

DATAVERSE HOLDINGS (PTY) LTD

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

COMPLIANCE PLAN

1. INTRODUCTION

The Personal Protection of Information Act 4 of 2013 ("POPIA") took effect on 1 July 2020. Responsible parties were granted a grace period until 30 June 2021 to ensure compliance with POPIA.

Dataverse Holdings (Pty) LTD ("Dataverse"), as a Responsible Party, is cognisant of the nature of the civil liability created in terms of section 99(1) of POPIA and that the restricted nature of the defences in terms of section 99(2) create significant risk for entities which may not be adequately addressed by the steps typically taken by entities to limit such risk.

Dataverse understands the importance of protecting the Personal Information for which they are responsible and for ensuring that a high level of compliance with POPIA is achieved.

As a result of the aforementioned, Dataverse designed this compliance plan carefully, to ensure compliance with POPIA.

From the outset, Dataverse has evaluated and shall continually evaluate whether it processes information lawfully. This is achieved by complying with the eight requisites in POPIA, namely:

- **Accountability**: Dataverse ensures that the conditions are complied with at the time of determination of the purpose and meaning of processing and processing itself. In doing so, Dataverse has appointed **Luke Harrison ("Luke")** to be the Compliance Officer. Luke is a knowledgeable employee and has received training from Burger Huyser Attorneys in relation to the compliance aspects of POPIA.
- **Processing limitation**: The processing of personal information is limited to lawful processing in a reasonable manner that does not infringe the privacy of any subject. In this regard, Dataverse, at all times evaluates whether it is processing information which directly relates to the purpose and scope of its instruction from the client and/or whether it is relevant to its

business activities and operations. Moreover, consent is requested from the data subject and information obtained by that data subject, even if such information relates to other data subjects. Data is processed in accordance with an agreement and on a contractual basis, where possible. Likewise, Dataverse also processes information about third parties, as required for purposes of its business activities.

- **Purpose specification**: When collecting information, Dataverse ensures that the information required, specific, defined, and for a lawful purpose, related to the function and business nature of Dataverse. Dataverse, when requesting information and documents, informs the data subject of the purpose of the required documents and information obtained.
- **Further processing limitation**: Dataverse, as an independent contractor, is employed by clients to collect the required information to perform the services as agreed upon in the service level contract. Dataverse equips its clients with the necessary information to make fact-based decisions in its entity, to optimize its services and products. Dataverse ensures that the personal information collected from data subjects are done with the consent and knowledge of the data subject, and in accordance with the privacy policy so disclosed to the data subject on the client's website. Dataverse ensures that the personal information collected and stored, is at all material times a requisite to render the services contemplated in the service level agreement, and processes the information in accordance with the lawful instructions obtained by the client, for the following purposes:
 1. To ensure that the client delivers personalized products that are unique and relevant to the data subject, in line with the limitation imposed on direct marketing as set out in the Act.
 - 1.1. Dataverse guides its clients to ensure that personal information collected, is done so lawfully and with the consent of the data subject;
 2. To optimize any platform, whether a website or social media platform of a client, to be more user-friendly to data subjects and to ensure a seamless experience for the data subject;
 3. To provide the data subject with location-related information and products, such as recommending the branch of the client closest to the data subject;

4. To assist its clients to measure the effectiveness and distribution of its products and services, and to understand the manner in which the data subject, who use the client's services, interact with the client's services, products and platforms;
5. To conduct and support research and innovation on products and services for general social welfare and technological advancement.

Save for processing the personal information collected from the data subject, as indicated and for the purposes as set out above, Dataverse does not share the personal information with any other entity and/or individual, save for the client on whose behalf it has been collected.

- **Information quality**: Dataverse takes steps to ensure that the information collected from data subjects is complete insofar as possible, accurate and continually updated where necessary. Clients are requested to update their information regularly and to inform Dataverse of any changes in personal information.
- **Openness**: Dataverse ensures that the data subject from whom personal information is obtained, is aware of the information collected, the source of the information, the name and address of the responsible party, the purpose for which the information is requested and what law and/or reason if any, prescribes the disclosure of such personal information.
- **Security Safeguards**: Dataverse takes reasonable steps to ensure that the personal information in its possession remains secure. Dataverse safeguards personal information by way of:
 - Utilising virtual private networks ("VPN" to encrypt internet traffic and disguise the individual's online identity;
 - Individual passwords and login details;
 - Limited access for certain individuals to ensure only authorised individuals have access to the data subjects' personal information;
 - Employing Multi-Factor Authentication ("MFA") to ensure that the personal information is secured. The MFA requires an individual to present a combination of two or more credentials to verify the individual's identity to login to the personal information;

- Passwords remain confidential and are not divulged to any other individual nor third parties.
- Dataverse audits its personal information quarterly to ensure that:
 - The personal information stored is still required for the purpose for which it was collected;
 - The personal information is still securely stored;
 - The personal information collected is still accurate and correct. Where it is not, Dataverse contacts the data subject to ensure that the personal information is updated.

If it comes to the attention of Dataverse that there has been a security breach and/or that its information was accessed by an unauthorised person, Dataverse will notify the regulator and the affected data subjects as a matter of priority.

- **Data Subject's Participation**: Dataverse is cognisant of the fact that data subjects have the right to know the nature and extent of any personal information which Dataverse has, pertaining to such data subject and he/she may request the records or description of the information held by means of Dataverse's PAIA manual, which will be made available on request, and which is placed at reception.

Further steps by Dataverse to ensure compliance with POPIA:

STEPS:	DESCRIPTION:	COMPLETED:
	Appointment of Information Officer	Luke Harrison luke@dataverse.africa.com Appointment date: _____
	Review of information on data subjects	Completed annually or regularly with due regard to ongoing instructions.
	Disclosure of Information	Preceded by a request to the data subject for consent to divulge any personal information. Preceded further by a request made in terms of the Promotion of Access to Information Act (PAIA) manual.

	Adequate policies in place	Data subjects are referred to the privacy policy of Dataverse contained on Dataverse's website: Information is at all times processed with due regard to the 8 items listed in this compliance plan. This compliance plan was drafted as a reminder of and to record the process and policies in place in relation to the protection of personal information of data subjects. Information is further obtained and processed by agreement between Dataverse and the data subject, for a specific purpose and in line with the business activities of Dataverse.
	Training	The Information or Compliance Officer underwent training and continues to undergo training in relation to POPIA which training is facilitated by legal professionals at Burger Huyser Attorneys Inc, for purposes of ensuring that he understands the protocols to be implemented as well as the reasons for the protocols and factors that must be considered at all times.

	Appropriate Measures	Dataverse implements appropriate, reasonable technical and organisational measures to secure the integrity and confidentiality of any personal information in its possession or control. In doing so, Dataverse stores information in [] that are secured and stored privately. Dataverse has ensured that only one employee, being the appointed Information Officer, Luke, has access to any personal information collected by Dataverse. Any personal information is safeguarded by way of: 1. Utilising virtual private networks ("VPN") to encrypt internet traffic and disguise the individual's online identity; 2. Individual passwords and login details; 3. Limited access for certain individuals to ensure only authorised individuals have access to the data subjects' personal information; 4. Employing Multi-Factor Authentication ("MFA") to ensure that the personal information is secured. The MFA requires an individual to present a combination of two or more credentials to verify the individual's identity to login to the personal information; 5. Passwords remain confidential and are not divulged to any other individual nor third parties. 6. Dataverse audits its personal information quarterly to ensure that: 6.1. The personal information stored is
--	-----------------------------	--

DataVerse is aware of the consequences of non-compliance with POPIA, specifically:

CRIMINAL	CIVIL
POPIA imposes various criminal offences for non-compliance. Non-compliance with POPIA can result in imprisonment not exceeding 10 years and/or a fine not exceeding R10 million.	In terms of section 99 of POPIA, a data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of POPIA.

