PRIVACY POLICY

April 2018

Disclaimer and Copyright

While APRA endeavours to ensure the quality of this publication, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this publication.

© Australian Prudential Regulation Authority (APRA)

This work is licensed under the Creative Commons Attribution 3.0 Australia Licence (CCBY 3.0). This licence allows you to copy, distribute and adapt this work, provided you attribute the work and do not suggest that APRA endorses you or your work. To view a full copy of the terms of this licence, visit https://creativecommons.org/licenses/by/3.0/au/

Policy Statement

Purpose

The purpose of this policy is to:

- provide guidance to Australian Prudential Regulation Authority (APRA) staff, secondees and contractors (APRA staff) on the *Privacy Act 1988* (Privacy Act) and the Australian Privacy Principles (APPs) specifically on the collection, storage and use of personal and sensitive information;
- clearly communicate to APRA staff and the public a better understanding of the sort of personal and sensitive information that APRA holds and APRA's information handling practices; and
- enhance the transparency of APRA's operations in relation to holding personal and sensitive information including the notification of eligible data breaches as required under the Privacy Act.

This policy applies to both paper and digital records.

Policy

APRA is the prudential regulator of the Australian financial services industry. It oversees authorised deposit-taking institutions (such as banks, building societies and credit unions), general insurers, life insurers, friendly societies, private health insurers, reinsurance companies, and most of the superannuation industry. APRA also acts as a national statistical agency for the Australian financial sector.

APRA collects, stores and uses a variety of personal and sensitive information in a number of capacities, including as the prudential regulator, a government agency and as an employer and contractor.

The APPs set out standards, rights and obligations in relation to the collecting, handling, holding, accessing and correcting of personal and sensitive information.

The APPs require the collection of personal and sensitive information about an individual only from the individual unless it is unreasonable or impracticable to do so.

APRA as the prudential regulator has collection powers that apply to regulated entities. Personal and sensitive information about an individual will normally be collected from regulated entities and will not be collected from the individual as it is unreasonable or impracticable to do so.

APRA in its capacity as an employer and a contractor will obtain personal and sensitive information about an individual from that individual unless it is unreasonable or impracticable to do so.

APRA is committed to:

- having access to the appropriate information, including personal and sensitive information, to enable APRA to fulfil its prudential regulatory remit and its obligations as an employer, contractor and Australian Government agency;
- ensuring that personal and sensitive information held is accurate and securely maintained; and
- ensuring individuals have a means to access and, if necessary, request the correction of personal and sensitive information held by APRA.

To support this commitment, APRA has an appropriate framework to monitor and manage personal and sensitive information.

Personal information is defined in the Privacy Act to mean:

'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not'.

Sensitive information is defined to mean:

information or an opinion about an individual's:

a) racial or ethnic origin; or
b) political opinions; or
c) membership of a political association; or
d) religious beliefs or affiliations; or
e) philosophical beliefs; or
f) membership of a professional or trade association; or
g) membership of a trade union; or
h) sexual orientation or practices; or
i) criminal record;

that is also personal information; or

a) health information about an individual; or
b) genetic information about an individual that is not otherwise health information; or
c) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
d) biometric templates.

The following principles guide the management by APRA of personal and sensitive information collected:

1. Personal and sensitive information is collected as part of APRA's:
   - prudential regulation – information is only collected when it is reasonably necessary and directly related to prudential supervision;
   - responsibilities as an Australian Government agency; and
   - role as an employer and a contractor.

2. Individuals, other than APRA staff, have the option of not identifying themselves, or of using a pseudonym when dealing with APRA. Individuals must be identified when required by a prudential framework law.[1]

3. APRA staff have the option of not identifying themselves or using a pseudonym when making a public interest disclosure.

4. Unsolicited personal and sensitive information will only be kept if it is relevant to APRA's activities; and then only in accordance with the *Archives Act 1983*.

5. Personal and sensitive information collected during a prudential review will be primarily used for APRA prudential regulation and enforcement-related activities both within Australia and, if necessary after the appropriate safeguards are put in place, overseas, and will ordinarily not be disclosed to external parties.

6. APRA will take the necessary reasonable steps to ensure that both personal and sensitive information collected as part of APRA's activities as an employer and contractor is kept accurate, up-to-date, complete and relevant.

7. APRA will protect personal and sensitive information collected in its activities:
   - from misuse, interference and loss; and
   - from unauthorised access, modification and disclosure.

8. In the unlikely event that an information data breach occurs, APRA must provide notification of the breach to the Office of the Australian Information Commissioner (OAIC) if it is an eligible data breach under the Privacy Act.

9. Where it holds information about an individual, APRA will give that individual access to that information, except where:
   - the information is protected under section 56 of the *Australian Prudential Regulation Authority Act 1998* (APRA Act);
   - access can be refused under the *Freedom of Information Act 1982* (FOI Act) when appropriate; or
   - giving access would be likely to prejudice APRA's enforcement-related activities.

Personal and sensitive information that APRA collects is used:

- for prudential regulation and enforcement activities in respect of the Australian financial services industry;
- to respond to requests under the FOI Act or Privacy Act;
- to provide information to those requesting to be on an APRA mailing list;
- to employ staff, engage contractors and maintain the operations of APRA in compliance with legislation, rules and guidelines;
- to answer inquiries and process complaints made to APRA or respond to inquiries from the Commonwealth Ombudsman; and
- in correspondence with overseas regulators.

[1] Prudential regulation framework law is defined in subsection 3(1) of the APRA Act.

The Chief Security Officer has been delegated authority to approve minor revisions to this policy statement and to approve any standards, procedures and guidelines that are required to support this policy.

Procedure

Purpose

The purpose of the Procedures is to support the Privacy Policy.

The APPs guide the implementation and conduct of this procedure.

Background

The purposes for establishing APRA are set out in section 8 of the APRA Act, which states:

1. APRA exists for the following purposes:
   a) regulating bodies in the financial sector in accordance with other laws of the Commonwealth that provide for prudential regulation or for retirement income standards;
   b) administering the financial claims schemes provided for in the *Banking Act 1959* and the *Insurance Act 1973*;
   c) developing the administrative practices and procedures to be applied in performing that regulatory role and administration.

2. In performing and exercising its functions and powers, APRA is to balance the objectives of financial safety and efficiency, competition, contestability and competitive neutrality and, in balancing these objectives, is to promote financial system stability in Australia.

APRA is an Australian Government agency that employs staff and engages contractors.

In fulfilling its purposes, APRA consults with a number of bodies including:

- regulated entities or the representatives of regulated entities;
- other Government agencies;
- other organisations with which APRA has entered into a Memoranda of Understanding;
- certain overseas regulators and other international bodies involved in prudential regulation policy development;
- members of the public; and
- the OAIC, regarding matters that relate to Privacy Act and Freedom of Information Act functions.

The list of Memoranda of Understanding that APRA has entered into is available on APRA's website.[2]

[2] Refer http://www.apra.gov.au/AboutAPRA/Pages/ArrangementsandMoUs.aspx

Collection and use of personal and sensitive information

APRA collects and uses personal and sensitive information as:

1. a prudential regulator and an Australian Government agency; and
2. an employer and contractor, as set out below.

Personal and sensitive information will not be used for any purpose other than that for which it was collected, unless:

- such use is authorised or required by law, including where the use meets an exception in the APPs; or
- a person has consented to the use.

1. Collection and use of personal and sensitive information as the prudential regulator and Australian Government agency

APRA only collects and uses personal and sensitive information for purposes that are directly related to its functions or activities, and only when exercising its powers as the prudential regulator and as an Australian Government agency and it is necessary for or directly related to such purposes.

Personal and sensitive information is collected from individuals, third parties, Commonwealth, State, Territory and overseas agencies, and public sources. Personal and sensitive information is collected:

- under prudential regulation framework laws;
- under other relevant legislation;
- for law enforcement purposes; or
- for the purposes of APRA's operations.

APRA's collection and use of personal and sensitive information is carried out by lawful and fair means, by exercising its powers and duties to prudentially regulate the financial sector, administer the Financial Claims Schemes provided for under the relevant Acts and develop the administrative practices and procedures to be applied in performing APRA's role as an Australian Government agency.

APRA collects and uses personal and sensitive information:

- where it is required, authorised or for the purpose of a 'prudential regulation framework law'[3];
- where it is required or authorised in any regulation or statutory instrument made under the relevant Acts;
- where it is required or authorised under the:
  - *Privacy Act 1988*;
  - *Freedom of Information Act 1982*; and
  - *Public Governance, Performance and Accountability Act 2013, Rules and guidelines*;
- other relevant Commonwealth legislation and guidelines;

[3] Prudential regulation framework law is defined in subsection 3(1) of the APRA Act.

- from consultations APRA conducts. Personal and sensitive information may be collected as part of the consultation process. APRA publishes all submissions on the APRA website unless a respondent expressly requests APRA in writing that all or part of a submission is to remain in confidence. Such information will not be released unless APRA is under a legal obligation to do so;
- from responses to inquiries and complaints made to APRA;
- from requests to be on mailing lists to provide information about APRA's activities; and
- from information required to be collected and used as a Government agency.

APRA's personal information digest provides detailed information about the kind of personal and sensitive information APRA collects, how that information is collected and the purposes for which it is collected, held, used and disclosed.

APRA's Annual Report contains further information about APRA's collection, handling and disclosure of personal information. APRA's Annual Reports are available on APRA's website.

2. Collection and use of personal and sensitive information of staff, secondees and contractor information

APRA collects and uses personal and sensitive information about its staff, secondees and contractors (and applicants for those positions) for personnel, security and related purposes. That collection is authorised by:

- Commonwealth laws, including:
  - APRA Act;
  - *Safety, Rehabilitation and Compensation Act 1988*;
  - *Work Health and Safety Act 2011*;
  - *Long Service Leave (Commonwealth Employees) Act 1976*;
  - *Maternity Leave (Commonwealth Employees) Act 1973*;
  - *Paid Parental Leave Act 2010*;
  - *Superannuation Act 1976*;
  - *Superannuation Act 1990*;
  - *Superannuation Benefits (Supervisory Mechanisms) Act 1990*;
  - *Superannuation Guarantee (Administration) Act 1992*;
  - *Superannuation Productivity Benefit Act 1988*; and
- other government guidelines and directions.

The personal information relates to the employee, secondee or contractor and may include:

- applications for employment including the employee's résumé; statements addressing the assessment criteria for positions applied for, psychometric assessment reports utilised throughout the selection process and referees' reports;
- written tasks undertaken by the potential employee during the selection process for positions applied for;
- notes from the selection committee during the selection process;
- the employee's employment and contractor's contract, and other records relating to their terms and conditions of employment and engagement;
- details of personal interests and their immediate family members supplied by some employees for the purpose of managing perceived or potential conflicts of interest;
- copies of academic qualifications;
- records relating to the employee's salary, benefits and leave;

- medical certificates or health-related information supplied by an employee, their medical practitioner, or obtained by APRA through an independent medical examination;
- contact details;
- taxation details;
- superannuation contributions; and
- information relating to the employee's training and development, and pay and performance reviews.

APRA's personal information digest provides detailed information about the kind of personal and sensitive information APRA collects, how that information is collected and the purposes for which it is collected, held, used and disclosed.

Personnel and sensitive information of APRA staff, secondees and contractors is disclosed to Commonwealth agencies, law enforcement agencies, health providers and advisors, and other persons authorised by Commonwealth, State or Territory law to receive it. It is also disclosed to other entities to whom a person gives APRA consent to disclose personal and/or security information.

Disclosure of personal and sensitive information including to overseas entities

APRA will not disclose personal information about a person except where it is:

- disclosed subject to a Memorandum of Understanding entered into by APRA;
- in accordance with the law; or
- in accordance with the person's consent.

APRA discloses personal information to certain overseas regulators and other international bodies involved in prudential regulation policy development. Arrangements APRA makes with those overseas recipients regarding the disclosure of this information give appropriate protection over the confidentiality and the use of the personal information.

Accessing or correcting personal and sensitive information

APRA aims to ensure that the personal and sensitive information it holds is accurate, up-to-date and complete.

A person should ensure any personal and sensitive information provided is accurate, up-to-date and complete, and notify APRA if they believe that the information is outdated, inaccurate or incomplete.

A person is entitled to access their personal and sensitive information held by APRA, subject to some conditions and exceptions imposed by law. Requests for access to personal and sensitive information can be made to APRA's Freedom of Information Coordinator.

Requests for correction of personal and sensitive information can also be made by contacting the Freedom of Information Coordinator (details below).

Complaints

Complaints about breaches of the APPs by APRA or requests for assistance may be made to the FOI Coordinator on 02 9210 3000, by email at foi@apra.gov.au or by post to:

Freedom of Information Coordinator
Australian Prudential Regulation Authority
GPO Box 9836
Sydney NSW 2001

APRA prefers that complaints about breaches of APPs be made or confirmed in writing, so it can be sure about the details of the complaints. Generally, APRA will only accept complaints from or on behalf of a person who believes an act or practice of APRA has interfered with their privacy and may have breached a Privacy Principle.

A complaint should identify whether it is about:

- the collection of personal information;
- the use of personal information;
- the disclosure of personal information;
- the security or storage of personal information;
- the accuracy of personal information;
- a refusal to give access to their personal information; and
- a refusal to change or delete personal information.

APRA's Freedom of Information Coordinator normally deals with privacy complaints. Otherwise, if the complaint is about the Freedom of Information Coordinator, the complaint will be dealt with by someone who was not involved in the conduct that is complained about.

APRA will attempt to confirm (as appropriate and necessary) with the person making the complaint:

- their understanding of the conduct relevant to the complaint;
- their understanding of the APPs relevant to the conduct complained of; and
- what they expect as an outcome.

APRA will inform the person making the complaint:

- whether APRA will conduct an investigation;
- the name, title, and details of a contact person; and
- the estimated completion date for the investigation process.

APRA's investigation of a complaint will normally look at matters including:

- Did the alleged conduct occur?
- Why did APRA collect the information?
- Was the information stored by APRA in a 'record' (as defined in the Privacy Act) or a generally available publication?
- Did APRA comply with the relevant APPs or the requirements of the Privacy Act when dealing with the information?

After APRA has completed its enquiries, APRA will contact the person who has made the complaint, usually in writing, to advise the outcome and invite the person to consider if they wish to make a response to APRA's conclusions about the complaint.

If a response is received, APRA will assess it and advise if APRA has changed its view.

If the person making the complaint is not satisfied with the outcome, APRA will advise further options including, if appropriate, the ability for the person to seek a review of APRA's response by the Privacy Commissioner within the OAIC.

Other information relevant to your privacy

Visiting APRA's websites

APRA administers the following websites:

- a public website - www.apra.gov.au;
- a Financial Claims Scheme (FCS) website - https://www.fcs.gov.au/;
- an APRA careers website - https://apracareers.nga.net.au/; and
- and a separate graduate recruitment website - http://apragraduatecareers.com.au

APRA has social media pages hosted by third parties who have their own privacy policies.

Where APRA's websites allow visitors to make comments or provide feedback APRA may collect visitors' contact details. These contact details will only be used for the purpose for which they are provided and will not be added to a mailing list without consent.

Analytics tools and cookies

APRA's web analytics tool, provided by a third party provider, uses cookies to collect or view website traffic information. The information collected may include the IP address of the device used by visitors to the site and information about sites that IP address has come from, the pages and documents accessed on APRA's website and the next site visited. APRA uses the information to maintain, secure and improve the website. Visitors to APRA's website can opt out of the collection of this information by disabling cookies in their browser.

No attempt will be made to identify users or their browsing activities except, in the unlikely event of an investigation, where a law enforcement agency may exercise a warrant to inspect the Internet Service Provider's logs.

Use and disclosure

APRA does not give personal information collected online to other agencies, organisations or anyone else without the person's consent, unless the individual would reasonably expect, or has been told, that information of that kind is usually passed to those agencies, organisations or individuals, or the disclosure is otherwise required or authorised by law.

Security

APRA takes steps to protect the personal information it holds against loss, unauthorised access, use, modification or disclosure, and other misuse. These steps include password protection for accessing the electronic APRA IT systems, securing paper files and physical access restrictions.

When APRA receives information, either via email or any other means, the information is stored in a secure environment.

When no longer required, personal information is destroyed in a secure manner, or deleted in accordance with APRA's Records Disposal Authority or other General Records Authorities authorised under the *Archives Act 1983*.

There are inherent risks associated with the transmission of information via the internet. Although APRA has implemented security measures, it is not possible to provide absolute guarantees as to the security of data provided via an online transmission. APRA has alternative methods of obtaining and providing information. Normal mail, telephone and fax facilities are available.

Contracted service providers

APRA requires all contractors and their subcontractors to comply with the requirements of the Privacy Act. Such agreement between APRA and its contractors ensures that personal information in the possession of a contractor receives the same level of privacy protection as it would within APRA.

Links to other sites

APRA's website has links to other related websites. When transferred to another site, APRA cannot take responsibility for the protection of privacy on the new site accessed through links from APRA's website. Users should familiarise themselves with the terms and privacy policies of the new site.

APRA

APR 2018