PAIA & POPI Manual

This manual was prepared in accordance with Section 51 of the Promotion of Access to Information Act of 2000 to address the requirements of the Protection of Personal Information Act Nº 4 of 2013.

This manual applies to Skypiom (Pty) Ltd
Registration Nº 2011/129576/07

Approved by: Thomas Kritzer, Managing Director
Approval date: 20th June 2018
Last amended on: 10th April 2025

1. Version Control

Version	Date	Author	Description
0.1	18/06/2018	Thomas Kritzer	Draft policy
1.0	20/06/2018	Thomas Kritzer	Release version
1.1	08/05/2018	Thomas Kritzer	Contact details updated
1.2	07/09/2020	Sven Ragaller	Contact details updated
1.3	26/06/2021	Thomas Kritzer	Updating of Section 2, 3 & 4 and annexures.
1.4	27/06/2022	Thomas Kritzer	Updating of Section 5 and contact details updated
1.5	12/12/2022	Thomas Kritzer	Updating of Sections 2.8 and 5.
1.6	24/05/2023	Thomas Kritzer	Contact details updated
1.7	05/07/2023	Thomas Kritzer	Updating of Sections 2.4, 2.7, 2.8, 4.11
1.8	10/04/2025	Thomas Kritzer	Updating of Sections 2.4, 4.8

2. Introduction

2.1. Purpose

The promotion of the Access to Information Act of 2000 (PAIA) gives third parties the right to approach private bodies (and the government) to request information held by them, which is required in the exercise or protection of any right.
The Act accordingly requires that procedures be put in place by public and private bodies to enable persons to obtain access to records swiftly, inexpensively and effortlessly. In terms of the Act, a private body includes juristic entities such as companies.

On request, the private body – in this instance Skypiom – is obliged to release such information unless PAIA expressly states that the records containing such information may not be released. This manual informs requestors of procedural and other requirements that a request must meet as prescribed by PAIA and furthermore serves as a guide on how a requester of information may request access to that information held by Skypiom.

This manual is not exhaustive of, nor does it comprehensively deal with, every procedure provided for in PAIA. Requesters are advised to familiarise themselves with the provisions of PAIA before making any requests to Skypiom in terms of PAIA.

Skypiom makes no representation and gives no undertaking or warranty that the information in this manual or any information provided by it to a requester is complete or accurate, or that such information is fit for any purpose. All users of any such information shall use such information entirely at their own risk, and Skypiom shall not be liable for any loss, consequential or otherwise, expense, liability or claims, howsoever arising, resulting from the use of this manual or of any information provided by Skypiom or from any error therein.

All users irrevocably agree to submit exclusively to the law of the Republic of South Africa and to the exclusive jurisdiction of the courts of South Africa in respect of any dispute arising out of the use of this manual or any information provided by Skypiom.

This document serves as the information manual of Skypiom and its subsidiaries, if applicable, as required in terms of PAIA.

2.2. Availability of This Manual

As provided for in terms of section 51(2), this manual will be updated on an as required basis. Once the amendments have been finalised the latest version will be made public through Skypiom's website (https://www.skypiom.com).

Alternatively, a requester may contact Skypiom per the particulars outlined in section 3.5 of this manual and request to obtain an electronic copy of this manual.

2.3. Guide to the South African Human Rights Commission

A guide to PAIA, as contemplated under Section 10 of PAIA, is made available from the South African Human Rights Commission and contains information required by a person who wishes to exercise any right contemplated under PAIA, which may be obtained from:

The South African Human Rights Commission (PAIA Unit)
Private Bag 2700, Houghton, 2041
Telephone: +27 11 484-8300
Fax: +27 11 484-7146
www.sahrc.org.za
PAIA@sahrc.org.za

2.4. Nature of Business

Skypiom is software company that develops a comprehensive learning management and compliance tracking system, which includes legislative tracking and AML sanctions screening. The system is marketed under the name of "Skypiom Compliance". Skypiom Compliance is in essence a tapestry of modules and solutions each uniquely built for edTech & regTech challenges and requirements. As quintessential part of the solution is granular measurability, which can only exist when specific data is collected. As a result, Skypiom is accountable for the lawful processing of the Personal Information it collects, stores and disposes of.

2.5. Contact Details of Skypiom

Name: Skypiom (Pty) Ltd
Registration Number: 2011/129576/07
Physical Address: W17 Watershed, 17 Dock Road, V&A Waterfront, 8002, Cape Town, South Africa
Postal Address: Postnet Suite 747, Private Bag X16, Constantia, 7848, Cape Town, South Africa

2.6. Contact Details of the Information Officer of Skypiom

Information Officer: Thomas Kritzer, Managing Director
Physical Address: W17 Watershed, 17 Dock Road, V&A Waterfront, 8002, Cape Town, South Africa
Postal Address: Postnet Suite 747, Private Bag X16, Constantia, 7848, Cape Town, South Africa
Telephone: +27 21 012 5600
Email: info@skypiom.com

2.7. Records Available in Accordance with Other Legislation

Records kept in accordance with such other legislation as may be applicable to Skypiom, includes, but is not limited to the following:

i. Basic Conditions of Employment Act 57 of 1997
ii. Compensation for Occupational Injuries and Health Diseases Act No. 130 of 1993
iii. Companies Act 71 of 2008
iv. Consumer Protection Act, No 68 of 2008
v. Electronic Communications and Transactions Act 25 of 2002
vi. Employment Equity Act, No 55 of 1998
vii. Financial Advisory and Intermediary Services Act, No 37 of 2002
viii. Financial Intelligence Centre Act, No 38 of 2001
ix. Labour Relations Act 66 of 1995
x. National Credit Act, No 34 of 2005
xi. Occupational Health and Safety Act 85 of 1993
xii. Promotion of Access to Information Act 2 of 2000

xiii. Skills Development Levies Act No. 9 of 1999
xiv. Unemployment Insurance Contributions Act 4 of 2002
xv. Value Added Tax Act 89 of 1991

2.8. Subjects and Categories of Records held

Companies Act Records	Documents of incorporation, memorandum of incorporation, minutes of board of directors' meetings, records relating to the appointment of directors/auditor/secretary/public officer and other officers, share register and other statutory registers.	Retention period of electronic files: at least 5 years
Financial Records	Tax returns, accounting records, banking records, rental agreements, tax returns, PAYE, UIF and SDL records, documents issued to employees for income tax purposes including payslips, VAT, workmen's compensation, all other statutory compliances.	Retention period of electronic files: at least 5 years
Job Applicant, Employee & Director Records	Educational information, employment history and criminal behaviour, Employment contracts including age, ID number, physical and postal address and contact details, disciplinary records, salary records, leave records, including sick leave, job evaluation results, personality profiles and cognitive ability records, scorecards and correspondence.	Retention period of electronic files: at least 7 years
Customers & Public Users – Natural Person	Names, contact numbers, date of birth, ID number, demographic, sex, language, employee codes, educational information, occupation, email address, training records, personality profiling and cognitive ability records and correspondence, complaint records.	Retention period of electronic files: at least 7 years while Service Level Agreement (SLA) is in place. If the SLA has been terminated then all *Customer & Public Users – Natural Person information* shall be deleted or obfuscated 3 months after the termination of the SLA.
Customers – Juristic Person	Names of contact persons, their email addresses and contact numbers, name of legal entity, physical and postal address, contact details, financial information; registration number;	Retention period of electronic files: at least 7 years

	VAT number, authorised signatories, agreements, including services rendered, as well as addendums.	
Contracted Service	Names of contact persons, name of legal entity, physical and postal address, contact details, financial information; registration number; VAT number, authorised signatories, agreements and addendums as well as correspondence.	Retention period of electronic files: at least 5 years
Contracted Service Providers	Names of contact persons, name of legal entity, physical and postal address, contact details, financial information; registration number; VAT number, authorised signatories, agreements and addendums as well as correspondence.	Retention period of electronic files: at least 5 years

Specifically pertaining to the National Credit Act, No 34 of 2005:
Documents must be retained for three years from the earliest of the following dates: the creation, signing, or receipt of the document by the registrant; the termination date of the agreement; or, in the case of a denied or ungranted credit application, the date of receipt of the application. This requirement applies to the documents listed below.

Regulation 55(1)(b):
Records of registered activities such as declined credit applications;

- Reason for the credit application decline;
- Pre-agreement statements and quotes;
- Documentation supporting steps taken under section 81(2) of the Act;
- Record of payments made;
- Documentation supporting steps taken following consumer default.

Regulation 55(1)(c) in respect of operations:

- Record of income, expenses, and cash flow;
- Credit transaction flows;
- Management accounts and financial statements.

Regulation 55(1)(d) regarding the Credit Bureau:

- All documents related to disputes, including but not limited to, documents from the consumer;
- Documents from the entity responsible for the disputed information;
- Documents related to the investigation of the dispute;
- Correspondence to and from information sources as specified in section 70(2) of the Act and Regulation 18(7) concerning disputed information.

Regulation 55(1)(a) regarding Debt Counsellors:

- Application for debt review;
- Copies of all documents submitted by the consumer;
- Copy of the rejection letter;

- Debt restructuring proposal;
- Copy of any order made by the tribunal and/or the court and a copy of the clearance certificate.

Regulation 56 regarding section 170 of the Act:

- Application for credit;
- Credit agreement entered into with the consumer.

Regulation 17(1) regarding Credit Bureau information:
Documents with a required retention period of the earlier of 10 years or a granted rehabilitation order:

- Sequestrations
- Administration orders.

Documents with a required retention period of 5 years:

- Rehabilitation orders
- Payment profile.

Documents with a required retention period of the earlier of 5 years or until a court rescinds judgment or the credit provider abandons it under section 86 of the Magistrate's Court Act No 32 of 1944:

- Civil Court Judgments.

Documents with a required retention period of 2 years:

- Enquiries.

Documents with a required retention period of 1.5 years:

- Details and results of disputes lodged by consumers.

Documents with a required retention period of 1 year:

- Adverse information.

Documents with an unlimited required retention period:

- Liquidation.

Documents required to be retained until a clearance certificate is issued:

- Debt restructuring.

2.9. Records Automatically Available

No notice has been published pursuant to Section 51(1)(b)(ii), regarding the categories of records which are automatically available without having to request access in terms of the Act. The following records are automatically available at the registered office of Skypiom on payment of the prescribed fee for reproduction:

i. Records of the company lodged in terms of government requirements such as the Registrar of Deeds;
ii. Documentation and information relating to the company which is held by the Companies and Intellectual Properties Commission in accordance with the requirements set out in set out in section 25 of the Companies Act 71 of 2008;
iii. Product and services brochures;
iv. News and other marketing Information; and
v. Certain other information relating to the company is also made available on its website from time to time.

2.10. Records That Are Not Automatically Available

Records of the company which are not automatically available must be requested in terms of the procedure set out in this PAIA manual, and which may be subject to the restrictions and right of refusal to access as provided for in the Act.

3. Access to Records Held by Skypiom

3.1. Access

Records held by Skypiom may be accessed on request only once the requirements for access have been met. A requester is any person making a request for access to a record of Skypiom and in this regard PAIA distinguishes between two types of requesters:

i. Personal Requester: a personal requester is a requester who is seeking access to a record containing Personal Information about the requester. Subject to the provisions of PAIA and applicable law, Skypiom will provide the requested information, or give access to any record with regard to the requester's Personal Information. The prescribed fee for reproduction of the information requested will be charged by Skypiom.

ii. This requester (other than a personal requester) is entitled to request access to information pertaining to third parties. However, Skypiom is not obliged to grant access prior to the requester fulfilling the requirements for access in terms of PAIA. The prescribed fee for reproduction of the information requested will be charged by Skypiom.

3.2. Request Procedure

A requester must comply with all the procedural requirements contained in PAIA relating to a request for access to a record. A requester must complete the prescribed form enclosed in Appendix and submit same as well as payment of a request fee to the Information Officer at the postal or physical address or email address stated herein. The requester must provide sufficient detail on the request form to enable the Information Officer to identify the record requested and the requester. When completing a request on the prescribed form, the requester must also indicate and/or include:

i. The record or records requested;
ii. Proof of identity of the requester;
iii. What form of access is required; and
iv. The postal address or email address of the requester.

A requester must state that they require the information in order to exercise or protect a right, and clearly state what the nature of the right is so to be exercised or protected. The requester must also provide an explanation of why the requested record is required for the exercise or protection of that right.

Skypiom will, within 30 (thirty) days of receipt of the request, decide whether to grant or decline the request and give notice with reasons to that effect. The 30 (thirty) day period within which Skypiom has to decide whether to grant or refuse the request, may be extended for a further period of not more than 30 (thirty) days if the request is for a large number of information.

The requester shall be informed in writing whether access has been granted or denied. If, in addition, the requester requires the reasons for the decision in any other manner, they must state the manner and the particulars so required. If a request is made on behalf of another person, the requester must then submit proof of the capacity in which the requester is making the request to the satisfaction of the Information Officer.

If an individual is unable to complete the prescribed form due to illiteracy or disability, such a person may make the request orally to the Information Officer.

Skypiom will commence processing a request within 10 (ten) days from the aforesaid decision date, unless the requestor has stated special reasons that would satisfy the Information Officer that circumstances dictate that this time period should

not be complied with, and will complete the request within 30 (thirty) days from commencement thereof.

3.3. Grounds for Refusal

Grounds for Skypiom to refuse a request for information may relate to:

i. The mandatory protection of privacy of a third party who is a natural person;
ii. The mandatory protection of the commercial information of a third party;
iii. The mandatory protection of confidential information of third parties if it is protected in terms of any agreements;
iv. The mandatory protection of the safety of individuals and protection of property;
v. The mandatory protection of records which would be regarded as privileged in legal proceedings;
vi. The mandatory protection of the commercial activities of Skypiom;
vii. The research information of Skypiom or a third party, if its disclosure would disclose the identity of Skypiom, the researcher or the subject matter of the research and would place the research at a serious disadvantage; and
viii. The requests for information that are clearly frivolous or which involve an unreasonable diversion of resources shall be refused.

3.4. Remedies if Request for Information is Refused

i. Internal Remedies
Skypiom does not have internal appeal procedures. As such, the decision made by the Information Officer pertaining to a request is final and requestors will have to exercise such external remedies at their disposal if a request is refused and the requestor is not satisfied with the response provided by the Information Officer.

ii. External Remedies
A requestor that is dissatisfied with the Information Officer's refusal to disclose information, may within 30 (thirty) days of notification of the decision, apply to a court for relief. Likewise, a third party dissatisfied with the Information Officer's decision to grant a request for information, may within 30 (thirty) days of notification of the decision, apply to a court for relief. For purposes of PAIA, courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status.

3.5. Fees

PAIA provides for two types of fees, as contemplated by PAIA, namely:

i. A request fee, which will be a standard fee; and
ii. An access fee, which must be calculated by taking into account reproduction costs, search and preparation time and cost, as well as postal costs.

When the request is received by the Information Officer, such officer shall by notice require the requester, other than a personal requester, to pay the prescribed request fee (if any) before further processing of the request.
If the search for the record has been made and the preparation of the record for disclosure, including arrangement to make it available in the requested form, requires more than the hours prescribed in PAIA for this purpose, the Information Officer shall notify the requester to pay as a deposit the prescribed portion of the access fee which would be payable if the request is granted.
The Information Officer shall withhold a record until the requester has paid the required fees. A requester whose request for access to a record has been granted,

must pay an access fee for reproduction and for search and preparation, and for any time reasonably required in excess of the prescribed hours to search for and prepare the record for disclosure including making arrangements to make it available in the request form.

If a deposit has been paid in respect of a request for access, which is refused, then the Information Officer will repay the deposit to the requester within 5 (five) business days.

3.6. Record Keeping

Personal requesters or requesters as defined in 3.1. retain the right to interact with Skypiom regarding Personal Information. Evidence of such interaction will be kept on record.

4. POPI Compliance

Section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy.

The right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.

POPI gives customers the right to, in the prescribed manner, request Skypiom to:

i. Correct or delete Personal Information about that person in Skypiom's possession or under Skypiom's control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or destroy or delete a record of Personal Information about the customer that Skypiom is no longer authorised to retain access and/or request the correction or deletion of any Personal Information held about them that may be inaccurate, misleading or outdated.
ii. Skypiom endorses the spirit of the PAIA Act and POPI Act and believes that this Manual will assist requesters in exercising their rights.
iii. The following sections lays out the measures that Skypiom are and will be taking to be in compliance with POPI.

4.1. Conditions for Lawful Processing of Information

Skypiom is committed to complying with the eight conditions of lawful processing of Personal Information as set out in POPI, namely:

i. Accountability: Skypiom must ensure that the seven other conditions are met throughout the data processing lifecycle.
ii. Processing Limitation: Skypiom must process the Personal Information in a manner that is adequate, relevant, and not excessive for the purposes it is being processed for.
iii. Purpose Specification: Skypiom must have a specific and lawful purpose that is related to its business activities.
iv. Further Processing Limitation: Anything else done with the data must be compatible with the original purpose for collection.
v. Information Quality: Skypiom must make sure the Personal Information it collects is correct.
vi. Openness: Skypiom will be open and transparent about its processes around Personal Information.
vii. Security Safeguards: Skypiom needs to safeguard the integrity and confidentiality of the Personal Information it processes.
viii. Data Subject Participation: Customers have the right to know if Skypiom holds their Personal Information and how it is being used or shared.

4.2. Consent for Processing Personal Information

i. Skypiom shall obtain consent to process Personal Information whenever necessary.
ii. In cases where Skypiom does not seek the consent of its customers, Skypiom will process their data to comply with a legal obligation on its part or to protect a legitimate interest.
iii. If a customer withdraws consent, or if a legitimate objection is raised, Skypiom will cease processing their Personal Information.

4.3. Source of Personal Information

Skypiom collects personal information directly from the customer whose information it needs unless:

i. The information is public information; or
ii. Consent to collecting personal information from another source has been obtained from the customer; or
iii. It does not prejudice the customer if the information is obtained from another provider; or
iv. The information is needed to maintain law and order or national security; or
v. The collection of information is required by law; or
vi. Insofar as the information collected is required to conduct proceedings in any court or tribunal, such proceedings having commenced or being contemplated; or
vii. This information is necessary to protect Skypiom's legitimate interests; or
viii. Seeking consent would compromise the purpose of collecting information; or
ix. Seeking consent is not reasonably practical in the circumstances.

4.4. Purpose for Processing of Personal Information

Chapter 3 of POPI states that *"Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive".* Skypiom will only collect and process Personal Information where legally and contractually permitted, authorised, and obliged to do so. Personal Information will be used to:

i. comply with legislation and/or lawful obligations;
ii. give effect to a contractual relationship between Skypiom, a customer and/or public user;
iii. conduct Skypiom's business operations; and
iv. to protect the legitimate interests of Skypiom, a customer, the public user, or any third parties.

4.5. Personal Information Processed by Skypiom

Skypiom collects and processes Personal Information pertaining to a customer's learning and development as well as personality and cognitive ability by virtue of a HPCSA listed personality profiling tool ("SOPCAPS"), which includes but is not limited to the below (Table 1). The type of information collected will depend on the need for which it is collected and will be processed for that purpose only. Skypiom does not share Personal Information with third parties.

Skypiom follows a strict paperless business policy in line with the Electronic Communications and Transactions Act 25 of 2002 to which end all physical documents will be converted into electronic formats, after which the physical document will be destroyed.

Skypiom will destroy or delete any records of personal information (so that its customers are no longer identifiable) as soon as reasonably possible after the time period for which Skypiom was allowed to hold the information has expired.

4.6. Personal Information Access Control

Skypiom shall secure the integrity of the Personal Information in its possession or under its control by:

i. Taking appropriate, reasonable, technical and organisational measures to prevent loss of, or damage to, or unauthorised destruction of the Personal

Information or unlawful access to or processing of the Personal Information and which provide a level of security appropriate to the risk represented by the processing and the nature of the Personal Information to be protected;

ii. Taking reasonable steps to ensure the reliability of any of its employees who have access to Personal Information;

iii. Limiting access to the Personal Information only to those employees who need to know to enable Skypiom to achieve the purposes and objectives of any agreement in terms of which processing is required and ensure that employees used by it to process the Personal Information have undergone training in the care and handling of the Personal Information;

iv. Providing the owner of the Personal Information with full co-operation and assistance in relation to any requests for access or correction or complaints made by data subjects.

4.7. Restriction on processing Personal Information

Skypiom must restrict the processing of Personal Information in the following situations:

i. If the accuracy of the information is contested, for the time necessary for Skypiom to verify the accuracy of the information.

ii. If the purpose for which the personal information was collected has been fulfilled and the information is being retained only for the purposes of proof.

iii. It is unlawful to process the Personal Information and the customer opposes destruction or deletion and requests its restriction.

iv. If the customer requests transfer thereof to another automated data processing system.

4.8. Disclosure of Systems, Procedures and Storage

Skypiom makes use of a number of systems, procedures and storage solutions that comprise the entire value offering:

i. Skypiom Compliance exists within the Amazon Web Services (AWS) environment and is thus housed within an ISO and SOC compliant environment. All data, which includes Personal Information, is encrypted using AWS Encryption options as appropriate for both structured (SQL Database) data and unstructured (S3) data. All communication between user browsers and Skypiom servers is encrypted using relevant Secure Sockets Layer (SSL) encryption protocols. The security certificates are issued by AWS and Transport Layer Security (TLS) 1.3 is the current default encryption version. Further, Skypiom's servers are running Amazon Linux 2, a highly secure and commercial grade OS, enhanced for operation within the AWS cloud environment. Updates are applied in a timely manner, as released by Amazon and typically within less than one week of release. Some servers' updates are managed directly by AWS.
AWS implements and maintains technical and organisational security measures applicable to AWS cloud infrastructure services under globally recognised security assurance frameworks and certifications, including ISO 27001, ISO 27017, ISO 27018, PCI DSS Level 1, and SOC 1, 2 and 3. These technical and organisational security measures are validated by independent third-party assessors, and are designed to prevent unauthorised access to or disclosure of customer content.

ii. All Skypiom employees are furnished with MacBook laptops. Skypiom does not support nor permit an employee to use their own device. It is mandatory to activate FileVault, which is macOS's built-in disk encryption feature. FileVault is designed to encrypt a MacBook hard drive and all of the files located on the

drive using 128-bit Advanced Encryption Standard (AES) encryption with a 256-bit key. In addition, it is company policy to secure a MacBook laptop with an access password. Notwithstanding, each MacBook is linked to a unique Apple ID, via which a lost or stolen device can be remotely erased in the unlikely event that a device is lost or stolen.

iii. Skypiom's administrative information is stored on Dropbox for Business. Dropbox is designed with multiple layers of protection and is distributed across a scalable, secure infrastructure. These layers of protection include 256-bit Advanced Encryption Standard (AES) encryption for files at rest on Dropbox, and 128-bit or higher Advanced Encryption Standard (AES) encryption for Secure Sockets Layer (SSL)/Transport Layer Security (TLS) to protect data in transit between Skypiom's devices and Dropbox servers i.e. end-to-end encryption. Access to the Dropbox architecture is dependent on the employee's position and can be removed remotely.

iv. Each employee's laptop is backed up to an external hard drive, which – per company policy – is encrypted. This too is based on 128-bit Advanced Encryption Standard (AES) encryption with a 256-bit key.

4.9. Transborder Flow of Personal Information

Section 72 of POPI deals with transfers of Personal Information outside South Africa or trans-border information flows. Skypiom may not transfer Personal Information about a data subject to a third party who is in a foreign country unless certain protections are in place. These include, but are not limited to:

i. The third party who is the recipient of the information is subject to law, binding corporate rules or a binding agreement which provides an adequate level of protection.
ii. The data subject consents to the transfer.
iii. The transfer is necessary for the performance of a contract between the data subject and Skypiom.
iv. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between Skypiom and a third party.
v. The transfer is for the benefit of the data subject.

Since Skypiom may transfer data transborder for processing, Skypiom will ensure that the aforementioned actions have been taken and the applicable measures have been put in place to ensure compliance with POPI in the event that it participates in a transborder transfer of Personal Information.

4.10. Disclosure and Transfer of Personal Information to Others

Skypiom may from time to time transfer and/or disclose Personal Information to other parties, including its group companies or subsidiaries, and/or government entities if required to do so by law.

Such disclosure shall always be subject to a written agreement concluded between Skypiom and such other person ("the recipient") obligating the recipient to comply with strict confidentiality, with all the information security conditions and provisions as contained in this Policy and as contained in POPI itself.

4.11. Retention, Archiving and Destruction of Personal Information

Personal Information is not retained for longer than is necessary for achieving the purpose for which it was collected and subsequently processed. The exceptions to the above principle specifically provided in POPIA are where:

i. the retention of the record is required or authorised by law;
ii. Skypiom reasonably requires the record for lawful purposes related to its functions or activities;
iii. the retention of the record is required in terms of an agreement between the Skypiom and a customer and/or public user; or
iv. the record is retained for historical purposes, with Skypiom having established appropriate safeguards against the record being used for any other purpose.

When Skypiom is no longer authorised to retain Personal Information, it shall dispose such Personal Information or records of Personal Information or de-identify / obfuscate them in a manner that prevents their reconstruction in an intelligible form. Each department is responsible for regularly managing the destruction of its Personal Information. Before destruction, Personal Information must be reviewed to ensure it is eligible for disposal. Upon completion of this review process, the department manager shall authorise the disposal of the Personal Information.

5. Personal Information Impact Assessment

A Personal Information Impact Assessment (PIIA) is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data.

In order to assess the impact of the data privacy laws, and what Skypiom needs to do in order to comply with these laws, an initial base line DPIA will be conducted by the Information Officer and/or their deputies, which will form the basis of the Skypiom's data privacy framework.

Further PIIA's must be carried out when new technologies or new systems, solutions and research studies are implemented or where personal information processing is likely to result in high risk to both the data subjects and to Skypiom. A PIIA must:

i. describe the nature, scope, context and purposes of the processing;
ii. assess necessity, proportionality and compliance measures;
iii. identify and assess risks to the individual; and
iv. identify any additional measures to mitigate those risks.

All PIIA's must be assessed and signed off by the Information Officer and/or their deputy. In order to give effect to the above, all directors, employees and/or any other representatives who process personal information on behalf of Skypiom must familiarise themselves with the requirement to conduct a PIIA and ensure where one is required that it is conducted in accordance with the relevant Skypiom's PIIA Policy.

List of Annexures:

1. Objection to the Processing of Personal Information (Form 1 of the Regulations)
2. Request for Correction or Deletion or Personal Information (Form 2 of the Regulations)
3. Application for consent to direct marketing (Form 4 of the Regulations)
4. Request for Access to Record of Private Body (Form C)
5. Customer consent to process Personal Information (Data Subject Consent Form)

Form 1

Objection to the Processing of Personal Information in terms of Section 11(3) of the Protection of Personal Information Act, 2013 (Act no. 4 of 2013).

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 2]

Note:
1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

A	DETAILS OF DATA SUBJECT
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	Code ( )
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f)** *(Please provide detailed reasons for the objection)*

Signed at ..... this ..... day of .....20……..

.....
Signature of data subject/designated person

Form 2

Request for Correction or Deletion of Personal Information or Destroying or Deletion of Record of Personal Information in terms of Section 24(1) of the Protection of Personal Information Act, 2013 (Act no. 4 of 2013).

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 3]

Note:
1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is inpossession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF THE DATA SUBJECT
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED**
REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN. *(Please provide detailed reasons for the request)*	

Signed at ..... this ..... day of .....20……..

.....
Signature of data subject/ designated person

Form 4

Application for the Consent of a Data Subject for the Processing of Personal Information for the purpose of direct marketing in terms of Section 69(2) of the Protection of Personal Information Act, 2013 (Act no. 4 of 2013).

FORM 4

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING IN TERMS OF SECTION 69(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 6]

TO: _____
_____
_____
_____
(Name of data subject)

FROM: _____
_____
_____
_____
Contact number(s): _____
Fax number: _____
E-mail address: _____
(Name, address and contact details of responsible party)

Full names and designation of person signing on behalf of responsible party:

_____

.....
Signature of designated person

Date: _____

PART B

I, _____*(full names of data subject)* hereby:

☐ Give my consent.

To receive direct marketing of goods or services to be marketed by means of electronic communication.

SPECIFY GOODS or SERVICES:

SPECIFY METHOD OF COMMUNICATION: FAX:
E - MAIL:
SMS:
OTHERS – SPECIFY:

Signed at ..... this ..... day of .....20.....

.....
Signature of data subject

Form C

Request for Access to the Record of Private Body, (Section 53(1) of the Promotion of Access to Information Act, 2000 (Act No.2 of 2000).

J752

REPUBLIC OF SOUTH AFRICA

FORM C
REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY
(Section 53(1) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000))
[Regulation 10]

A. Particulars of private body
The Head:

B. Particulars of person requesting access to the record

(a) The particulars of the person who requests access to the record must be given below.
(b) The address and/or fax number in the Republic to which the information is to be sent must be given.
(c) Proof of the capacity in which the request is made, if applicable, must be attached.

Full names and surname: ……

Identity number: | | | | | | | | | | | | | |

Postal address: ……

Telephone number: (……) …….. Fax number: (……) ……..

E-mail address: ……

Capacity in which request is made, when made on behalf of another person:

C. Particulars of person on whose behalf request is made

This section must be completed ONLY if a request for information is made on behalf of another person.

Full names and surname: ……

Identity number: | | | | | | | | | | | | | |

D. Particulars of record

(a)	Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.
(b)	If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1. Description of record or relevant part of the record:

……

……

……

……

2. Reference number, if available:

……

……

……

……

3. Any further particulars of record:

……

……

……

……

E. Fees

(a)	A request for access to a record, other than a record containing personal information about yourself, will be processed only after a request fee has been paid.
(b)	You will be notified of the amount required to be paid as the request fee.
(c)	The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.
(d)	If you qualify for exemption of the payment of any fee, please state the reason for exemption.

Reason for exemption from payment of fees:

……

……

……

……

……

F. Form of access to record

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in 1 to 4 below, state your disability and indicate in which form the record is required.

Disability: Form in which record is required:

Mark the appropriate box with an **X**.

NOTES:
(a) Compliance with your request for access in the specified form may depend on the form in which the record is available.
(b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.
(c) The fee payable for access to the record, if any, will be determined partly by the form in which access is requested.

1. If the record is in written or printed form:						
	copy of record*		inspection of record			
2. If record consists of visual images - (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.):						
	view the images		copy of the images*		transcription of the images*	
3. If record consists of recorded words or information which can be reproduced in sound:						
	listen to the soundtrack (audio cassette)		transcription of soundtrack* (written or printed document)			
4. If record is held on computer or in an electronic or machine-readable form:						
	printed copy of record*		printed copy of information derived from the record*		copy in computer readable form* (stiffy or compact disc)	

*If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.	YES	NO

G. Particulars of right to be exercised or protected

If the provided space is inadequate, please continue on a separate folio and attach it to this form.
The requester must sign all the additional folios.

1. Indicate which right is to be exercised or protected:

……..

……..

……..

2. Explain why the record requested is required for the exercise or protection of the aforementioned right:

……..

……..

……..

H. Notice of decision regarding request for access

You will be notified in writing whether your request has been approved / denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

……..

Signed at …….. this day…… of ……..year ……

……
SIGNATURE OF REQUESTER /
PERSON ON WHOSE BEHALF REQUEST IS MADE