Protection of Personal Information Act (POPIA) Policy

1. INTRODUCTION

POPIA refers to the South African Protection of Personal Information Act which seeks to regulate the Processing of Personal Information and to give effect to section 14 of the Constitution, being the constitutional right to privacy.

The right to protection of "personal information" is not only applicable to natural persons but also extends to legal entities, including companies, communities or other legally recognized organizations. This Policy stipulates Trive Investment South Africa process of processing personal data.

2. DEFINITION:

"**Data subject**" means the person to whom the personal information relates.

"**Responsible Party**" The Party who determines the processing of personal information and the manner of processing it. In terms of POPIA, Trive is the responsible party hereto.

"**Operator**" Person/ third party who process personal information for the responsible party by contract or mandate without coming under his/her/its direct authority.

"**Personal Information**" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.

"**Processing**" means broadly anything done with the Personal Information of Trive's clients and/or employees, including collection, collation, usage, updating, storage, dissemination, retrieval, merging linking, restriction, modification or destruction (whether such processing is automated or not).

"**Information Officer**" Person appointed who is responsible for safeguarding the personal information.

"**Information Regulator**" Responsible for regulating POPI and have the power to act on behalf of data subjects.

3. OBLIGATIONS

Trive's obligations under the POPIA are:

- To only collect information that we need for a specific purpose
- To ensure that the information is relevant and up to date
- Apply reasonable security measures to protect information
  To keep information for as much as we need it and for the period needed.

4. MINIMUM REQUIREMENTS FOR DETERMINING COMPLIANCE WITH POPIA:

- We will be conducting monitoring on all systems in order to understand the data is that is held, where is it held and thereafter identify existing gaps.
- Our Information Officer has ensured that a Compliance Framework is developed, implemented, monitored and maintained.
- A full assessment is conducted of all internal systems users to ensure adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information to establish which profiles needs to be added and to identify what access permissions need to be modified, granted or removed.
- We have proper policies and procedures in place for the dissemination of any information into and out of Trive.
- We have developed a manual which we monitor, maintain and made available as prescribed by POPIA.
- Internal measures are developed coupled with adequate systems to process requests for information or access thereto and internal awareness sessions are conducted regarding the provisions of the Act.
- Upon request, our Information Officer shall furnish copies of the manual to the relevant person upon completing the request forms and payment of fees determined by the Regulator.

5. APPLICATION OF POPIA FOR COLLECTION OF INFORMATION

The below will be considered:

- the legitimate grounds for collecting and using personal data collected,
- the lawful purpose for which data are being collected,
- the limit of processing and prohibiting of further processing,
- the extent of information that is required to prevent any excessive information collection,
- the information retention periods and requirements applicable together with destruction processes and procedures,
- The right of individuals to request such information and query the use thereof,
- The security measures required to prevent the unauthorised or unlawful processing of personal data or access to personal data, including accidental loss or destruction or damage to personal data.

6. EIGHT PROTECTION PRINCIPLES APPLICABLE TO TRIVE

The Act stipulates eight principles and Trive evaluates, develops, implements and maintains personal information processes in accordance with its requirements.

6.1. Accountability

6.2. Processing Limitations

6.3. Purpose Specification

6.4. Further Processing Limitations

6.5. Information Quality

6.6. Openness

6.7. Security safeguards

6.8. Data Subject Participation.

(Please refer to POPIA Manual for the eight (8) principles POPIA conditions and what each of these conditions entails.

7. SAFEGUARDING OUR DATA

POPIA makes it obligatory for Trive to put the security of data first. Therefore, it is important to better protect and manage the personal records and information which we process. This pertains to information of our clients, but it also concerns every employee under our service.

Trive will take reasonable measures using appropriate technical, organization, systems and administrative processes and safeguards to ensure integrity and confidentiality, prevent theft, loss, damage or unauthorized destruction, prevent unlawful access or processing, identify internal and external risks against identified risks.

Trive undertakes to contract with operators who apply POPIA security measures and ensure that such operators report any breaches or reasonable suspicion of breaches to Trive.

As per provisions of POPIA we will report any identified client's information that has been assessed, stolen, lost or corrupted to the Information Regulator. We will further report same to the affected client.

8. RETENTION OF RECORDS

Records will only be retained for as long as is necessary. Section 14(1) provides that "records of personal information must not be kept any longer than is necessary for achieving the purpose for which the information was collected for. Section 14(1) provides that, after which the information must be destroyed, deleted, de-identified or restricted as soon as possible.

We will retain information for a period of 5 years after termination of the business relationship with the client.

9. RIGHTS OF DATA SUBJECTS REGARDING DIRECT MARKETING BY MEANS OF UNSOLICITATED ELECTRONIC COMMUNICATIONS, DIRECTORIES AND AUTOMATED DECISION MAKING

Consumer Consent: Direct Marketing

Request for consumer consent to process personal information for direct marketing purposes.

9.1 FOR THE PURPOSE OF DIRECT MARKETING (SECTION 69): Opting In and Opting out Explained

Section 69 of the POPI Act requires Trive as the Responsible Party to obtain consent from the client before personal information can be processed for the purpose of direct marketing.

- We will provide the client with consent form to sign at the marketing field of onboarding.

- Our Onboarding Client Associates will ensure that the consent form is duly signed and that he/she clearly specifies the method of communication (sms, email or other). This consent form will be saved and securely filed on the clients file.
- We will only send the direct marketing to clients who opted-in for direct marketing. Where client opted-out from direct marketing, we will not send direct marketing to the respective client.

10. CONSEQUENCES OF NON-COMPLIANCE

Trive has appointed its COO as the custodian of personal information.

Section 107 of the Protection of Personal Information Act 4 of 2013 (POPI) provides for penalties of up to R1m and 12-month imprisonment, and R10m and up to 10 years' imprisonment for more serious offences.

Non-compliance with the Act could expose the Responsible Party to a penalty of a fine and/or imprisonment of up to 12 months. In certain cases, the penalty for non-compliance could be a fine and/or imprisonment of up 10 years.

11. CONTACT INFORMATION

The following people are to be contacted for any POPI related queries:

- Information Officer: travis.robson@trive.com
- Deputy Information Officer: Marius.gobler@trive.com

12. REVIEW

Executive Management will formally review the policy every 12 months or as required.