NATIONAL SUPERANNUATION FUND LIMITED

Data Privacy Policy

DOCUMENT CONTROL

DOCUMENT OWNER	**General Manager for Legal Risk & Compliance**
FILE NAME	**Data Privacy Policy**

DOCUMENT VERSION CONTROL

VERSION	REVIEW DATE	AUTHOR
Version 1.0	**21 August 2023**	**Phillomina Nagari**

DOCUMENT ENDORSEMENT & APPROVAL

BOARD/COMMITTEE.	MEETING MINUTE NO	DATE
Audit & Risk Committee	**Meeting No. 103**	**28 November 2023**
Board Meeting	**Meeting No. 155**	**7 December 2023**

DOCUMENT APPROVAL & SIGNOFF

APPROVED	TITLE	DATE	SIGNATURE
Tamzin Wardley	**Chair**		
Rajeev Sharma	**CEO**		

DOCUMENT REVIEW

Effective Date	7 December 2023
Next Review	7 December 2024

This policy will be reviewed as and when it is deemed appropriate, however no less frequently than every 12 months. This Policy review will be undertaken by the General Manager for Information Technology with the support of the Legal Risk & Compliance Division.

Contents

DEFINITIONS

Unless the context otherwise requires, the following definitions, abbreviations and acronyms apply:

Act means the *Superannuation (General Provisions) Act* 2000 (as amended).

ASF means Authorised Superannuation Fund.

Board means Nasfund's board of directors.

Fund means the National Superannuation Fund, an Authorised Superannuation Fund, so authorised by the Central Bank.

MDUF means Nasfund's Member Details Update Form (or the former SF2 form).

Nasfund means the National Superannuation Fund Limited, the licensed trustee of the Fund.

Officer means any other person who, because of his employment, or in the course of that employment has acquired protected information or has had access to protected documents as defined in Section 104 of the Act.

Person means an individual or a body corporate who is, for an individual, a director, executive officer or a manager of a licensee holder or of a subsidiary that is owned or controlled by a licence holder and includes, for a body corporate, a shareholder controller or indirect shareholder controller of a licence holder.

PPM means Nasfund's approved Policies & Procedures Manual (Revised January 2022).

produce means and includes permit access to.

protected document means a document (digital or otherwise) given or produced (whether before or after the commencement of this Act) under or for the purposes of this Act and containing information relating to the affairs of any person other than a document that has already been lawfully made available to the public.

protected information means information data or forecasts disclosed or obtained (whether before or after the commencement of the Act) under, or for the purposes of, the Act and relating to the affairs of any person other than information that has already been made available to the public.

1) INTRODUCTION

This Data Privacy Policy (**policy**) is developed for use by National Superannuation Fund Limited (**Nasfund**), the trustee of the Authorised Superannuation Fund (**ASF**) known as the National Superannuation Fund (**Fund**) to fulfil its fiduciary duty to members.

This policy outlines how protected information (or protected document) is collected, verified, stored, used, disclosed and destroyed by Nasfund, and provides information on member rights regarding member personal information.

2) SCOPE AND APPLICATION

This Policy applies to all directors, employees and contractors of Nasfund.

The ultimate accountability for this Policy rests with Nasfund's Board.

Nasfund's management and employees shall each be responsible for its implementation and compliance.

3) NASFUND RESPECTS MEMBER PRIVACY

Nasfund is required by law to keep secret any protected document or protected information.

Consequently, unless Nasfund is otherwise permitted in making such a disclosure, Nasfund is not required to and will not disclose any protected document or protected information.

4) WHAT CONSTITUTES PROTECTED INFORMATION AND WHAT IS A PROTECTED DOCUMENT?

In essence, a protected document is a document that contains protected information and protected information is any information that is so specific that a person can easily be found from it (identifiable). That is, any member specific data or personal information belonging to a member from which a member's may be easily identifiable.

For Nasfund's purposes, any member specific data collected by Nasfund, such as a member's personal information provided by a member during the member's onboarding process, would be protected information and any document which contains this member specific information would be a protected document. Based on this reasoning, Nasfund's Member Details Update Form (**MDUF**) would be a protected document and any information provided by a member in the MDUF would be protected information.

5) HOW AND WHY DOES NASFUND ACQUIRE PROTECTED INFORMATION?

As specified above, Nasfund acquires protected information from its members when a member sends through a completed MDUF.

From the information collected in these MDUFs, Nasfund is able to carry out one or more of its functions or activities.

6) IS NASFUND REQURED TO DISCLOSE PROTECTED INFORMATION?

Nasfund has a fiduciary duty to its members and is therefore, not compelled to share any protected document or protected information unless otherwise required by law.

Certain situations may require Nasfund to disclose protected information (or protected document) to a third party. In such cases, Nasfund will take reasonable steps to ensure that any such disclosure is permitted by law and Nasfund will further ensure that the third party protects such protected information or protected document in accordance with all applicable PNG Law.

In some situations, Nasfund may also be required by law to provide certain information about a member's membership and interest in the fund to the member's validly (named) nominee, but only upon the relevant member's death.

Nasfund has an obligation to protect and preserve member information and hence, Nasfund may at its sole discretion, refuse to disclose member information if Nasfund deems the request suspicious, intrusive or such that it would be considered as against the member's will.

7) RETENTION, SECURITY AND DESTRUCTION

Nasfund shall retain protected information (or protected document) in hard copy and electronic formats, including cloud storage for a period of 7 years.

Nasfund shall take reasonable security measures to ensure the safety of any protected information (or protected document) which Nasfund may retain (on behalf of its members) from misuse, interference, and loss and from unauthorised access, modification, or disclosure. These include physical (for example, security passes to enter Nasfund's offices and storage of files in lockable cabinets) and technology (for example, restriction of access, firewalls, the use of encryption, user logons, passwords, biometric authentication, and digital certificates) security measures.

In some cases, Nasfund may engage third parties to host electronic data (including data in relation to the services Nasfund provide) on its behalf. These data warehouses may be located overseas. These data warehouses will have in place appropriate security and privacy protocols which not only comply with the privacy laws of the relevant jurisdiction but are to Nasfund's standards and satisfaction.

8) ONLINE SECURITY

As far as reasonably practicable, Nasfund will ensure that its relationship with any third-party service providers (including Nasfund's licensed fund administrator provider and Nasfund's licensed investment manager) must incorporate appropriate protection of member specific data by including protective provisions in respective contracts.

9) WHAT IS A DATA BREACH?

A data breach means a breach of Nasfund's information technology (IT) security framework leading to the accidental or unlawful loss, alteration, unauthorised disclosure of, and access to Nasfund's IT Framework or any of its Contributing members' protected document or protected information (i.e. member specific data or a member's personal information).
A breach may be accidental or deliberate and may take any of the following forms:

- access by an unauthorised third party into the Nasfund IT Framework;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal (Member/Organisational) data to an incorrect recipient;
- computing devices containing members'/Nasfund's personal data being lost or stolen;
- alteration of member personal data without members' permission; and
- the loss of availability of members' personal (specific) data.

A data breach may be broadly defined as a security incident that affects the confidentiality, integrity or availability of the Nasfund's organisational data including any document or information which should otherwise be protected.

In short, data breach occurs whenever any data protected data or protected information (belonging to a member or Nasfund) is accidentally lost, destroyed, corrupted or disclosed without a legal justification or cause.

If an employee becomes aware of a breach, the employee is required to:

i. contain the breach;
ii. assess the potential adverse consequences against the person implicated as well as the effect on the organisation;
iii. assess how serious or substantial the breach is;
iv. ascertain the likelihood of such a breach recurring; and
v. most importantly, report the breach.

10) REPORTING OF DATA BREACH

All Nasfund employees are required to report any actual, potential or suspected data breach to their immediate line supervisor for escalation to Nasfund's Steering Committee which comprises of the following members :

Committee Member	Name
Chief Executive Officer	Rajeev Sharma
General Manager Member & Employer Services	Anne Wilson
General Manager Talent & Culture	Vincent Lialu
General Manager Finance	Debbie Oli
General Manager Investments	Fiona Nelson
General Manager Legal, Risk & Compliance Officer	Lisa Costigan
General Manager Information Technology & Innovation	Arua Taravatu

The Steering Committee will advise on any containment or remedial steps, which will have to be taken.

11)ANNUAL REVIEW OF THIS POLICY

The Board shall review this policy at least annually and amend its provisions to ensure its continued appropriateness.