PRIME SUPER

Privacy Policy

August 2022

VERSION	8
PREPARED BY (TEAM)	Compliance
DATE APPROVED	August 2022
APPROVED BY AND HOW	Trustee Board through a Board meeting
EFFECTIVE DATE	August 2022
NEXT REVIEW	As required (legislative or business changes)

Version control

ISSUE DATE	VERSION	REVIEWED BY	SUMMARY OF CHANGES
May 2018	6	Compliance	Review
April 2020	7	Compliance	Reformat and minor amendments
August 2022	8	Compliance	Review and insertion of Privacy Impact Assessments and Third Party risk measures.

1 Glossary

APPs	The Australian Privacy Principles
CA	*Corporations Act 2001 (Cth) and Regulations*
Fund	The regulated and registered superannuation fund under SIS known as 'Prime Super'.
Member or "You"	A member of the Fund
Permitted General Situation	Means a "permitted general situation" as defined under section 16A of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).
Permitted Health Situation	Means a "permitted health situation" as defined under section 16B of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).
Prime Super Pty Limited	Prime Super Pty Limited acting either as a trustee of a regulated fund or in its personal capacity or both as the context requires.
Privacy Act	*Privacy Act 1988* (Cth)
Relevant Law	Any Act, Regulation, government policy, contract, trust deed, common law principle, relevant document or precedent as the context requires.
SIS	*Superannuation Industry (Supervision) Act 1993 (Cth) & Regulations*
Trustee, "Us", "Our", or "We"	Prime Super Pty Limited

2 Introduction

This Privacy Policy is produced by Prime Super Pty Limited as Trustee of the Fund in compliance with the *Privacy (Enhancing Privacy Protection) Act 2012* (Cth) which amends the Privacy Act to incorporate the APPs.

In accordance with the APPs, this Policy explains to members and sponsoring employers (participants) of the Fund:[1]

(a) the kinds of personal information that we collect and hold;

(b) how we collect and hold personal information;

(c) the purposes for which we collect, hold, use and disclose personal information;

(d) how an individual may access personal information about them that is held by us and seek correction of such information;

[1] APP 1.4.

(e) how to lodge an enquiry or complaint in relation to privacy and how we deal with these;

(f) our process for disclosing personal information to overseas recipients.

The Fund is subject to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) which, in certain cases, can require that certain information be provided to the Australian Transaction Reports and Analysis Centre (AUSTRAC) or that information be withheld from a person seeking it. Where a conflict exists between a right or entitlement under this legislation and the Privacy Act, the former will generally prevail.

3 What is "personal information" and "sensitive information"

In accordance with section 6 of the Privacy Act:

- ***"personal information" means information or an opinion about an identified individual, or an individual who is reasonably identifiable:***

  (g) whether the information or opinion is true or not; and

  (h) whether the information or opinion is recorded in a material form or not.

- ***"sensitive information"*** means:

  (a) Information or an opinion about an individual's:

  (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;

  that is also personal information; or

  (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.

4 Types of personal information collected and held

4.1 Member and members' dependant's information

We collect and hold personal information that is reasonably necessary for the functions and activities of the Fund,[2] including name, address, date of birth, telephone number, email address, tax file number, occupation, employer, personal health information and nominated beneficiaries, if these details have been provided.

Members may, from time to time, provide their email contact details. Where this occurs we are able to communicate with participants electronically and will hold the email address for this purpose. Where a member has provided their email address and no longer wishes to receive email communications to that address, they can contact us to have the email address deleted or changed.

From time to time, members will be informed that they are able to complete a Nomination of Beneficiaries Form to indicate who should receive their entitlements if they die. The Nomination of Beneficiaries form assists us when deciding who should receive a death benefit. Information contained on the Nomination of Beneficiaries Form is stored by us and may be disclosed to claimants should a member die while a member of the Fund.

4.2 Tax File Number (TFN) information

Collection of TFN is authorised by the relevant law. We are also required by law to ask members to provide their TFN. By providing a TFN we are authorised to use that TFN for the purposes contained in the *Superannuation Industry (Supervision) Act 1993*. Purposes currently authorised include:

(a) Use when taxing eligible termination payments;

(b) Finding and amalgamating members' superannuation benefits where insufficient information is available; and

(c) Passing members' TFN to a relevant State or Commonwealth authority when required by law.

Members are not required to provide their TFN. Declining to quote a TFN is not an offence. However, if a TFN is not provided, either now or later:

(a) The Member may pay more tax on their superannuation benefits and / or contributions than they have to; and

(b) It may be more difficult to find their superannuation benefits if they lose track of them.

The lawful purposes for which a TFN can be used and the consequences of not quoting a TFN may change in future as a result of changes to the relevant law. To provide the Fund with a TFN please contact the Fund on Freecall 1800 675 839.

[2] APP 3.2.

5 Types of personal information collected and held

5.1 Health Information

From time to time, we may receive sensitive information, typically occupation or health information from members when they apply for some types of insurance cover.

Information provided on insurance application forms is collected so that we and the insurer (who will be given the information) can assess a member's eligibility for insurance cover applied for.

If a claim is made for an insurance benefit, information about a member will be both collected from the member's medical practitioners and disclosed to medical practitioners and other experts nominated by the insurer for the purpose of assessing the claim. We or the insurer may also disclose information about the member to other advisers and parties involved in evaluating a claim or the resolution of a complaint related to a claim or insurance benefit.

We will not collect any sensitive information about an individual unless:

(a) the individual consents to the collection of the information (eg. by providing it); and the information is reasonably necessary to manage or administer the Fund; or

(b) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a Permitted Health Situation exists in relation to the collection of the information by us; or

(d) the collection of the information is otherwise permitted or required under the APPs.

6 How we collect personal and sensitive information

Typically, we collect personal information about members, participants and beneficiaries when:

(a) they provide information to us through an application or other form, whether lodged electronically or in paper; and

(b) participants provide information to facilitate membership and / or payment of contributions; and

(c) members and/or participants provide information to the call centre over the phone; and

(d) members update their personal information through their online account; and

(e) information is provided during meetings with regional managers and/or financial planners; and

(f) Information is provided by another complying superannuation fund or Retirements Savings Account; and

(g) Information is provided to the Fund by an Australian government agency or department;

(h) They interact with us through a social media platform; and

(i) Beneficiaries provided their details to the Fund in order to make a claim for death benefits in relation to a member.

Where a participant provides information to facilitate membership and / or payment of contributions that is of a limited nature, we may contact them or members to request additional information.

Typically, we may also collect sensitive information about members when:

(a) they provide information to us through an application or other form, whether lodged electronically or in paper; and

(b) they apply for insurance cover; and

(c) they make a claim for a permanent incapacity or insured benefit; and

(d) they provide information to the call centre over the phone; and

(e) they update their personal information through their online account; and

(f) information is provided during meetings with regional managers and/or financial planners.

7 Why we collect, hold, use and disclose personal and sensitive information

7.1 Primary purpose

We collect personal information about participants that is reasonably necessary for, or directly related to, one or more of the functions or activities of the Fund, including to:

(a) Administer and manage the Fund, which includes accepting contributions from or on behalf of members, investing fund assets, providing insurance cover where relevant, regularly communicating with participants, the payment of benefits and fulfilling legal requirements that apply from time to time.

(b) Conduct research to discover the views of participants on service, existing products or services and new products or services being considered for introduction in the future.

Only information that is reasonably necessary for the functions or activities of the Fund is collected.

We will only collect personal information by lawful and fair means.[3]

We will only collect personal information about an individual from the individual unless it is unreasonable or impracticable to do so.[4]

If participants choose not to provide required information it may mean we are unable to provide superannuation services and that contributions or account balances may have to be transferred to a government run lost money facility.

7.2 Direct marketing and other purposes

[3] APP 3.5.
[4] APP 3.6(b).

Information collected may also be used to provide participants and members with information on other products or services that may be of interest. These products and services are generally provided by third parties, however, third parties will not be provided with participants' and members' personal information, except where we are compelled to do so by law. We may send information on products or services to members from time to time.

We will only provide participants and members with information on other products or services where a real and tangible benefit is offered to participants and members. This will generally be provided as part of our normal communication with participants and members.

From time to time it is possible that a special mail out may occur that only concerns information on other products or services. If participants or members do not wish to receive this type of information, they can contact us and request that no such information be sent.

Refer to Section 11 of this Policy on how we may use personal information for direct marketing purposes.

8 How we deal with unsolicited personal information

If we receive personal information and we did not solicit the information, we must, within a reasonable period after receiving the information, determine whether or not we could have collected the information under APP 3 (as reflected under section7.1of this Policy) if we had solicited the information.[5] We may use or disclose personal information to make this determination.[6]

If we determine that:

(a) we could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

we must, as soon as practicable but only if it is lawful and reasonable to do so:

(a) destroy the information; or

(b) ensure that the information is de-identified.

9 Notifying individuals about the collection of their personal information

9.1 General notifications

In collecting personal information about an individual, we will take reasonable steps to notify the individual, or to ensure that they are aware, of the following matters:[7]

(a) our identity and contact details;

(b) the purposes for which we collect the personal information;

[5] APP 4.1.
[6] APP 4.2.
[7] APP 5.2.

(c) the main consequences (if any) for the individual if all or some of the personal information is not collected by us;

(d) any other entity, body or person (or types) to which we usually discloses personal information of the kind collected;

(e) that our Privacy Policy contains:

(i) information about how the individual may access the personal information about the individual that is held by us and seek correction of such information; and

(ii) information about how the individual may complain about a breach of the APP and how we may deal with such a complaint.

Accordingly, our privacy collection statements will include the above notifications.

9.2 Information from a third party

We will notify an individual if we collect, or have collected, their personal information and the circumstances of that collection.[8]

9.3 Collecting information under the law or a court order

If the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order, we will notify the individual of the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection).[9]

9.4 Disclosing information to overseas recipients

If we are likely to disclose personal information to overseas recipients, we will notify the individual of that fact and the countries in which such recipients are likely to be located, if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.[10]

10 How information held may be used and disclosed

10.1 General use or disclosure of information

Even though we collect information, information is routinely handled by our administrator, which may change from time to time. The administrator has no right to retain information collected by us when it ceases to be the administrator and has no right to use information collected by us of any purpose except to administer the Fund as directed by us.

The Administrator receives, compiles and stores personal information on our behalf, without acquiring a proprietary right in or to the information. Other organisations that are contracted to provide services to us on behalf of the Fund may also receive, compile and store personal information on our behalf, without acquiring rights in or to the information.

These include but are not limited to:

(a) **Auditors** – that check our accounts and the Fund's accounts for compliance with accounting standards and to help prevent fraud.

[8] APP 5.2(b)(i).
[9] APP 5.2(c).
[10] APP 5.2(i) and (j).

(b) **Insurance companies –** that provide insurance cover for Fund members. The Insurer may pass the personal information to medical practitioners and other relevant professionals – for assessing increased insurance applications and/or during the claims process for insurance benefits.

(c) **Third Party Vendors** – that are either engaged by the Administrator or by the Trustee to provide a variety of services.

(d) **Mailing companies** – that compile and send out documents to members such as annual statements.

(e) **Market research companies** – that undertake research and client satisfaction surveys on our behalf and on behalf of the Fund.

(f) **Regulators** - that monitor compliance with legislation such as the Australian Taxation Office (ATO), the Australian Prudential Regulation Authority (APRA), the Australian Securities and Investments Commission (ASIC) and the Australian Transaction Reports and Analysis Centre (AUSTRAC).

(g) **Australian Financial Complaints Authority (AFCA) or any court or tribunal** – in order to resolve member complaints or as required under any relevant court order; and

(h) **Agents and Advisers** – such as lawyers and varied consulting firms (including financial advisers) that provide advice to the Trustee/members on various issues.

Information released to the above and other organisations is kept private and secure. Unless disclosure is required by law, we ensure parties who receive information about participants have appropriate systems in place to comply with applicable privacy laws before permitting them to handle information.

In some instances it may be necessary to release information to other parties, such as a participant, for the purposes of making contributions, or another superannuation fund, to or from which a member would like to transfer money. From time to time disclosure may be required by law. Where we have a legal obligation to disclose information we will disclose the information. This may occur if, for example, we are required to provide information in relation to splitting superannuation interests in the event of marriage breakdown or under a court order. In some cases the law may prevent us from telling members that information has been provided.

For the purposes of considering employment applications, we may disclose personal information from candidates to referees, recruiters and employment screening service providers.

10.2 Use or disclosure of information for a secondary purpose

If we hold personal information about an individual that was collected for a particular purpose (**the primary purpose**), we must not use or disclose that information for another purpose (**the secondary purpose**) unless:[11]

(a) the individual has consented to the use or disclosure of the information; or

(b) the individual would reasonably expect us to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information – directly related to the primary purpose; or

(ii) if the information is not sensitive information – related to the primary purpose; or

(c) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a Permitted General Situation exists in relation to the use or disclosure of the information by us.

11 Direct marketing

From time to time, we may engage in direct marketing activities which involve the use or disclosure of personal information. We will only use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if the following has been complied with.

11.1 Information provided by an individual for the purpose of direct marketing:[12]

(a) we collect the information from the individual; and

(b) the individual would reasonably expect us to use or disclose the information for that purpose; and

(c) the individual has been provided with a simple means to easily request not to receive direct marketing communications from us (i.e an opt out request); and

(d) the individual has not made such a request to us.

11.2 Other situations:[13]

(a) we collect the information from:

(i) the individual and the individual would not reasonably expect us to disclose the information; or

(ii) someone other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

[11] APP 6.1 and APP 6.2.
[12] APP 7.2.
[13] APP 7.3.

(c) the individual has been provided with a simple means to easily request not to receive direct marketing communications from us; and

(d) in each direct marketing communication with the individual we include a prominent statement that the individual may make such a request; and

(e) the individual has not made such a request to us.

11.3 Sensitive information

We may only use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.[14]

11.4 Requests made by individuals

An individual may make requests:[15]

(a) not to receive direct marketing communications from us; and

(b) to provide them with the source of any information being disclosed for direct marketing purposes.

If an individual requests not to receive direct marketing communications from us, we will give effect to the request within a reasonable period after the request is made.[16]

If an individual requests the source of any information being disclosed for direct marketing purposes, we will notify the individual within a reasonable period after the request is made, unless it is impracticable or unreasonable to do so.[17]

An individual will not be charged for making such requests.

12 How personal information may be disclosed to overseas recipients

Before we disclose any personal information about an individual to a person who is not the individual, and who is not in Australia (**overseas recipient**), we will take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.[18]

We will also endeavour to ensure that:

i. the overseas recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the APP protect the information; and

ii. there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme;[19]

[14] APP 7.4.
[15] APP 7.6.
[16] APP 7.7(a).
[17] APP 7.7(b).
[18] APP 8.1.
[19] APP 8.2(a).

13 Security of personal information

Information is securely held in digital form, though paper files also exist particularly in relation to archives, complaints and insurance applications.

13.1 Holding personal information

If we hold personal information, we will take steps as are reasonable in the circumstances to protect that information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.[20]

13.2 Personal information that is no longer required for any purpose

If we hold personal information about an individual and:

(a) we no longer need the information for any legitimate purpose; and

(b) the information is not contained in a Commonwealth record; and

(c) we are not required by or under an Australian law, or court/tribunal order, to retain the information,

we will take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.[21]

13.3 Data breach

We must take reasonable steps to protect the Personal Information we hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. We maintain a Data breach response plan which sets out the processes and procedures to follow in the event of a data breach involving Personal Information held by us

14 How an individual may access their personal information

14.1 Accessing personal information

Generally, members and participants have a right to know what information we hold about them and to ensure it is correct.

Members and participants can contact us to find out what information we hold on them and to correct errors in information held, except where the Relevant Law may prevent access or correction.

Members and participants seeking to access their personal information should contact us to arrange reasonable access. We will respond to a request within a reasonable period and give access to information in the manner requested if it is reasonable and practicable to do so.[22]

14.2 When we may not provide access to personal information

Generally, we are required to give an individual access to their personal information except where:[23]

---

[20] APP 11.1.
[21] APP 11.2.
[22] APP 12.4
[23] APP 12.3.

(a) we reasonably believe that giving access would pose a serious threat to the life, health or safety of any individual, or to public health over public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the us and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal our intentions in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under the Relevant Law or a court/tribunal order; or

(h) both of the following apply:

  (i) we have reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to our functions or activities has been, is being or may be engaged in;

  (ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter;

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within us in connection with a commercially sensitive decision-making process.

14.3 Notification of refusal to give access

If we cannot give an individual access to personal information (due to one of the above reasons) or to give access in the manner requested by an individual, we will give the individual a written notice that sets out:[24]

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal.

14.4 Access charges

In some cases it may be necessary to charge a fee to access or compile certain information. Participants will be informed about any fee before it is charged. Any fee charged will not be excessive and a fee will not apply to the making of the request.[25]

15 Correction of personal information

[24] APP 12.9.
[25] APP 12.8(b).

We will take steps (where applicable) as are reasonable in the circumstances to ensure that:[26]

(a) the personal information that we collect is accurate, up to date and complete; and

(b) the personal information that we use or disclose is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

15.1 Correcting personal information

If:

(a) an individual requests to correct their personal information; or

(b) we are satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading,

we will take steps as reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading. [27]

15.2 Notification of correction to third parties

Where we have previously disclosed this personal information to another APP entity, we will endeavour to notify that APP entity of the correction unless it is impracticable or unlawful to do so.[28]

15.3 Refusing to correct information

If we are unable to correct personal information, we will give the individual a written notice that sets out:[29]

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal.

If requested by the individual, and if it is reasonable in the circumstances, we will associate a statement with the information that it is inaccurate, out of date, incomplete, irrelevant or misleading in a way that will be apparent to users of the information.[30]

15.4 No correction charges

All requests for correction will be actioned within a reasonable period.[31] There will be no fee charged for making a request, for correcting personal information, or for associating a statement with personal information.[32]

---

[26] APP 10.1 and APP 10.2.
[27] APP 13.1.
[28] APP 13.2.
[29] APP 13.3.
[30] APP 13.4.
[31] APP 13.5(a).
[32] APP 13.5(b)

16 Information management and the internet

There are security risks when transmitting and accessing information via the internet. Participants should assess these when deciding whether to use the internet services provided by us. Use of the internet when dealing with us and the Fund is voluntary.

Our web-hosting service provider records certain information from parties who log on to the website including:

(a) server address;

(b) top-level domain name (e.g. .com, .gov, .au);

(c) date and time of the visit;

(d) pages viewed;

(e) downloads; and

(f) site transferred from.

Except where a warrant, court order or the Relevant Law requires it, we will try not to identify users or their browsing activities and will not disclose these to any party.

Our website may use cookies for the purposes of statistical analysis and providing enhanced customer service. A 'cookie' is a piece of information sent to the user's web browser to help the website remember information about the user. We will not send participants unsolicited information on account of them having accessed the website.

17 Privacy complaints and enquiries

To raise an enquiry or complaint, participants should contact our customer service staff on 1800 675 839 or write to us at Locked Bag 5103 Parramatta, NSW 2124 or email administration@primesuper.com.au.

We will investigate the complaint and advise the participant of the outcome within 90-days of receipt. If a participant is dissatisfied with the resolution, he or she can refer the matter to the Office of the Australian Information Commissioner (OAIC) by calling 1300 363 992 or by visiting their website: www.oaic.gov.au.

Please also refer to the *Enquiries and Complaints Policy* which outlines the Trustee's policy and procedures for dealing with an enquiry or a complaint.

18 Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an assessment which identifies how an internal Trustee project is going to impact the personal information held by the Trustee and recommends effective strategies to minimise or eliminate any negative impacts.

This enables the Trustee to:

- identify potential impacts on personal information collected and stored or to be collected and stored in the Trustee's IT systems;
- understand key privacy risks that may arise as a result of a project;
- understand how personal information and its usage flows in a project;

- recommend strategies to mitigate negative privacy impacts; and
- build privacy considerations, security and controls into the design of a project.

The PIA must be completed for projects where personal information is involved with the exception of those that do not propose any changes to existing personal information handling practices. It is the responsibility of the project owner to initiate the initial PIA assessment and to complete a full PIA when required. The Risk and Compliance team will then undertake a compliance check to ensure the APPs are complied with and review the PIA to ensure its adequacy.

19 Third Party Risk

19.1 Due Diligence

A due diligence review is required for third party arrangements, which will include a review of the privacy compliance requirements and will involve the preparation of a PIA.

19.2 Information Security Risk Assessments

Information security, must be implemented for all business projects, and/or third party arrangements, when business changes are to be introduced through the provision of third party services. This is essential in all instances where Trustee/Fund information will be shared with or managed by a third party, regardless of the size or complexity of those services. The Risk and Compliance/ Legal team will consider whether personal information is shared under the contractual arrangements and assess the risk and required controls accordingly.

19.3 Privacy Contractual Clauses

All third party arrangements are reviewed by Risk and Compliance/Legal team to ensure the contract contains the following (non-exhaustive) third party requirements:

- clauses requiring the Trustee to be notified about any event impacting the personal information (such as data loss) as soon as practicable;
- allow the Trustee or another party on its behalf, reasonable access to test the adequacy of the service providers control environment,
- not to do anything that would cause or result in the Trustee breaching the Privacy laws and/or applicable regulations;
- maintain appropriate internal processes and policies to prevent against unlawful use or disclosure of information; and
- appropriate indemnity clauses.