DATA PROTECTION POLICY

2025

Contents

The DHL Provident Fund (the Fund) is committed to upholding the constitutional right to privacy by ensuring the lawful processing and protection of personal information in compliance with the Protection of Personal Information Act, 4 of 2013 (POPIA) and the Fund's Cyber Risk Management Plan.

This policy outlines the Fund's commitment to managing personal information responsibly and transparently, particularly in the context of its fiduciary responsibilities to members, pensioners, beneficiaries, employers, and all other stakeholders.

During its operations, the Fund collects and processes a wide range of personal information, including but not limited to identity numbers, contact details, employment and remuneration data, medical records, and financial information. Given the sensitive nature of this information, the Fund has an ethical and legal duty to ensure it is processed with the highest standards of data protection and security.

This Data Protection Policy defines the principles, roles, and responsibilities governing the collection, use, storage, sharing, and disposal of personal information. It provides a framework for compliance with applicable laws and aims to reinforce a culture of privacy, security, and accountability within the Fund and among its service providers.

The Board of the Fund acknowledges that it retains ultimate responsibility for ensuring compliance with legislative and regulatory requirements and compliance with the Protection of Personal Information Act (POPIA) and Joint Standard 2 on Cybersecurity.

1. Definitions

Unless the context indicates otherwise, the following definitions apply in this policy:

"Data Breach": A data breach refers to any incident where there is a loss of, damage to, or unauthorised destruction of personal information; unauthorised access to or disclosure of personal information; processing of personal information in a manner not in accordance with the Fund's policies or applicable laws. Examples include, but are not limited to, accidental loss of records, cyber-attacks, ransomware, unauthorised access by employees or third parties, and theft or loss of devices containing personal data.

"Data Subject": The individual to whom personal information relates, including Fund members, beneficiaries, dependants, pensioners, and other identifiable persons.

"Information Officer": The person appointed by the Fund in terms of POPIA to ensure compliance with the Act and to oversee the implementation and enforcement of this policy.

"Joint Standard 2 of 2024": Joint Standard 2 on Cybersecurity and Cyber Resilience establishes comprehensive requirements for financial institutions to enhance their cybersecurity and cyber resilience capabilities. This standard aims to ensure that financial

institutions can effectively manage and mitigate cyber risks, protect sensitive information, and maintain the integrity and availability of their systems.

"Operator": A third party who processes personal information on behalf of the Fund, in terms of a contract or mandate.

"Personal Information": Information relating to an identifiable, living natural person, or where applicable, an identifiable, existing juristic person, as defined in POPIA. This includes, but is not limited to, identity numbers, names, contact details, financial information, employment history, medical information, and biometric data.

"POPIA": Means the Protection of Personal Information Act which is designed to protect personal information processed by public and private bodies. It aims to ensure that personal data is collected, stored, and used responsibly and securely

"Processing": Any operation or activity concerning personal information, whether automated or not, including collection, receipt, recording, organisation, storage, updating, retrieval, use, dissemination, or destruction.

"Responsible Party": The Fund, which determines the purpose of and means for processing personal information.

2. Policy Objectives

The primary objectives of this policy are to:

i. **Ensure Compliance**
Ensure that the Fund complies with the obligations imposed by POPIA, the Joint Standard 2 and any other applicable data protection laws and regulations.

ii. **Promote Accountability and Good Governance**
Embed data protection responsibilities into governance structures, risk management frameworks, and operational procedures.

iii. **Safeguard the Rights of Data Subjects**
Protect the privacy and data rights of Fund members and other stakeholders by ensuring their personal information is processed lawfully, fairly, and transparently.

iv. **Prevent Data Breaches and Misuse**
Implement appropriate technical and organisational measures to protect personal information against accidental or unlawful destruction, loss, alteration, unauthorised access, or disclosure.

v. **Foster Stakeholder Trust**
Maintain the trust of members and stakeholders by demonstrating a commitment to privacy and ethical data handling practices.

vi. **Clarify Roles and Responsibilities**
Define the roles and responsibilities of employees, trustees, service providers, and operators with respect to data protection.

vii. **Enable Effective Risk Management**
Establish controls and processes to manage the risks associated with the collection and processing of personal information.

viii. **Support Data Subject Participation**
Provide mechanisms for data subjects to access, correct, and control their personal information, and to lodge complaints or queries regarding data protection practices.

3. Data Breach Management

The Fund recognises that a data breach can have significant consequences for both the Fund and the data subjects whose personal information may be compromised. To this end, the Fund is committed to the early detection, prompt response, and effective management of all data breaches in compliance with POPIA.

Breach Detection and Reporting
All employees, service providers, or stakeholders must immediately report any suspected or actual data breach to the Information Officer.

Reports should include the nature of the breach, the data involved, when and how it was detected, and any initial containment actions taken.

Breach Response and Containment
Upon receiving a breach notification, the Information Officer will:

- Convene a data breach response team (as applicable).
- Assess the scope and impact of the breach.
- Take immediate steps to contain and mitigate the breach, such as disabling compromised systems, revoking access rights, or isolating affected data.
- Preserve all evidence related to the breach for investigation and legal compliance.

Risk Assessment
A formal risk assessment will be conducted to determine:

- The sensitivity and volume of personal information involved.
- The potential harm to affected data subjects (e.g., identity theft, financial loss, reputational damage).
- The likelihood of the breach resulting in harm.
- The necessity of notifying affected parties and the Information Regulator.

Notification Obligations
In terms of POPIA, the Fund will notify:

- ✓ The Information Regulator of the data breach as soon as reasonably possible after becoming aware of it.
- ✓ Affected data subjects where there is a reasonable belief that the breach may result in material harm to them.

The notification will include:

- ✓ A description of the nature of the breach.
- ✓ Details of the personal information affected.
- ✓ Potential consequences of the breach.
- ✓ Measures taken or to be taken by the Fund to address the breach.
- ✓ Steps data subjects should take to mitigate adverse effects.
- ✓ Contact details for further information or support.

Notifications may be provided via email, telephone, or public announcements, depending on the circumstances.

Remediation and Review

Following the resolution of the breach, the Fund will:

- ✓ Conduct a post-incident review to determine root causes and systemic weaknesses.
- ✓ Implement necessary corrective actions and improve internal controls to prevent recurrence.
- ✓ Review and update relevant policies, procedures, and training programs.
- ✓ Document the breach and the Fund's response for audit and compliance purposes.

Roles and Responsibilities

The Information Officer is responsible for overall breach coordination, regulatory communication, and reporting.

IT personnel, operators and relevant third-party service providers must assist in identifying the breach, conducting forensic investigations, and implementing technical remedies.

All employees and trustees have a duty to report breaches and cooperate with investigation and resolution efforts.

4. Third Party Management

Cognisance must be taken of the fact that the Fund does not directly manage the operations and/or data of the Fund. This is outsourced to third parties who rely on complex technology systems to comply with the respective Service Level Agreements. These information systems are subject to serious threats that can have adverse effects on the Fund's operations, assets, and data if they are exploited or hacked thereby compromising the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems.

A risk assessment employing a risk-based approach, concludes that third party vendors represent the greatest risk. Concomitantly, such vendors will be subject to the following high-level requirements:

a. *The Fund will ensure that any third-party service providers who process or stores sensitive data comply with stringent data protection standards compatible with the Cyber Security Plan. Contracts or service level agreements with third parties, both current and future, must include the requirements contained in the Cyber Plan.*

b) Before engaging third-party service providers after the implementation of this Policy, the Fund will conduct a cybersecurity risk assessment to evaluate the security posture of the vendor. The Fund may also require third parties to undergo periodic security audits or assessments to ensure ongoing compliance with the Fund's data protection standards.

c) Where a vendor is ISO 27001, ISEA 3402 and/or SOC I and II certified, the Fund must ensure that such certification is renewed on expiry.

d) Data shared with third parties will be done on a need-to-know basis, and only after ensuring that adequate contractual, technical, and organisational

5. Review of this Policy

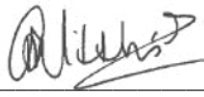
This Data Protection Policy will be reviewed annually by the Board of Trustees or when significant changes occur in the regulatory environment or the fund's operations. The Board will ensure continuous alignment with the fund's POPIA Privacy Policy, Cyber Risk Plan and other related policies.

Signed:  Date 30 May 2025

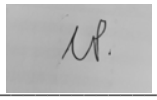
Chairman of the Board

Signed:  Date 30 May 2025

Employer Trustee

Signed:  Date 30/05/2025

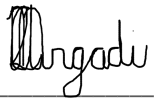
Employer Trustee

Signed:  Date 06 June 2025

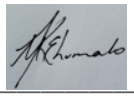
Employer Trustee

Signed:  Date 30 May 2025

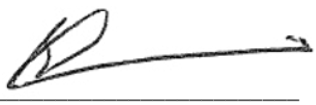
Member Trustee

Signed:  Date 30/05/2025

Member Trustee

Signed:  Date 06 June 2025

Member Trustee

Signed:  Date 25 July 2025

Member Trustee

Signed:  Date 03/06/2025

Principal Officer