-to-date.

NPP 8 Anonymity

Anonymity is an important element of privacy. Where it is legal and practical to do so, organisations should allow individuals to interact anonymously. De-identified information may be sufficient for an organisation's purposes in some cases, especially when the transaction is of a minor nature.

Example: Identifying information is not always necessary

Doreen is shopping online for car insurance and logs onto 4U Insurance Pty Limited's website to obtain an estimate. The website requires Doreen to enter certain information before generating an estimate.

Doreen inputs information about her car (the age, make and model), no claim bonus, age, driving history and address where the car will be garaged. Doreen is happy to enter these details as she believes it is relevant to obtaining the estimate.

However, additional information requested by 4U Insurance requires Doreen to provide her full name and drivers licence number. Doreen does not believe this information is necessary but cannot generate the online estimate without entering these details.

When Doreen calls 4U Insurance to complain she is told their computer systems are set up so estimates can only be produced once the name and drivers licence fields are filled.

Allowing individuals to interact anonymously may mean that no personal information is

collected and therefore no privacy obligations will apply to that information.

NPP 3 Data Quality and NPP 6 Access and Correction

There is a close relationship between NPP 3 and NPP 6. NPP 6 allows individuals to request access to personal information held about them, subject to certain exceptions. NPP 6 also requires organisations to correct personal information that is incorrect or to place a note against the information where there is a dispute regarding its accuracy.

NPP 6 is another mechanism that enables organisations to maintain the data quality of the personal information they hold. Encouraging individuals to exercise their access rights can assist organisations in demonstrating they are taking reasonable steps to comply with their obligations under NPP 3. For more information about the coverage of NPP 6 see our [Private Sector Information Sheet 4](#).

Complex issues may arise when an individual challenges the accuracy of personal information that is based on an opinion, evaluation or diagnosis and seeks to have this information corrected or deleted from their record.

There may be important medical, legal and safety reasons why a health provider would need to keep a complete record containing an opinion, evaluation or diagnosis alongside any correction requested by a patient. Examples of this might be information contained in records relating to psychiatric conditions or sexually transmitted diseases.

The [Guidelines on Privacy in the Private Health Sector](#) contain more detailed guidance on what considerations need to be taken into account when managing sensitive information like this.

Good privacy is good business

Good privacy practice is also good business.

Personal information that is accurate, complete and up-to-date is more likely to benefit an organisation.

Poor handling practices can raise regulatory and operational risks, undermine business productivity and lower the level of customer confidence.

The Office encourages businesses, irrespective of whether they are covered by the Privacy Act, to consider the benefit of introducing practices that will protect the quality of the personal information they handle.

Further information

- [National Privacy Principles](#)
- [Information Sheets](#)
- [Frequently Asked Questions – Health Privacy](#)

Private Sector Information Sheets

Information sheets are advisory only and are not legally binding. The National Privacy Principles in Schedule 3 of the Privacy Act legally bind organisations.

Information sheets are based on the Office of the Privacy Commissioner's understanding of how the Privacy Act works. They provide explanations of some of the terms used in the NPPs and good practice or compliance tips. They are intended to help organisations apply the NPPs in ordinary circumstances. Organisations may need to seek separate legal advice on the application of the Privacy Act to their particular situation. Nothing in an information sheet limits the Privacy Commissioner's ability to investigate complaints under the Privacy Act or to apply the NPPs in the way that seems most appropriate to the facts of the case being dealt with. Organisations may also wish to consult the Commissioner's guidelines and other information sheets.

Office of the Privacy Commissioner

Privacy Enquiries Line **1300 363 992** - local call (calls from mobile and pay phones may incur higher charges)
TTY 1800 620 241 – no voice calls; Fax + 61 2 9284 9666; GPO Box 5218, Sydney NSW 2001.

Private Sector Information Sheet 28
Web HTML and PDF published May 2009
ISBN 978-1-877079-66-5
© Commonwealth of Australia 2009

www.privacy.gov.au