OPSI PRIVACY POLICY

Version 1. 0

30th June 2021

OPSI Systems

Table of Contents

1 Document Control

1.1 Change History

Revision	Date	Author	Description
V1.0	2021/06/30	Sean Aspoas, Rick de Klerk	First released version of the document. Based on template and comments from iOCO. Added sections regarding Special Personal Information, Data of Children, Direct Marketing, Automated Processing, and Transferal of Data. Updated the definitions. Miscellaneous additions and changes.

2 Abbreviations & Definitions

Term	Stands For
OPSI	Opsi Systems (Pty) Ltd and its subsidiaries, including but not limited to OPSI Africa (Pty) Ltd
Data Protection Laws	Means all applicable law relating to data protection, privacy and security when processing Personal Information under the Agreement. This includes without limitation applicable international and local data protection, privacy, export or data security directives including the Electronic Communications and Transactions Act 25 of 2002, Protection of Personal Information Act 4 of 2013 (POPIA) and the General Data Protection Regulation. (GDPR)
Personal Information	Personal data is any data recorded electronically or in hard copy, that if viewed on its own, or collectively with other data, can be used to uniquely identify an individual or a legal entity.
Processing	Means any operation, or set of operations, performed on Data, by any means, such as by collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction and "Processing" shall have a corresponding meaning.
GDPR	General Data Protection Regulation
POPIA	Protection of Personal Information Act
Information Officer (IO)	The Information Officer (IO) as required and defined by POPIA, also filling the role of Data Protection Officer (DPO) for GDPR requirements.
Child	A natural person under the age of 18 years.
Data subject	A natural person to whom Personal Information relates. In the context of POPIA, this also includes juristic persons.
Data Protection Officer (DPO)	See Information Officer (IO).
Privacy Notice	A statement made to a data subject that describes how the organization collects, uses, retains, and discloses Personal Information. A Privacy Notice is sometimes referred to as a Privacy Statement.

3 Introduction

Data protection and privacy through lawful, legitimate and responsible processing and use of personal data is a fundamental human right under the South African Constitution. The OPSI Privacy Policy outlines the core principals which OPSI endeavours to pursue in relation to the processing of personal data.

The principals set out in this Policy ensure that personal data is processed in line with regulatory requirements, industry-wide best practices, and our code of conduct. The Protection of Personal Information Act (POPI Act or POPIA) and the General Data Protection Regulation (GDPR) are the primary pieces of legislation that governs how OPSI collects and processes personal data.

4 Purpose

The purpose of this OPSI Policy is to set out the basic principles relating to the processing of Personal Information. This Policy sets out how OPSI process the personal data of its staff, trading partners, suppliers, and other third-parties.

5 Scope

- This policy applies to OPSI, its subsidiaries, affiliates and business employees (i.e. employees, directors, senior managers, executives, temporary staff members, agents, consultants, seconded, home-based, casual and agency staff, volunteers and interns), OPSI service providers and OPSI business associates and partners.
- This policy is intended to assist the directors, officers, employees, and appointed agents of OPSI in assessing the legal position applicable to a particular decision, behaviour, conduct, act or omission.

6 Consequences of non-compliance

- Wilful and deliberate non-compliance with this policy can expose OPSI to significant regulatory sanctions, fines, criminal and/or civil liability. The reputational damage arising from such non-compliance will negatively affect OPSI's ability to attract and maintain clients.
- Employees who fail to comply with this policy may be subject to disciplinary action including dismissal and personal liability such as fines and/ or imprisonment under the relevant laws.

7 Governance and Implementation

- This policy must be approved by the OPSI Board of Directors.
- This policy should be reviewed every two years or when a significant event occurs, considering any changes to regulatory requirements and business operations.
- The Executives and Management of OPSI are responsible for the successful implementation of the provisions of this policy.

8 Roles and responsibilities

Assigning roles and responsibilities is necessary to give effect to the requirements of this policy:

8.1 Information Officer

The OPSI Information Officer (IO) is accountable for ensuring that OPSI and its employees comply with the requirements set out in this process.

- The IO is responsible for:
    - Overseeing all dispensations, waivers, and breaches to or of this process.
    - Facilitating the review(s) as set out in the policies or standards.
    - Ensuring this policy is effectively implemented within OPSI.
    - Communicating with data subjects.
    - Working with the regulator in relation to investigations and audits.
- The IO may delegate their responsibility (but not accountability) for implementation of this policy to an appropriate OPSI executive.

8.2 Board of Directors

- The OPSI Board of Directors is ultimately accountable for ensuring that OPSI and its employees comply with the requirements set out in this policy; and
- In addition, the board must ensure that OPSI complies with all applicable laws, regulations, and supervisory requirements.

8.3 Employees

- All employees within OPSI are responsible for complying with this policy.

9 Policy Principles

9.1 Processing of Data

OPSI's core principles are based on the provisions of POPI and GDPR and must ensure that all personal data is:

- Processed lawfully, fairly and in a transparent manner.
- Collected only for specified, clear and legitimate purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed.
- Accurate and kept up to date where applicable.
- Not kept in a format which allows identification of a data subject for longer than is necessary for the purposes for which the data is processed.
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Additionally, OPSI must ensure that:

- Personal Information is not transferred to another country without appropriate safeguards being in place.
- OPSI allows people to exercise their rights in relation to their personal data. OPSI is responsible for and must be able to demonstrate compliance with all the above principles.

9.1.1 Automated Decision Making

- OPSI only performs automated decision making using Personal Information with the express consent of the data subject, or where such automated decision making is clearly stipulated in an agreement between OPSI and the data subject.

9.1.2 Transferal of Information

Personal Information may not be transmitted beyond the borders of the Republic of South Africa, or beyond the boards of a European country subject to GDPR, without confirming that the transferal adheres to the following criteria:

- The third-parties or services that the data is transferred to adhere to laws and/or policies which are at least as protective as POPIA or GDPR respectively; or
- That the third-parties or services are governed by an agreement with OPSI that dictates the processing of Personal Information in line with the conditions of this Privacy Policy and applicable privacy notices.

9.2 Lawfulness, Fairness and Transparency

When collecting and processing Personal Information for any specific purpose, OPSI must always have a lawful basis for doing so. For processing Personal Information to be lawful, at least one of the following circumstances must be met:

- The data subject has given their consent for one or more specific purposes.
- The processing is necessary for the performance of a contract to which the data subject is a party.
- To comply with OPSI's legal obligations.
- To protect the vital interests of the data subject or another person.
- To pursue OPSI's legitimate interests where those interests are not outweighed by the interests and rights of the person.

OPSI should document the above lawful reasons relied upon when processing Personal Information for each specific purpose.

9.3 Consent as a lawful basis for processing

Consent may not always be the only basis for being able to process data. This will depend on the specified circumstance or scenario. A person's consent must be:

- Specific.
- Informed (explained in plain and accessible language).
- Unambiguous.
- Separate and unbundled from any other terms and conditions provided to the data subject.
- Freely and genuinely given.

9.3.1 Direct Marketing

OPSI may collect the information of persons who have contacted OPSI via marketing channels for information or to initiate a business relationship. OPSI may use such information to communicate with the customer for direct marketing, but only under the following criteria:

- The information collected and purpose for use is expressly communicated to the customer.
- Consent for contact was obtained from the customer.
- The communication contains contact details for OPSI to ensure the customer is aware of who is contacting them.
- The communication is limited to the purpose that the customer agreed to, based on the context of the channel of communication.

- Such data will be deleted following communication with the customer for the purpose described unless retention of the information is required either to render ongoing product and/or business-related services, or for which the customer has agreed.
- That the customer has the means to opt-out of any communications that they receive.

9.4 Openness

- A person must be able to withdraw their consent without reservation. Once consent has been given, it will need to be updated where OPSI wishes to process the personal data for a new purpose that is not compatible with the original purpose for which they were collected.
- Chapter 6 of POPIA and Chapter 3 Section 1 of GDPR requires OPSI to ensure that any information provided by OPSI to people about how their personal data will be processed (a Privacy Notice) is concise, easily accessible, easy to understand and written in plain language.
- OPSI must demonstrate transparency by providing people with the appropriate Privacy Notices before it collects and processes their Personal Information and at the appropriate times throughout the processing of their Personal Information.
- Where OPSI obtains any Personal Information about a person from a third party (for example, CVs from recruitment or background criminal checks in relation to employee on-boarding) it must check that it was collected by the third party in accordance with this policy's requirements that the sharing of such Personal Information with OPSI was clearly explained.

10 Data Minimisation

- The Personal Information that OPSI collects and processes must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.
- Personal Information must only be processed when necessary for the performance of duties and tasks and not for any other purposes.
- Accessing of Personal Information where there is no authorisation to do so, or where there is no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offence.
- When collecting Personal Information, as required for the performance of duties and tasks, there should not be a request that a person provides more Personal Information than is necessary for the intended purposes.
- Where Personal Information is no longer needed for the specific purposes for which it was collected, such information must be deleted, destroyed and/ or anonymised according to OPSI's 'Data and Record Retention and Disposal Policy' and OPSI's 'Information, Data Management and Control Policy' .

10.1 Special Personal Information

OPSI, in line with the requirements of POPIA, will restrict the collection of special Personal Information to only that which is necessary under legal obligations and with explicit consent of the individual.

Special Information includes the following:

- Religious or philosophical beliefs
- Race or ethnic origin
- Trade union membership
- Political persuasion
- Health and sex life
- Criminal records
- Biometric information

10.2 Data of Children

Information of children will only be collected in line with the criteria set in Chapter 3, Part C, Section 35 of POPIA, which includes:

- Carried out with the prior consent of a competent person.
- Necessary for the establishment, exercise, or defence of a right or obligation in law.
- Necessary to comply with an obligation of international public law.
- For historical, statistical or research purposes to the extent that:
    - The purpose serves a public interest and the processing is necessary for the purpose concerned, or it appears to be impossible or would involve a disproportionate effort to ask for consent; and
    - Sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
- Personal Information which has deliberately been made public by the child with the consent of a competent person.

11 Accuracy

- Personal Information that OPSI collects and processes must be:
    - Accurate and, where required, kept up to date; and
    - Corrected and/or deleted, without delay, where an error has been discovered.
- Where appropriate, any inaccurate or expired records should be deleted or destroyed.

12 Storage Limitation

- The Personal Information that OPSI collects and processes must not be kept in a form that identifies a person for longer than what is necessary in relation to the purposes for which it was collected (this is subject to compliance with any legal, accounting or reporting requirements).
- There must be a regular review of any Personal Information which has been processed in the performance of duties to assess whether the purposes for which the information was collected has expired.
- Where appropriate, reasonable steps must be taken to delete or destroy any personal data that OPSI no longer requires in accordance with OPSI's 'Data and Record Retention and Disposal Policy' and OPSI's 'Information, Data Management and Control Policy'.
- All Privacy Notices should inform data subjects of the period for which their personal data will be stored or how such period will be determined.

13 Security of Personal Information

- The Personal Information that OPSI collects and processes must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage, and against unauthorised or unlawful processing.
- OPSI must develop, implement, and maintain appropriate technical and organisational measures for the processing of Personal Information considering the:
    - Nature, scope, context, and purposes for such processing; and
    - The volume of Personal Information processed, and the likelihood and severity of the risks of such processing for the rights of persons.

- OPSI must regularly evaluate and test the effectiveness of such measures to ensure that they are adequate and effective. There is a responsibility for ensuring the security of Personal Information processed throughout the performance of duties.
- All procedures that OPSI has put in place to maintain the security of Personal Information, from collection to destruction, must be observed and adhered to.
- Confidentiality, integrity, and availability of Personal Information must be maintained at all times:
    - Confidentiality means that only people who need to know and are authorised to process any Personal Information can access it.
    - Integrity means that Personal Information must be accurate and suitable for the intended purposes.
    - Availability means that those who need to access the Personal Information for authorised purposes can do so.
- Sharing Personal Information with third parties is prohibited unless:
    - OPSI has agreed to this in advance; and
    - There has been an issuance to the respective person, of a Privacy Notice, beforehand and where such third party is processing the Personal Information on OPSI's behalf.

14 Persons' Rights

- Chapter 3(5) of POPIA and Chapter 3 of GDPR provides people with several rights in relation to their information. These rights include:
    - The right to withdraw consent unconditionally.
    - The right to be informed about how OPSI collects and processes Personal Information.
    - The right to, on request, receive a copy of the Personal Information that OPSI holds.
    - The right to have, on request, inaccurate personal data corrected or incomplete information completed.
    - The right to ask OPSI to delete or destroy Personal Information if the Personal Information is no longer necessary in relation to the purposes for which it was collected, consent has been withdrawn (where applicable), a person has objected to the processing, the processing was unlawful, the Personal Information has to be deleted to comply with a legal obligation and/or the Personal Information was collected from a person under the age of 13 and they have reached the age of 13.
    - The right to restrict processing if there is a reasonable belief that the personal data is inaccurate.
    - The right to receive or ask OPSI to transfer Personal Information to a third party.
    - The right to be notified of a Personal Information breach.
    - The right to make a complaint to the Data Protection Authority (GDPR), the Information Regulator of South Africa (POPIA) or another appropriate supervisory authority.

15 Data Protection

- A Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment, is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data. DPIAs are required for processing Personal Information likely to result in a high risk to the individuals. A DPIA must:
    - Describe the nature, scope, context, and purposes of the processing.
    - Assess necessity, proportionality, and compliance measures.
    - Identify and assess risks to individuals.
    - Identify any additional measures to mitigate those risks.

16 Record Retention

All records pertaining to this policy should be retained in accordance with OPSI's 'Data and Record Retention and Disposal Policy' and OPSI's 'Information, Data Management and Control Policy'.

--- End of Document ---