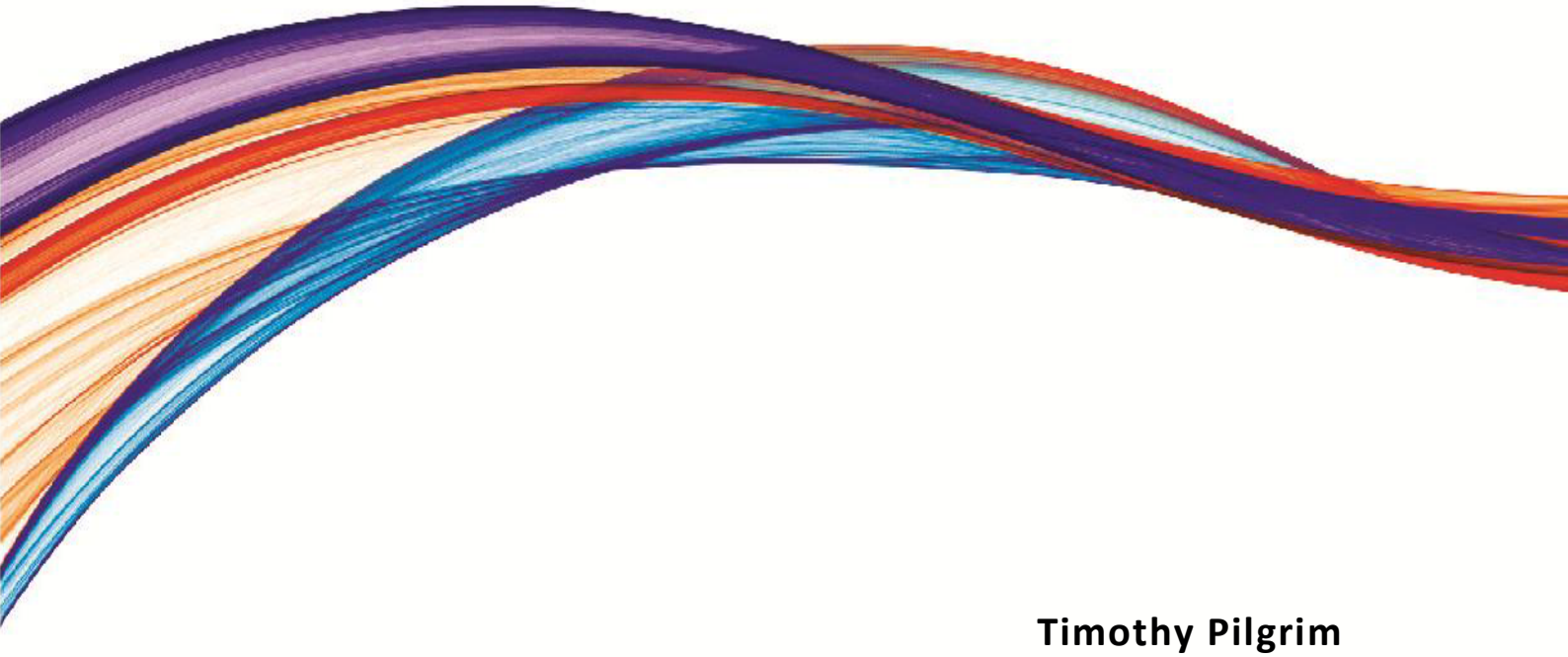
Australian Government

Office of the Australian Information Commissioner

Managing Data Risk

Submission to the Australian Prudential Regulation Authority on the Draft Prudential Practice Guide (PPG 235)

April 2013



Timothy Pilgrim
Australian Privacy Commissioner

Contents

Introduction

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Australian Prudential Regulation Authority (APRA) *Draft Prudential Practice Guide – Managing Data Risk* (PPG 235; Draft Practice Guide).[1]

This submission broadly outlines ways in which the Draft Practice Guide may benefit from amendments to include content regarding the proper handling of personal information in accordance with the *Privacy Act 1988 (Cth)* (Privacy Act)[2] and other legislation.

About the OAIC

The OAIC was established by the *Australian Information Commissioner Act 2010* (Cth) (AIC Act)[3] and commenced operation on 1 November 2010.

The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner.

The former Office of the Privacy Commissioner was integrated into the OAIC on 1 November 2010.

The OAIC brings together the functions of information policy and independent oversight of privacy protection and freedom of information (FOI) in one agency, to advance the development of consistent workable information policy across all Australian government agencies.

The Commissioners of the OAIC share two broad functions:

- the FOI functions, set out in s 8 of the AIC Act — providing access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982* (Cth)[4], and
- the privacy functions, set out in s 9 of the AIC Act — protecting the privacy of individuals in accordance with the Privacy Act and other legislation.

The Information Commissioner also has the information commissioner functions, set out in s 7 of the AIC Act. Those comprise strategic functions relating to information management by the Australian Government.

---

1 Available at: www.apra.gov.au/CrossIndustry/Consultations/Documents/Draft-PPG-235-Managing-Data-Risk-December-2012.pdf.
2 Available at: www.comlaw.gov.au/Details/C2013C00125.
3 Available at: www.comlaw.gov.au/Details/C2010A00052.
4 Available at: www.comlaw.gov.au/Details/C2012C00904.

The Privacy Act

Personal information

The Privacy Act regulates the way in which 'personal information' is handled by most Australian Government agencies and private sector businesses. 'Personal information' is any information about an individual whose identity is apparent, or can reasonably be ascertained, from the information.[5] What constitutes personal information will vary, depending on what can reasonably be ascertained in a particular circumstance, but may include:

- bank account details
- credit card information
- credit reports and credit information files including loan repayment history information
- insurance information
- assets, liabilities, income and expenses
- transaction details regarding investments, loans, or other financial assets
- occupation, salary, tax file numbers (TFNs), ABN or superannuation details
- contact details (telephone, fax and email address).

In the experience of the OAIC, financial institutions generally hold, generate and store large amounts of personal information.

Application of the Privacy Act

The National Privacy Principles

The National Privacy Principles (NPPs) set out in Schedule 3 to the Privacy Act regulate the way that private sector organisations (organisations) handle personal information. The NPPs set out the collection, storage, security, use, disclosure and access and correction obligations of organisations covered by the Privacy Act. In general, the NPPs apply to all businesses and non-government organisations with an annual turnover of more than $3 million, all health service providers, and a limited range of small businesses.[6]

[5] See s 6(1) of the *Privacy Act 1988* (Cth) at: www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249829.

[6] See the OAIC's information sheets on the NPPs at: www.privacy.gov.au/materials/types/infosheets/view/6583.

The Privacy Act also covers more specific matters, such as the use of TFNs[7] and how credit information is handled by credit reporting agencies (CRAs) and credit providers.[8]

Extra-territorial application of the Privacy Act

Section 5B of the Privacy Act provides that the Act may apply to the acts and practices of organisations that occur outside Australia or its external territories. In particular, s5B(3) provides that where an organisation:

- 'carries on business in Australia or an external Territory'
- collects personal information in Australia or an external Territory (i.e., from an individual or individuals physically located in Australia),[9] either before or at the time of the act or practice, or
- holds personal information in Australia or an external Territory, either before or at the time of the act or practice

the Privacy Act will apply to the act or practice.

Any organisation which collects, uses and discloses personal information of Australian citizens or residents and has an 'organisational link' with Australia may be covered by the Privacy Act.[10] As such, even where a business moves their data management responsibilities outside of Australia (offshoring/outsourcing), the acts or practices of that business may still be covered by the Privacy Act.

Privacy enforcement

If an organisation is covered by the Privacy Act, and it breaches the Privacy Act, the OAIC can act against the organisation, either:

- in response to a complaint from an individual, or
- as part of an investigation initiated by the Commissioner of his or her own volition; these are referred to as Own Motion Investigations (OMIs).[11]

The OAIC's usual practice is to attempt conciliation to resolve complaints. Possible resolutions include:

- an apology

---

7 See ss 17 and 18 of the *Privacy Act 1988* (Cth) at: www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249873.

8 See Part IIIA of the *Privacy Act 1988* (Cth) at: www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249890.

9 See the Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 at www.comlaw.gov.au/Details/C2012B00077/Explanatory%20Memorandum/Text.

10 See Privacy Act s 5B at www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249828.

11 See Privacy Act Part V Division 1 at: www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249927.

- a change to the respondent's practices or procedures
- staff counselling
- taking steps to address the matter, for example providing access to personal information, or amending records
- compensation for financial or non-financial loss
- other non-financial options, for example a complimentary subscription to a service.[12]

In the case of a complaint brought by an individual, the Commissioner can make a determination where conciliation does not resolve the matter. Determinations can be enforced, if necessary, in the Federal Court or Federal Magistrates Court.[13]

With respect to OMIs, the OAIC publishes reports of these investigations where there is a public interest in doing so. While currently there are no remedy powers available to the Commissioner in relation to OMIs, additional powers will be available upon the commencement of the privacy reforms in March 2014 (see *Privacy reform*).

Privacy reform

The Australian Privacy Principles

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) (Reform Act) received royal assent on 12 December 2012.[14] The Reform Act will make substantial changes to the Privacy Act, the majority of which will come into force on 12 March 2014. Amongst other changes, the NPPs (and their public sector equivalent, the Information Privacy Principles)[15] will be replaced by a single set of harmonised privacy principles, the Australian Privacy Principles (APPs).[16]

Organisations currently regulated by the NPPs will be covered by the APPs. The OAIC is developing guidance on the application and operation of the APPs.

---

12 See www.privacy.gov.au/complaints/outcomes.

13 See Privacy Act s 55A at www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249956.

14 See *Privacy Amendment (Enhancing Privacy Protection) Act 2012* at: www.comlaw.gov.au/Details/C2012A00197.

15 See Privacy Act, s 14 at www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249862

16 See *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, Schedule 1 at www.comlaw.gov.au/Details/C2012A00197. See also the OAIC's APP fact sheet at www.oaic.gov.au/publications/privacy_fact_sheets/Privacyfactsheet17_Australian_privacy_principles.pdf.

Privacy reform – enforcement implications

From 12 March 2014, the Commissioner will have enhanced enforcement powers, including the ability to:

- make a determination in the case of OMIs
- accept enforceable undertakings
- seek civil penalties in the case of serious or repeated breaches of privacy
- conduct assessments of privacy performance for businesses and Australian Government agencies.

Changes to credit reporting laws

As part of the reforms to the Privacy Act, credit reporting laws will also be amended. Part IIIA of the Privacy Act will be replaced by a new Part IIIA. Changes to credit reporting laws include:

- the introduction of more comprehensive credit reporting, which will allow the reporting of information about an individual's current credit commitments and their repayment history information over the previous two years[17]
- a simplified and enhanced correction and complaints process
- a prohibition on the reporting of credit related information about children
- a prohibition on the reporting of defaults of less than $150
- the introduction of specific rules to deal with pre-screening of credit offers
- the introduction of specific provisions that allow an individual to freeze access to their credit related personal information in cases of suspected identity theft or fraud
- the introduction of civil penalties for breaches of certain credit reporting provisions.

The new Part IIIA also allows the Commissioner to develop a code of practice about credit reporting, called a CR code, to supplement the new credit reporting provisions. Under Part IIIA the Commissioner may request a CR code developer to develop a CR code. The OAIC is currently consulting on guidelines for developing codes.[18]

[17] See the OAIC's fact sheet for more information at: www.oaic.gov.au/publications/privacy_fact_sheets/privacy_fact_sheet16_credit-reporting_repayment-history.html.

[18] See the OAIC's consultation draft on the *Guidelines for developing codes* at: www.oaic.gov.au/news/consultations/code_development/draft_code_development_guidelines.html#_Toc350433059.

Comments on the Draft Practice Guide

Reference to 'personal information'

Financial institutions retain large amounts of personal information, and it is critical that they are aware of their statutory obligations concerning the collection, disclosure, use and storage of personal information.

The OAIC recommends that the Draft Practice Guide expressly refer to 'personal information' as defined in the Privacy Act. The OAIC also suggests that the definition of 'personal information' should be included at the start of the Draft Practice Guide.

Reference to 'privacy'; Definition of 'confidentiality'

There may be a number of points in the Draft Practice Guide where specific privacy implications could be incorporated. Alternatively, the OAIC suggests that detailed consideration be given to what constitutes 'confidentiality', as this could be defined to include 'privacy', e.g. paragraphs [11], [13], [40], [42] and [59] of the Draft Practice Guide.

The OAIC also suggests that the definition of 'confidentiality' should be included at the start of the Draft Practice Guide.

Reference to the NPPs and the APPs

The OAIC recommends that the Draft Practice Guide expressly refer to the obligations regarding the handling of personal information set out in the Privacy Act.

As noted above, organisations (including banks, credit unions and other financial institutions) are subject to the NPPs, which include obligations as to how personal information may be collected, used, managed and disclosed.

The OAIC has highlighted particular obligations under the NPPs and APPs that may be relevant to the Draft Practice Guide below. Further guidance on the NPPs can be found in the OAIC's Guidelines on the National Privacy Principles.[19] The OAIC's draft guidelines on the APPs will soon be released for public consultation.[20] The OAIC is also soon to release guides comparing the requirements of the NPPs with the APPs.

Collection of personal information

The OAIC recommends that the Draft Practice Guide refer to an organisation's obligations under NPP 1.

NPP 1 refers to the collection of personal information and requires, in broad terms, that:

[19] Available at: www.privacy.gov.au/materials/types/download/8774/6582.

[20] For more information regarding the OAIC's consultations, please see the OAIC's consultations page at www.oaic.gov.au/news/consultations.html.

- personal information may only be collected where necessary for a function or activity of the organisation
- collection must not be by unfair or unlawful means, and
- reasonable steps must be taken to provide the individual to which the information relates with notice of specified matters, including the identity of the organisation collecting the information, the purpose of the collection, and the contact details of the organisation.

The OAIC notes that NPP 1 will be replaced by APP 2 which deals with the collection of solicited personal information.

Use and disclosure of personal information

The OAIC recommends that the Draft Practice Guide refer to an organisation's obligations under NPP 2.

NPP 2 relates to the use and disclosure of personal information, and provides that personal information may only be used or disclosed for the purpose for which it was collected (the 'primary purpose'), unless a specified exception applies. Accordingly, an organisation may disclose personal information for the primary purpose for which it was collected. This requires an organisation to have a clearly defined purpose for the initial collection of personal information, which is also consistent with the requirements of NPP 1.

The OAIC notes that NPP 2 will be replaced by APP 6 which deals with the use or disclosure of personal information.

Data security

The OAIC recommends that the Draft Practice Guide refer to an organisation's obligations under NPP 4.

NPP 4 relates to data security and requires organisations to take 'reasonable steps' to protect the personal information that they hold from misuse or loss and from unauthorised access, use, modification or disclosure.

The OAIC has the authority to investigate a possible breach of NPP 4, s 18G(b), or Guideline 6.1(a) of the TFN Guidelines, or conduct an own-motion investigation into an act or practice of an entity covered by the Privacy Act, including when information security has been breached.

The OAIC is currently developing guidance on the reasonable steps with respect to information security that organisations are required to take under the Privacy Act. The guide highlights the importance of preventative measures as part of an organisation's approach to information security. Such measures can assist in minimising the security

risks to personal information. A consultation draft[21] was released for comment in December 2012. A revised draft incorporating comments received during the consultation will be published in due course.

The OAIC has also published a Data Breach Notification Guide[22] which outlines steps that organisations should consider in preparing for and responding to information security breaches, including notifying affected individuals.

The OAIC notes that NPP 4 will be replaced by APP 11, which deals with the security of personal information.

Trans-border data flows

The OAIC notes that the Draft Practice Guide refers to outsourcing and/or offshoring data management responsibilities. The OAIC strongly recommends APRA refer to NPP 9 which relates to trans-border data flows.

Financial institutions in Australia need to comply with the requirements in NPP 9 which outlines the circumstances where an organisation can transfer personal information it holds to an entity outside Australia. Currently, NPP 9 provides that organisations cannot avoid their Privacy Act obligations by sending personal information offshore.

NPP 9 outlines the circumstances in which an organisation can transfer personal information it holds outside Australia. NPP 9 generally prohibits an organisation from disclosing personal information to someone in a foreign country who is not subject to a comparable information privacy scheme. The scheme may be a law of that country regulating personal information-handling, a treaty or other instrument, or a contract.

The exceptions to this rule include where:

- the individual consents to the transfer (NPP 9(b)),
- the transfer is necessary for performing a contract between the individual and the organisation, or to implement pre-contractual measures requested by the individual (NPP 9 (c))
- the transfer is necessary for concluding or performing a contract in the interest of the individual between the organisation and a third party (NPP 9(d))
- the transfer is for the benefit of the individual and the organization can show grounds for a belief that if it were practicable to obtain consent the individual would be likely to give it (NPP 9(e)), or

[21] Available at: www.oaic.gov.au/news/consultations.html#info_security.
[22] Available at: www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html.

- the organisation has taken reasonable steps to ensure that the recipient will handle the information consistently with the NPPs (NPP 9(f)).

The OAIC notes that NPP 9 will be replaced by APP 8 which deals with cross-border disclosures of personal information.

Tax File Number information

The OAIC recommends that the Draft Practice Guide expressly refer to an organisation's obligations concerning tax file number (TFN) information.

The Tax File Number Guidelines 2011 (TFN Guidelines)[23] issued under the Privacy Act regulate the collection, storage, use, disclosure, security and disposal of individuals' TFN information. The Guidelines are legally binding.

Guideline 6 of the TFN Guidelines states that TFN recipients must take 'reasonable steps' to safeguard TFN information. This includes protecting TFN information from misuse and loss, and from unauthorised access, use, modification or disclosure, and ensuring that access to records containing TFN information is restricted to individuals who need to handle that information for legal purposes.

As well as constituting a breach of the TFN Guidelines, unauthorised use or disclosure of TFNs can be an offence under the *Taxation Administration Act 1953* (Cth) (TAA)[24] and attract penalties including imprisonment and monetary fines.

Credit providers and credit reporting agencies

The OAIC recommends that the Draft Practice Guide expressly refer to the obligations for credit providers and CRAs set out under the Privacy Act.

Section 11B of the Privacy Act notes that certain kinds of persons are 'credit providers' for the purposes of the Privacy Act. These include banks (as defined in s 6 of the Privacy Act), and other corporations that provide loans (including issuing by credit cards).

A CRA is a business that operates databases that record information about an individual's credit worthiness, commonly known as 'credit reports'.

Part IIIA of the Privacy Act governs the handling of credit information files, credit reports and other credit worthiness information about individuals by CRAs and credit providers. CRAs can generally only disclose credit reports about individuals to businesses that are credit providers, and only for certain purposes. Similarly, credit providers are subject to rules governing their handling of those credit reports, and other credit worthiness

[23] Available at: www.comlaw.gov.au/Details/F2011L02748.
[24] Available at: www.comlaw.gov.au/Details/C2013C00069.

information. The Privacy Act imposes heavy penalties for unauthorised access to credit information files and credit reports.

CRAs and credit providers also have obligations dealing with quality, access and correction. For example, pursuant to s 18G(a), CRAs must take 'reasonable steps' to ensure that personal information is accurate, up-to-date, complete and not misleading. CRAs and credit providers must also ensure that credit information files and credit reports are subject to security safeguards as are 'reasonable in the circumstances'. For example, pursuant to s 18G(b) of the Privacy Act credit providers must ensure that credit information files and credit reports are protected through adequate security measures against loss, unauthorised access, modification, disclosure or other misuse.

In addition to Part IIIA, CRAs and credit providers must also comply with the binding Credit Reporting Code of Conduct[25].

De-identification of data

The OAIC suggests that the Draft Practice Guide refer to de-identification as a tool for managing data risks.

One useful option for protecting privacy when releasing datasets that contain information about individuals is to de-identify the datasets prior to release. Nevertheless, de-identification is not infallible; and in some circumstances, it may be possible to re-identify data or information by matching it with other datasets or information. It is paramount that de-identification is administered to a high standard, together with appropriate risk management strategies, so that the risk of re-identification can be minimised.

The OAIC is currently developing guidance for Federal Government agencies and organisations on de-identification. This guidance will soon be released for public consultation.[26]

[25] Available at: www.privacy.gov.au/materials/types/codesofconduct/view/6787.

[26] The Australian Government National Statistical Service has developed a range of information sheets on de-identification. These information sheets are designed to explain, and provide advice on, a range of issues around de-identifying data. Please refer to their website: http://www.nss.gov.au/nss/home.NSF/NSS/C8C0B53B4AC18C45CA25793300179082?opendocument.