

Objective

Privacy and security of Personal Information are global concerns. Individuals expect their Privacy to be respected and their Personal Information to be protected by the organisations with which they interact. The key objective of this Policy is to establish minimum requirements to ensure that Suncorp manages all Personal Information and reports notifiable data breaches to the Office of the Australian Privacy Commissioner, in a manner that is compliant with all applicable Privacy laws and Suncorp policies and standards. Suncorp also maintains a separate Suncorp Group Privacy Policy and a Credit Reporting Policy (external facing), which provides general information to customers about how Suncorp collects, uses, discloses, manages and enables access to customer and credit related Personal Information.

Suncorp may incur harsh penalties for breaches of Privacy, including fines and liability for compensation. Privacy breaches may also lead to significant reputational damage.

Application

This Policy applies to all Employees and Officers when handling Personal Information held by Suncorp.

In addition, where Suncorp relies on a Third Party to manage Personal Information on Suncorp's behalf, Suncorp will ensure that the Third Party complies with the requirements of this Policy.

Policy Statements

1. Suncorp is open and transparent about its Privacy arrangements

Suncorp is accountable for all Personal Information under its effective control and is open and transparent about how it manages Personal Information. In addition to the provision of Privacy Statements referred to below, the Suncorp Group Privacy Policy, which is available on the Suncorp website and each website of Suncorp's different brands where applicable, provides general information about how companies in Suncorp manage Personal Information of customers.

2. All Personal Information must be collected in a lawful manner

Personal Information about an Individual is to be collected only when it is relevant and necessary for Suncorp's functions or activities and only through lawful means. Sensitive Information is collected when it is reasonably necessary for one or more of Suncorp's functions or activities and with the Individual's Consent, whether express or implied. Individuals must have the option of anonymity or the use of a pseudonym unless identification is required by Australian law, or their use is impracticable.

3. Privacy Statements are to be provided to Individuals when collecting Personal Information

In Australia, Functions must have processes to ensure the applicable Privacy Statement is made available to Individuals at or before the time the Personal Information is collected. To ensure consistency, every Privacy Statement must incorporate the minimum requirements detailed in the Privacy Statement Template as applicable to each

jurisdiction. In New Zealand, appropriate disclosures must be made to the Individual in accordance with New Zealand privacy laws.

Each legal entity collecting Personal Information should adopt a single Privacy Statement, or in New Zealand, a single disclosure document covering their activities, subject to the following exceptions:

- A single legal entity carrying out activities that require different Disclosures;
- A brand or marketing strategy that requires multiple Disclosures; and
- A Privacy Statement being specific to a single function or activity.

4. All Personal Information collected must be Used and Disclosed in accordance with the Privacy Statements

Suncorp will not Use or Disclose Personal Information for purposes other than those for which it was collected as outlined in the Privacy Statements or in New Zealand as outlined in corresponding disclosure documentation, except:

- If the Personal Information is subject to the Australian Privacy regime, where the Individual reasonably expects the Personal Information to be Used or Disclosed for a secondary purpose which is related to a purpose for which it was collected. In the case of Sensitive Information, any secondary Use or Disclosure must be directly related to the purpose of collection; or
- If the Personal Information is subject to the New Zealand Privacy regime, Suncorp may Use and Disclose the Personal Information for a secondary purpose only if that secondary purpose is directly related to a purpose of collection; or
- With the Consent of the Individual; or
- As otherwise required or authorised by law.

When Using Personal Information (other than Sensitive Information) for Direct Marketing purposes, Suncorp must provide Individuals with appropriate opt-out mechanisms.

When using Sensitive Information that is subject to the Australian Privacy regime for Direct Marketing, the applicable Function must obtain an Individual's Consent for such Use or Disclosure.

Suncorp must ensure that if the collection of an Australian government identifier, for example a tax file number, is required when completing a business process, these will not be used for any other purpose than for which they were collected.

5. Suncorp will provide the means for Individuals to access their Personal Information where it is lawful to do so

The Suncorp Group Privacy Policy outlines relevant details on how Individuals can obtain access to, and seek correction of, their Personal Information. This also includes information about how the Individual may complain about a Privacy related issue.

Where a request is refused, Suncorp will advise the Individual in writing with an explanation of the refusal and information on the recourse available.

6. The protection of Personal Information must adhere to Suncorp's risk appetite and security protocols

Suncorp will identify and appropriately manage Privacy risks within the parameters of Suncorp and individual Function risk appetite and security protocols when dealing with Personal Information, including any Disclosure to Third Parties, whether based in the relevant jurisdiction or overseas. This includes:

- Completing Privacy Impact Assessments ("PIAs") to identify and ensure appropriate action is taken to manage the Privacy risks and impacts associated with any new initiatives or changes to existing processes relating to products, Platforms, or customers involving the collection, Use or Disclosure of any Personal Information;

- Establishing appropriate processes to ensure the ongoing data quality and integrity of Personal Information held by Suncorp, including processes for reviewing, updating and correcting an Individual's Personal Information upon request;
- Ensuring appropriate processes are in place to protect Personal Information from misuse, interference and loss, as well as unauthorised access, modification or disclosure in accordance with the Security Management Policy, associated security standards, and the IT Acceptable Use Policy;
- Ensuring appropriate processes are in place for training, monitoring and overseeing Third Parties, where they deal with Personal Information on Suncorp's behalf, to ensure that they comply with Privacy obligations applicable to Suncorp;
- Establishing appropriate processes for timely identification, reporting and remediation (where applicable) of Privacy incidents, including regulatory notifications where required;
- Establishing appropriate processes for permanent De-Identification and/or Destruction of Personal Information once it is no longer required for Suncorp's functions or activities; and
- Maintaining adequate monitoring, oversight and reporting arrangements to evaluate the continued effectiveness of Privacy management processes and systems.

7. Suncorp ensures adequate training of, and awareness by, its Employees of Suncorp's Privacy management procedures

Suncorp adequately informs Employees of its Privacy management procedures when dealing with Personal Information, by integrating Privacy compliance into staff training programs. This training will ensure Employees understand their obligations when managing Personal Information and how, in turn, their own Personal Information is managed by Suncorp.

8. Suncorp will adhere to the requirements of the Notifiable Data Breaches Scheme and the European Union (EU) General Data Protection Regulation (GDPR), to the extent the latter applies

Suncorp will have processes in place to comply with the requirements of the Notifiable Data Breaches Scheme. Suncorp will review all privacy incidents in a timely manner to determine whether any individuals are likely to be at risk of serious harm as a result of a Privacy breach. Where Eligible data breaches are identified Suncorp will promptly notify the OAIC and affected individuals.

The GDPR contains data protection requirements that applies to all businesses based in the EU, as well as those based outside the EU who offer products or services to, or otherwise monitor the activity of, people living in the EU. Consequently, some businesses covered by the Australian Privacy Act 1988 and/or New Zealand Privacy Act 1993 must also comply with the GDPR. As Suncorp primarily offers financial products and services to customers in Australia and New Zealand only, the provisions of the GDPR will generally not apply. Policies and procedures that involve the design, implementation or management of processes and systems that handle personal data must have regard to GDPR requirements and when they may be triggered.

Roles and Responsibilities

Employees:

- Be familiar with, and always act in accordance with, the processes relevant to their role and Function that have been developed to protect the Privacy of Individuals;
- Immediately report any potential or actual Privacy incidents to their leader or Risk and Compliance representative;
- Ensure all identified Privacy incidents and breaches are promptly logged in IRIS; and
- Ensure Privacy compliance training is completed on time.

Functions:

- Develop and maintain adequate processes to ensure Personal Information is handled in accordance with this Policy, and Suncorp's Privacy obligations;
- Promote Privacy compliance by integrating Privacy into staff training programs;
- Regularly review and maintain Privacy Statements to ensure they are up to date and consistent with the Privacy Statement Template;
- Regularly review customer privacy disclosures where used in forms, call scripts or other collateral to ensure they remain fit for purpose;
- Complete PIAs for initiatives that involve the collection, Use or Disclosure of Personal Information and meet the thresholds of the PIA Questionnaire; and
- Establish appropriate processes for:
 - Identification, assessment, reporting and management of Privacy risks across the business.
 - Facilitating access to, and correction of, Personal Information;
 - Receiving and responding to Privacy enquiries and complaints; and
 - Managing Privacy incidents in line with the Suncorp Breach Management Standard and applicable Data Breach Response Plans.

Privacy Officer (in Australia and New Zealand):

- Design, implement and oversee Suncorp-wide Privacy compliance and ensure adequate training and awareness arrangements are in place;
- Regularly review the Suncorp Group Privacy Policy to ensure it is up to date;
- In Australia, regularly review and update the Privacy Statement Template having regard to any internal or external developments;
- In consultation with the Australian or New Zealand Regulatory Affairs teams and Privacy Officers as appropriate, liaise with the relevant regulatory body to discuss matters pertaining to Suncorp-wide Privacy matters;
- Provide guidance on the management of any significant Privacy incidents and, where necessary, report to the relevant regulatory body, in accordance with the Incident Management and Breach Management Standards; and
- In New Zealand, the Head of Risk must be made aware and they will advise the Chief Risk Officer on any privacy incidents that may have a Group impact.

CRO (Compliance and Regulatory Affairs teams in Australia and New Zealand):

- Evaluate and advise on PIAs completed. In New Zealand, this is the responsibility of each entity's Privacy Officer;
- Promote a culture that minimises the risk of a Privacy incident occurring through guidance, recommendations and support that reinforces risk management as core to everything Suncorp does;
- Assist Functions to achieve their objectives by providing independent challenge and oversight of risk management activities, capability and performance; and
- Ensure adequate monitoring and reporting of compliance with this Policy and applicable legislation.
- Ensure that risk and compliance teams of the impacted Function/s are made aware of Privacy incidents and the Chief Risk Officer and General Counsel are made aware of any serious and/or significant Australian Privacy incidents in a timely manner.

Internal Audit:

— Provide independent review and oversight of the governance and controls that are in place to manage Privacy compliance.

Policy Exemptions

No exemptions apply to this Policy. Country level policies should only be developed where there are local legal or regulatory requirements to do so.

Policy Breaches

All Policy breaches must be recorded in IRIS in accordance with the Incident Management Standard, with the Policy Owner notified. Non-compliance with this Policy may result in disciplinary action (including termination of employment).

To the extent that this Policy imposes an obligation on Suncorp, it does not form a contractual term, condition or representation

Key Terms

Unless otherwise defined within this Policy, commonly used terms and phrases within this Policy are defined within the Standard Definitions Document. Suncorp has adopted definitions that align to the Australian Privacy Act (1988). To the extent that the definitions in the Australian legislation are inconsistent with New Zealand legislation or inoperative in New Zealand, the definitions in the Privacy Act 1993 will apply in New Zealand.

Consent	May be express or implied consent.
Credit Related Information	Includes the Personal Information of a customer as well as consumer and commercial credit records about a customer such as repayment history, credit default information, loan repayment information, credit opinions or other credit related information as outlined in the Suncorp Credit Reporting Policy.
Data Breach Response Plan	A Data Breach Response Plan sets out the roles and responsibilities involved in managing a data breach. It describes the steps Functions will take if a data breach occurs. Data Breach Response Plans must be in writing to ensure that staff clearly understand what need to happen in the event of a data breach.
De-Identification	Personal Information is de-Identified if the information is no longer about an identifiable Individual or an Individual who is reasonably identifiable. De-Identified information is not Personal Information.
Destruction	Personal Information is Destroyed or disposed of when it can no longer be retrieved.
Direct Marketing	Involves the Use or Disclosure of Personal Information to communicate directly with an Individual to promote goods and services.

Disclosure	The act of making Personal Information known, accessible or visible to a related company within Suncorp or to a Third Party.
Eligible Data Breach	<p>An eligible data breach occurs where:</p> <ul style="list-style-type: none"> — there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that Suncorp holds, — this is likely to result in serious harm to one or more individuals, and — Suncorp has not been able to prevent the likely risk of serious harm with remedial action. <p>Serious harm can include serious physical, psychological, emotional, economic, financial, reputational damage and other forms of serious harm.</p>
Individual	<p>A natural person and could include:</p> <ul style="list-style-type: none"> — a potential or existing customer or Supplier; or — an employee or representative of a corporate customer or Supplier; or — a Third-Party claimant or witness involved in a claim.
Personal Information	<p>Any information or an opinion about an identified Individual, or an Individual who is reasonably identifiable:</p> <ul style="list-style-type: none"> — whether the information or opinion is true or not; and — whether the information or opinion is recorded in a material form or not. <p>Personal Information also includes Sensitive Information and Credit Related Information.</p> <p>Examples of the types of Personal Information Suncorp collects about Individuals include names, postal addresses, email addresses, phone numbers, file notes about likes and preferences.</p> <p>Personal Information includes Unsolicited Personal Information.</p> <p>.</p>
Privacy	The rights and obligations of Individuals with respect to the collection, Use, Disclosure, security, integrity, access, correction and Destruction of Personal Information.
Privacy Statement	A document that Discloses who the Individual is dealing with and some or all of the ways the collecting Suncorp entity collects, Uses, Discloses and manages Personal Information of the Individual.
Privacy Statement Template	The template owned by the Privacy Officer to enable the development of Privacy Statements by Functions.

Sensitive Information	<p>In accordance with the Australian Privacy regime, Sensitive Information means:</p> <ul style="list-style-type: none"> (a) information or an opinion about an Individual's: <ul style="list-style-type: none"> (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record, <p>that is also Personal Information; or</p> (b) health information about an Individual; or (c) genetic information about an Individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.
-----------------------	---

Third Party	Parties that are not related to Suncorp and are contracted to provide services or products to Suncorp.
-------------	--

Unsolicited Personal Information	The Personal Information that has been received by Suncorp where no active steps were taken to collect. Examples of this occurring include employment applications or misdirected mail.
----------------------------------	---

Use	Suncorp Uses Personal Information when it handles and manages that information within its effective control. Examples include accessing, reading, searching of the Personal Information or transferring the Personal Information to other entities or making decisions based on the Personal Information.
-----	---
