INTRODUCTION

This document describes the process followed by Autus Fund Managers (Pty) Ltd (the "Company") when responding to a breach of Personal Information. The process includes notification to the Data Subject and the Company's obligations to the relevant Regulatory Authorities.

REFERENCE DOCUMENTS

- The Protection of Personal Information Act, 2013 (Act no. 4 of 2013) ("POPIA");
- European Union General Data Protection Regulation ("GDPR").
- Personal Information Breach Register;
- Personal Information Protection Impact Assessment; and
- Personal Information Retention Policy.

DEFINITIONS

"Data Subject" means the person to whom the Personal Information relates.

"Operator" means a natural or juristic person, public authority or any other institution which Process Personal Information on behalf of the Responsible Party.

"Personal Information" means any information relating to an identifiable, living natural person, or to the extent applicable, a juristic person. This includes, but is not limited to, information relating to race, gender, sex, pregnancy, marital status, ethnic and social origin, colour, sexual orientation, age, physical or mental health, religion, disability, language, information relating to educational, medical, financial, criminal or employment history, any identifying number, e-mail address, physical address, telephone number, location information, online identifier or biometric Personal Information.

"Personal Information Access Request" means a process designed to ensure the Company complies with its legal obligations when providing Data Subjects with access to their Personal Information.

"Personal Information Breach(es)" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to Personal Information transmitted, stored or otherwise processed.

"Processing" means any activity concerning Personal Information including the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use, dissemination by means of transmission, distribution or making available in any other form, or merging, linking, as well as restriction, degradation, erasure or destruction of Personal Information.

"Regulatory Authority" means the Information Regulator as established by POPIA or any other relevant Regulatory Authority.

"Responsible Party" means a public or private body or any other person that, alone or in conjunction with others, determines the purpose and means for Processing Personal Information.

PERSONAL INFORMATION BREACH RESPONSE

- The Information Officer must ensure that resources, with the relevant skills and knowledge, are established to respond to any Personal Information Breaches.

- Together with the Information Officer, the resources are responsible for ensuring that a Personal Information Breach response process exists and that a response to any Personal Information Breach can be executed timeously.
- The Information Officer has the authority to utilise external parties' services to deal with Personal Information Breaches.

PERSONAL INFORMATION BREACH RESPONSE DUTIES

The Information Officer and the resources responsible for Personal Information Breaches must implement the following processes:

- Validation;
- Investigation;
- Requirements to mitigate;
- Resolution tracking;
- Reporting;
- Coordination with the relevant regulatory authorities; and
- Notification to the relevant Data Subjects.

PERSONAL INFORMATION BREACH RESPONSE PROCESS

- The Information Officer and the reliable resources for Personal Information Breaches must ensure that a breach response process is initiated as soon as anyone notices that a suspected/ actual Personal Information Breach has occurred.
- The Information Officer must ensure that all information relating to the Personal Information Breach is documented.

PERSONAL INFORMATION BREACH NOTIFICATIONS

1. **Notifications from the Operator to the Responsible Party**
   The Information Officer of the Responsible Party must report any actual or suspected breach of Personal Information to the Responsible Party.

   The notification must include the following:
   - A description of the Personal Information Breach;
   - The types of Personal Information affected;
   - The consequences of the Personal Information Breach;
   - The number of Data Subjects affected by the Personal Information Breach; and
   - Processes implemented to remedy any future Personal Information Breaches.

2. **Notifications from the Responsible Party to the Regulatory Authority**
   The Information Officer must:
   - Ensure that the Personal Information Breach is reported to the relevant Regulatory Authority;
   - Perform a Personal Information Protection Risk and Impact Assessment;
   - Record the Personal Information Breach in the Personal Information Breach Register; and
   - Notify the relevant Regulatory Authority of the Personal Information Breach within 72 (seventy-two) hours of its occurrence.

3. **Notification from the Responsible Party to the Data Subject**

The Information Officer must notify Data Subjects of Personal Information Breaches.
The notification must contain the following information:

- A description of the Personal Information Breach;
- Types of Personal Information affected;
- The consequences of the Personal Information Breach;
- Number of Data Subjects affected by the Personal Information Breach; and
- Processes implemented to remedy any future Personal Information Breaches.

Information Officer

Francois Roux

Signature

25/06/2021

Date