MONEY DOC (PTY) LTD

Registration No. 2019/466808/07 | Authorised Financial Services Provider No. 52081

PROTECTION OF PERSONAL INFORMATION POLICY

POLICY STATEMENT

- This policy forms part of the policy owner's internal business processes and procedures.
- In this document, "Money Doc", "the organisation", "we", "us" and "our" refer to Money Doc (Pty) Ltd (Registration No. 2019/466808/07), an authorised financial services provider (FSP No. 52081). Any reference to Money Doc includes the policy owner.
- Money Doc's Director and Key Individual, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of Money Doc are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.
- Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

POLICY ADOPTION

Money Doc has adopted this policy as part of its commitment to protecting the personal information of its clients and other data subjects. This policy has been approved and adopted by the Director and Key Individual of Money Doc.

Table of Contents

1 INTRODUCTION 1

2 DEFINITIONS 1

2.1 Biometrics 1

2.2 Complainant 1

2.3 Consent 1

2.4 Data Subject 1

2.5 De-Identify 1

2.6 Deputy Information Officer 1

2.7 Filing System 1

2.8 Information Officer 1

2.9 Information Regulator 1

2.10 Operator 1

2.11 Personal Information 2

2.12 Processing 2

2.13 Record 2

2.14 Re-Identify 2

2.15 Responsible Party 2

2.16 Unique Identifier 3

3 POLICY PURPOSE 3

4 POLICY SCOPE AND APPLICATION 3

5 RIGHTS OF DATA SUBJECTS 4

5.1 The Right to Access Personal Information 4

5.2 The Right to have Personal Information Corrected or Deleted 4

5.3 The Right to Object to the Processing of Personal Information 4

5.4 The Right to Object to Direct Marketing 4

5.5 The Right to Complain to the Information Regulator 5

5.6 The Right to be Informed 5

6 GENERAL PRINCIPLES OF LAWFUL PROCESSING 5

6.1 Accountability 5

6.2 Processing Limitation 5

6.3 Purpose Specification 6

6.4 Further Processing Limitation 6

6.5 Information Quality 6
6.6 Open Communication 6
6.7 Security Safeguards 6
6.8 Data Subject Participation 7
7 INFORMATION OFFICER 7
8 DEPUTY INFORMATION OFFICER/S 7
9 SPECIFIC DUTIES AND RESPONSIBILITIES 7
9.1 Director and Key Individual 7
9.2 Information Officer 8
9.3 Deputy Information Officer 9
9.4 Information Technology and Security 9
9.5 Employees and other Persons acting on behalf of Money Doc 10
10 POPIA AUDIT 11
11 REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE 12
12 POPIA COMPLAINTS PROCEDURE 12
13 DISCIPLINARY ACTION 13
ANNEXURE A: PERSONAL INFORMATION REQUEST FORM 14
ANNEXURE B: POPIA PRIVACY NOTICE 15

1 INTRODUCTION

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA"). POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Through the provision of quality goods and services, Money Doc is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders. A person's right to privacy entails having control over their personal information and being able to conduct their affairs relatively free from unwanted intrusions.

Given the importance of privacy, Money Doc is committed to effectively managing personal information in accordance with POPIA's provisions.

2 DEFINITIONS

2.1 Biometrics

Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

2.2 Complainant

Means any person who lodges a complaint with the Information Regulator

2.3 Consent

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

2.4 Data Subject

Means the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies Money Doc with products or other goods.

2.5 De-Identify

Means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.6 Deputy Information Officer

Means the person designated to assist the Information Officer in performing their duties under POPIA and PAIA, and to whom the Information Officer may delegate powers and responsibilities.

2.7 Filing System

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.8 Information Officer

Means the person who is responsible for ensuring Money Doc's compliance with POPIA. The Information Officer is the head of Money Doc will be responsible for performing the Information Officer's duties.

2.9 Information Regulator

is an independent juristic person established under section 39 of the Protection of Personal Information Act (POPIA) to monitor, enforce, and promote compliance with POPIA and PAIA.

2.10 Operator

Means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with Money Doc to shred

documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

2.11 Personal Information

Means any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person;
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.12 Processing

Means any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- 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 any restriction, degradation, erasure or destruction of information.

2.13 Record

Means any recorded information, regardless of form or medium, including:

- Writing on any material;
- Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.14 Re-Identify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.15 Responsible Party

Means the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, Money Doc is the responsible party.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing their duties. Deputy Information Officers can also be appointed to assist the Information Officer.

2.16 Unique Identifier

Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

3 POLICY PURPOSE

This purpose of this policy is to protect Money Doc from the compliance risks associated with the protection of personal information which includes:

- ***Breaches of confidentiality.*** For instance, Money Doc could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- ***Failing to offer choice.*** For instance, all data subjects should be free to choose how and for what purpose Money Doc uses information relating to them.
- ***Reputational damage.*** For instance, Money Doc could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by Money Doc.

This policy demonstrates Money Doc's commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
- By cultivating an organisational culture that recognises privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of Money Doc.
- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of Money Doc and data subjects.
- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4 POLICY SCOPE AND APPLICATION

This policy and its guiding principles applies to:

- Money Doc's Director and Key Individual;
- All branches, business units and divisions of Money Doc, if any;
- All employees, independent contractors and interns, if any;
- All contractors, suppliers and other persons acting on behalf of Money Doc

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as Money Doc's PAIA Manual as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation where there is:

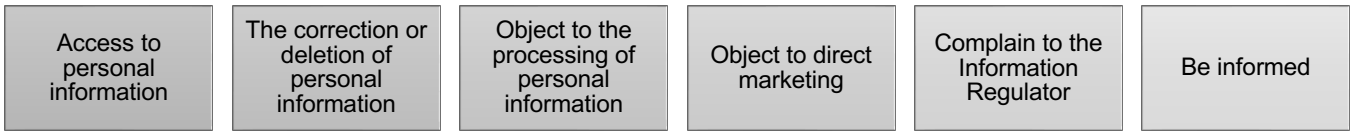
- A **processing** of…..…..
- ……**personal information**…….
- ……..entered into a **record**…….
- ……..……..by or for a **responsible person**……
- ……..who is **domiciled** in South Africa.

POPIA does **not** apply in situations where the processing of personal information:

- is concluded in the course of purely personal or household activities, or
- where the personal information has been de-identified.

5 RIGHTS OF DATA SUBJECTS

Where appropriate, Money Doc will ensure that its clients/customers are made aware of the rights conferred upon them as data subjects. Money Doc will ensure that it gives effect to the following six (6) rights. The right to:



5.1 The Right to Access Personal Information

Money Doc recognises that a data subject has the right to establish whether Money Doc holds personal information related to them including the right to request access to that personal information.

An example of a "Personal Information Request Form" can be found under "**Annexure A**".

5.2 The Right to have Personal Information Corrected or Deleted

The data subject has the right, in terms of section 24 of POPIA, to request, where necessary, the correction, deletion or destruction of their personal information. A data subject may request the correction or deletion of personal information where such information is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully. A data subject may also request the destruction or deletion of a record of personal information where Money Doc is no longer authorised to retain such record in terms of POPIA. A data subject who wished to exercise this right may submit the request at any time and free of charge, using **Form 2** of the Regulations or a form substantially similar thereto. Money Doc will ensure that such request mechanisms are reasonably accessible, including submission by hand, post or e-mail or any other appropriate communication channel made available by Money Doc.

Where a request for correction, deletion or destruction is submitted telephonically, Money Doc will record the request and, upon request, make such recording or a transcription thereof available to the data subject free of charge.

Money Doc will, within thirty (30) days of receipt of the outcome of the request, notify the data subject in writing of the action taken.

5.3 The Right to Object to the Processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of their personal information, in accordance with section 11(3) of POPIA.

In such circumstances, Money Doc will give due consideration to the request and the requirements of POPIA. Money Doc may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

A data subject who wishes to object to the processing of personal information, must submit the objection to the responsible party at any time during office hours and free of charge, using **Form 1** of the Regulations to the Act or a form substantially similar thereto. Money Doc will ensure that the objection mechanism is reasonably accessible, including submission by telephone call, email, hand or post or any other appropriate communication channel made available by Money Doc.

Where objection is submitted telephonically, Money Doc will electronically record the objection and, upon request, make such recording or a transcription thereof available to the data subject.

Money Doc must render such reasonable assistance as is necessary, free of charge, to enable the data subject to submit an objection.

5.4 The Right to Object to Direct Marketing

The data subject has the right to object, at any time, to the processing of their personal information for purposes of direct marketing, irrespective of whether such marketing is conducted by electronic or non-electronic means.

Money Doc will respect any such objection and ensure that no further direct marketing communications are sent to the data subject.

Money Doc does not conduct direct marketing.

5.5 The Right to Complain to the Information Regulator

The data subject, or any other person permitted in terms of POPIA, has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of their personal information.

Any person who wishes to submit a complaint to the Information Regulator must do so in writing, via the Information Regulator's website.

5.6 The Right to be Informed

The data subject has the right to be notified that their personal information is being collected by Money Doc.

The data subject also has the right to be notified in any situation where Money Doc has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

6 GENERAL PRINCIPLES OF LAWFUL PROCESSING

All employees and persons acting on behalf of Money Doc will at all times be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability

Money Doc will ensure that the provisions of POPIA and the principles outlined in this policy are complied with through the encouragement of desired behaviour. However, Money Doc will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

Failing to comply with POPIA could potentially damage Money Doc's reputation or expose Money Doc to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

6.2 Processing Limitation

Money Doc will ensure that personal information under its control is processed:

- in a fair, lawful and non-excessive manner, and
- only for a specifically defined purpose.

Money Doc will inform the data subject of the reasons for collecting their personal information. The information can be found in Money Doc's Privacy Notice/s. Alternatively, where services or transactions are concluded over the telephone or electronic video feed, Money Doc will maintain a voice recording of the stated purpose for collecting the personal information.

Money Doc will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected. Where personal information is shared with third parties, Money Doc will ensure that, **prior** to the sharing of personal information:

- complete a personal information impact assessment (PIIA) to identify, assess and mitigate the privacy risk associated with the processing of personal information through/with a third-party and ensure that adequate measures are in place to comply with POPIA; and
- enter into an appropriate data sharing agreement, containing adequate safeguards for the processing of personal information, with the third party.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of Money Doc's business and be provided with the reasons for doing so.

An example of a “POPIA Privacy Notice” can be found under “Annexure B”.

6.3 Purpose Specification

Money Doc will process personal information only for specific, explicitly defined and legitimate reasons. Money Doc will inform data subjects of these reasons prior to collecting or recording the data subject’s personal information.

All of Money Doc’s business units and operations must be informed by the principle of transparency.

6.4 Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

Therefore, where Money Doc seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, Money Doc will first obtain additional consent from the data subject.

6.5 Information Quality

Money Doc will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information be accurate (for example, the bank account details used to settle a client’s transactions are of the utmost importance), the greater the effort Money Doc will put into ensuring its accuracy.

Where personal information is collected or received from third parties, Money Doc will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

6.6 Open Communication

Money Doc will take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.

Money Doc will ensure that it establishes and maintains a “contact us” facility, via its website and by e-mail to the Information Officer, for data subjects who want to:

- Enquire whether Money Doc holds related personal information,
- Request access to related personal information,
- Request Money Doc to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

6.7 Security Safeguards

Money Doc will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information, bank account or credit card details, the greater the security required.

Money Doc will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on Money Doc’s IT network.

Money Doc will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which Money Doc is responsible. All existing employees will, after the required consultation process has been

followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses. An example of “Employee Consent and Confidentiality Clause” for inclusion in Money Doc’s employment contracts can be found under “**Annexure D**”. An example of an “SLA Confidentiality Clause” for inclusion in Money Doc’s service level agreements can be found under “**Annexure E**”.

Money Doc’s operators and third-party service providers will be required to enter into service level agreements with Money Doc where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

Money Doc must implement its incident response plan to:

- Prevent and manage security risks to personal information; and
- Respond to and notify the data subject and the Information Regulator of any security compromises as soon as reasonably practicable.

6.8 Data Subject Participation

A data subject may request the correction or deletion of their personal information held by Money Doc. Kindly refer to Money Doc’s Privacy Notice and/or PAIA Manual on our website. Money Doc will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information.

Money Doc will maintain a documented data subject request procedure to deal with any requests received in respect of POPIA or PAIA.

7 INFORMATION OFFICER

Money Doc’s Information Officer is responsible for ensuring compliance with POPIA. The Director and Key Individual of Money Doc, Mark Sluzki, is Money Doc’s Information Officer. The Information Officer will register with the Information Regulator established under POPIA prior to performing their duties, in accordance with “Annexure A” to the Guidance Note on Information Officers and Deputy Information Officers published by the Information Regulator.

The responsibilities of the Information Officer are set out in paragraph 9.2 below.

8 DEPUTY INFORMATION OFFICER/S

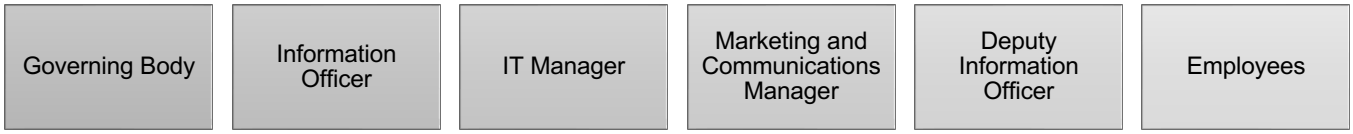
Money Doc appointed a Deputy Information Officer to assist the Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of any Deputy Information Officers.

Money Doc has appointed a Deputy Information Officer in the prescribed format in “Annexure B” to the Guidance Note on Information Officers and Deputy Information Officers published by the Information Regulator.

The responsibilities of the Deputy Information Officer are set out in paragraph 9.3 below.

9 SPECIFIC DUTIES AND RESPONSIBILITIES

The following persons have specific responsibilities in terms of Money Doc’s POPIA framework:



9.1 Director and Key Individual

Money Doc’s Director and Key Individual cannot delegate this accountability and is ultimately answerable for ensuring that Money Doc meets its legal obligations in terms of POPIA. The Director and Key Individual may however delegate some POPIA responsibilities to other capable individuals. The Director and Key Individual is responsible for ensuring that:

- A culture of privacy and compliance is created and integrated into training, governance and risk management of Money Doc.
- Money Doc complies with the 8 conditions for lawful processing as set out in POPIA as well as this policy.
- A POPIA compliance framework is developed, implemented and maintained, including policies, procedures and controls to give effect to POPIA.
- There is the necessary oversight over the implementation of all POPIA controls.
- The Information Officer and Deputy Information Officer has adequate resources, authority and independence.
- The Information Officer and Deputy Information Officer reports on POPIA compliance, breaches and risks.
- The scheduling of a periodic POPIA Audit in order to accurately assess and review the ways in which Money Doc collects, holds, uses, shares, discloses, destroys and processes personal information.
- All persons responsible for the processing of personal information on behalf of Money Doc are appropriately trained and supervised to do so.

9.2 Information Officer

Money Doc's Information Officer is responsible for:

	Area of responsibility	**Responsibilities**
1	***Governance, accountability and reporting***	▪ Ensure Money Doc's compliance with POPIA and the 8 conditions for lawful processing. ▪ Advise and keep the Director and Key Individual informed of POPIA obligations, risks, and incidents (including security compromises). ▪ Act as the central accountability function for POPIA within Money Doc. ▪ Continually analyse regulatory requirements and ensure alignment with organisational practices.
2	***Compliance framework and policy management***	▪ Ensure that a POPIA compliance framework is developed, implemented, monitored and maintained. ▪ Review and update: Privacy policies; information protection procedures; and related governance documents. ▪ Ensure alignment between legal requirements and operational processes.
3	***Risk management and impact assessments***	▪ Ensure that Personal Information Impact Assessments (PIIAs) are conducted. ▪ Identify and manage privacy risks and processing risks. ▪ Ensure appropriate security safeguards and controls are implemented. ▪ Ensure that POPIA audits are conducted regularly and remedial actions are implemented.
4	***Data subject rights, requests and accessibility***	▪ Ensure that Money Doc: · Has adequate systems to process requests for access, correction or deletion of personal information; and · Makes it easy for data subjects to submit requests and complaints (e.g., website contact channels). ▪ Handle and respond to all POPIA-related requests and complaints. ▪ Provide copies of the PAIA manual upon request (subject to prescribed fees).

5	***PAIA compliance***	▪ Ensure that the PAIA manual is developed, maintained and made available as required ▪ Oversee compliance with PAIA access to information obligations.
6	***Training, awareness and culture***	▪ Ensure that employees and representatives: · Are aware of POPIA obligations and risks; and · Understand security controls and data handling requirements. ▪ Organise and oversee ongoing POPIA training and awareness programmes. ▪ Address internal POPIA-related queries and guidance requests.
7	***Third-party and contractual oversight***	▪ Review and approve: · Contracts with operators and third parties; and · Employment contracts and service agreements impacting personal information. ▪ Ensure that: · Appropriate data protection clauses are included; and · Third parties comply with POPIA obligations.
8	***Monitoring, assurance and internal controls***	▪ Monitor Money Doc's ongoing compliance status. ▪ Ensure: · Adequate internal measures and controls exist; and · Compliance gaps are identified and addressed. ▪ Maintain records and evidence of compliance.
9	***Engagement with the Information Regulator***	▪ Act as the official point of contact with the Information Regulator. ▪ Cooperate in investigations and regulatory enquiries ▪ Provide guidance to Money Doc on regulatory expectations and enforcement risks.

9.3 Deputy Information Officer

The Deputy Information Officer will assist the Information Officer in performing their duties as set out in their appointment letter.

9.4 Information Technology and Security

Money Doc's Director and Key Individual is responsible for ensuring that Money Doc's information security management framework is developed, implemented, managed and maintained, including but not limited to:

- Ensuring that Money Doc's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Ensuring that personal information being transferred in bulk is appropriately electronically encrypted.
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.

- Performing regular IT audits to ensure that the security of Money Doc's hardware and software systems are functioning properly.
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on Money Doc's behalf. For instance, cloud computing services.

9.5 Employees and other Persons acting on behalf of Money Doc

Employees are responsible for:

	Area of responsibility	Responsibilities
1	***Confidentiality and responsible handling of personal information***	Employees and all persons acting on behalf of Money Doc must: ▪ Treat personal information as a confidential business asset. ▪ Respect the privacy rights of data subjects. ▪ Not disclose, use, or share personal information, internally or externally, unless required to perform their duties or authorised ▪ Escalate uncertainties to line management, or the Information Officer.
2	***Lawful processing of personal information***	Employees may only process personal information where a lawful basis exists, including: ▪ Consent of the data subject; ▪ Contractual necessity; ▪ Legal obligation; ▪ Protection of data subject interests; and ▪ Legitimate interests of Money Doc or a third party.
3	***Consent management and transparency***	Employees must ensure that: ▪ Personal information is processed only after informed, specific and voluntary consent is obtained (where required). ▪ Data subjects: · Understand the purpose of processing; and · Know how their information will be used and shared ▪ Consent is documented (written or recorded) and obtained directly from the data subject (with limited exceptions).
4	***Purpose limitation and minimality***	Employees must: ▪ Only collect and process personal information necessary for their role and relevant to the purpose. ▪ Not access or process personal information outside their job responsibilities.
5	***Secure handling of personal information (operational controls)***	▪ Implement access and device security · Use password protection and secure devices; · Lock screens when unattended; and · Do not share login credentials. ▪ Store and physical security

		· Store electronic data on authorised systems only and ensure that hard copies are in secure, restricted locations; and · Ensure that removable media is securely stored. ▪ Securely share personal information · Do not share personal information informally; and · Ensure the encryption of personal information, where required, and authorisation is obtained before sharing personal information. ▪ Not conduct any prohibited behaviours · Employees must not store personal information on personal devices, share personal information via insecure channels or transfer personal information outside of South Africa without approval.
6	***Data quality and accuracy***	Employees must: ▪ Take reasonable steps to ensure personal information is accurate, complete and up to date; and ▪ Escalate updates or corrections through line management or the Information Officer.
7	***Retention and destruction***	Employees must: ▪ Ensure personal information is retained only as long as necessary; and ▪ Seek authorisation before deleting or disposing of information.
8	***Information minimisation and control***	Employees must: ▪ Avoid creating duplicate records and maintaining unnecessary datasets; and ▪ Ensure personal information is stored in as few locations as possible.
9	***Training and awareness***	Employees must: ▪ Participate in POPIA awareness training; and ▪ Stay informed about risks, security practices and data protection requirements.
10	***Incident identification and escalation***	Employees must immediately report any actual breaches or suspected breaches, including: ▪ Unauthorised access; ▪ Loss or destruction of information; and ▪ Accidental disclosure

10 POPIA AUDIT

Money Doc's Information Officer will schedule a POPIA Audit to be conducted annually. The purpose of a POPIA audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information.
- Determine the flow of personal information throughout Money Doc. For instance, Money Doc's various business units, divisions, branches and other associated organisations.
- Redefine the purpose for gathering and processing personal information.
- Ensure that the processing parameters are still adequately limited.
- Ensure that new data subjects are made aware of the processing of their personal information.

- Re-establish the rationale for any further processing where information is received via a third party.
- Verify the quality and security of personal information.
- Monitor the extend of compliance with POPIA and this policy.
- Monitor the effectiveness of internal controls established to manage Money Doc's POPI related compliance risk.

In performing the POPIA Audit, the Information Officer will liaise with line managers in order to identify areas within in Money Doc's operation that are most vulnerable or susceptible to the unlawful processing of personal information. The Information Officer will be permitted direct access to and have demonstrable support from line managers and Money Doc's Director and Key Individual in performing their duties.

11 REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:

- Request what personal information Money Doc holds about them and why;
- Request access to their personal information; and
- Be informed how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a **"Personal Information Request Form".**

In addition, where the data subject requests the correction, deletion or destruction of a record of personal information, the Information Officer will provide the data subject with **Form 2** to the Regulations of POPIA. The Information Officer must render such reasonable assistance, as is necessary free of charge, to enable a data subject to complete **Form 2**. The Information Officer will process all requests within a reasonable time.

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against Money Doc's PAIA Manual.

12 POPIA COMPLAINTS PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. Money Doc takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- POPIA complaints must be submitted to Money Doc in writing by sending an e-mail to the Information Officer at Mark@moneydoc.africa.
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within one (1) working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within two (2) working days.
- The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on Money Doc's data subjects.
- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with Money Doc's Director and Key Individual where after the affected data subjects and the Information Regulator will be informed of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to Money Doc's Director and Key Individual within seven (7) working days of receipt of the complaint. In all instances, Money Doc will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

- The Information Officer's response to the data subject may comprise any of the following:
    - A suggested remedy for the complaint, or
    - A dismissal of the complaint and the reasons as to why it was dismissed.
- An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.

The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPIA-related complaints.

13 DISCIPLINARY ACTION

Where a POPIA complaint or a POPIA breach investigation has been finalised, Money Doc may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy. Examples of immediate actions that may be taken subsequent to an investigation include, but is not limited to:

- A recommendation to commence with disciplinary action;
- A referral to appropriate law enforcement agencies for criminal investigation; and
- Recovery of funds and assets in order to limit any prejudice or damages caused.

In the case of ignorance or minor negligence, Money Doc will undertake to provide further awareness training to the employee. Any gross negligence or the wilful mismanagement of personal information will be considered a serious form of misconduct for which Money Doc may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer:	
Name	Mark Sluzki
Contact Number	+27 83 297 6535
Email Address:	Mark@moneydoc.africa

Please be aware that we may require you to provide proof of identification prior to processing your request.

There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	

B. Request	
I request Money Doc to:	
(a) Inform me whether it holds any of my personal information	☐
(b) Provide me with a record or description of my personal information	☐

C. Instructions

D. Signature Page
Signature
Date

ANNEXURE B: POPIA PRIVACY NOTICE

POPIA PRIVACY NOTICE

We understand that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us and we are committed to safeguarding and processing your information in a lawful manner.

We also want to make sure that you understand how and for what purpose we process your information. If for any reason you think that your information is not processed in a correct manner, or that your information is being used for a purpose other than that for what it was originally intended, you can contact our Information Officer.

You can request access to the information we hold about you at any time and if you think that we have outdated information, please request us to update or correct it.

Our Information Officer's Contact Details	
Name	Mark Sluzki
Contact Number	+27 83 297 6535
Email Address:	Mark@moneydoc.africa

Our details:

Money Doc (Pty) Ltd

Physical address: Ground Floor South Block, 26 Baker Street, Rosebank, Johannesburg, 2196

Telephone: +27 83 297 6535

E-mail address: treasuryadmin@moneydoc.africa

The source of collection of your personal information:

We collect personal information directly / indirectly from the following data subjects:

- Prospective clients who enquire about our services
- Clients (individuals and companies), including the directors, shareholders, beneficial owners and authorised signatories of corporate clients

Personal information is collected directly from you through the completion of our client onboarding and FICA documentation and mandates, and through e-mail and other correspondence with us.

We may also collect information about you from other sources such as external third parties and from cookies on our website.

Law authorising or requiring collecting of the personal information:

As an authorised financial services provider, we are obligated in terms of the following legislation to collect your personal information insofar as it relates to the rendering of the relevant financial services to you:

the Financial Advisory and Intermediary Services Act 37 of 2002, the Financial Intelligence Centre Act 38 of 2001, the Currency and Exchanges Act 9 of 1933 and the Exchange Control Regulations, and the Income Tax Act 58 of 1962.

Purpose for Processing your Information:

We collect, hold, use and disclose your personal information mainly to provide you with access to the services and products that we provide. We will only process your information for a purpose you would reasonably expect, including:

- Complying with the obligations contained in the contract concluded between yourself and Money Doc.
- To facilitate your foreign exchange and cross-border payment transactions with authorised dealers and other counterparties on your instruction.
- To verify your identity and conduct client due diligence as required by the Financial Intelligence Centre Act.
- To confirm, verify and update your details.
- To comply with any legal and regulatory requirements.

Some of your information that we hold may include, your first and last name, email address, a home, postal or other physical address, other contact information, your title, birth date, gender, occupation, qualifications, past employment, residency status, your investments, assets, liabilities, insurance, income, expenditure, family history, medical information and your banking details.

Third parties and your personal information

We may need to share your information to third parties provide advice, reports, analyses, products or services that you have requested. Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us.

These third parties may include:

- Your employer (where applicable);
- Analytics and search engine providers assisting in the enhancement of our websites;
- Information Technology specialists assisting us with data storage, security, processing, analytics, etc;
- Auditors of Money Doc;
- Regulatory or governmental authorities, including the South African Reserve Bank, the Financial Intelligence Centre, the Financial Sector Conduct Authority and the South African Revenue Service;
- Authorised dealers (banks), counterparties and payment partners through which your transactions are concluded, including banks and payment partners outside South Africa where you instruct a cross-border payment.

The Transfer of your personal information outside of the Republic of South Africa

Your information may be hosted on servers managed by third-party service providers, which may be located outside of South Africa. Our third-party cloud storage providers are:

- Apple (iCloud), Microsoft (OneDrive) and Dropbox. These providers may store information on servers located outside South Africa, including in the United States of America and the European Union.

We confirm that the level of protection afforded to your personal information by that third country or international organisation is equal to the protection afforded by the POPI Act.

Complaints and objections

As a data subject, you have the right to –

- Request that we confirm, free of charge, whether or not we hold personal information about you;
- Request that we provide you with a description of the personal information we hold about you, and to explain why and how it is being processed (please complete Annexure A);
- Request that we consider your objections to the processing of your personal information (using Form 1 of the POPIA Regulations);
- Lodge a complaint with the Information Regulator (using Form 5 of the POPIA Regulations).

The Information Regulator

In the event that your personal information has not been processed in accordance with the POPI Act and the principles set out above, you have the right to lodge a complaint with the Information Regulator.

For further information regarding the complaints process, please visit the website of the Information Regulator, as indicated below.

Alternatively, you may contact the Information Regulator for further assistance:

The Information Regulator (South Africa)

Physical Address: Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191

Email: POPIAComplaints@inforegulator.org.za | Telephone: 010 023 5200

Website: https://inforegulator.org.za