Solution House Software (Pty) Ltd

PRIVACY STATEMENT AND AGREEMENT

BETWEEN

SOLUTION HOUSE SOFTWARE (PTY) LTD
(Hereinafter referred to as SHS/The Operator)

AND

_____
(Hereinafter referred to as The Customer/The Responsible Party)

May 2021

Version: 1.1

1. Introduction and Purpose

1.1 SHS is a company functioning within the software service industry which is obligated to comply with The Protection of Personal Information Act 4 of 2013 (herein referred to as POPIA/The Act).

1.1.1 Under the Act SHS is defined as an Operator

1.1.2 An End-User Customer is defined as the Responsible Party.

1.2 SHS guarantees its commitment to protecting the consumer's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws, both within South Africa and outside of it.

1.3 The purpose of this agreement is to inform customers of the SHS POPI Compliance Protocols, and to inform them regarding their own obligations under the Act.

1.3.1 It is the responsibility of The Customer to ensure they are familiar with the aspects of the POPI Act which apply to them

1.3.2 This agreement will provide a reasonable level of understanding regarding the Act and the data of which we facilititate collection, but SHS cannot be held liable for ensuring the comprehensive understanding of either The Customer or The Reseller and any breach that occurs on their part.

1.4 Under The Act, a significant portion of the burden of compliance rests with the the Responsible Party. It is important that all Responsible Parties familiarize themselves with the legislation and modify their Data Processes to ensure compliance.

2. Definitions

The list of definitions an dits contents has been limited to those applicable to the data collected by SHS on behalf of The Customer:

2.1 Data Subject means the person to whom personal information relates;

2.2 POPIA refers to the Protection of Personal Information Act 4 of 2013;

2.3 Responsible Party means a public or private body or any other person which, alone or in conjunction with others determines the purpose of and means for processing personal information.

2.4 Operator means a person who processes personal information on behalf of the responsible party.

2.5 Processing means any operation or activity, whether or not by automatic means, concerning personal information, including:

a) The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use of data
b) Dissemination by means of transmission, distribution or making available in any other form

2.6 Record means any recorded information

a) Regardless of form or medium, including any of the following:
    i) 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
    ii) 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; in the possession or under the control of a responsible party
b) Whether or not it was created by a responsible party and
c) Regardless of when it came into existence.

2.7 Personal Information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including:

a) Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, sexual orientation, age, physical or mental health, wellbeing, disability
b) Information relating to the education or the medical, financial, criminal or employment history of the person
c) Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person
d) The biometric information of the person

3. Policy Statement and Responsibilities

SHS guarantees its commitment to protecting The Customer and the Data Subjects' privacy and ensuring their Personal information is used appropriately, transparently, securely and in accordance with applicable laws, as far as it applies to our specific industry.

4. Data Subject Rights with regard to Protection of Personal Information.

4.1 Data Subjects have the following rights

a) Objection to the use of personal information
b) Notification if information is being used for something other than what was consented for

c) Establishing whether the responsible party holds information
d) Requesting that information can be corrected, destructed or deleted
e) Refusing processing for direct marketing by unsolicited electronic communications
f) Lodging a complaint with the Information Regulator
g) Instituting civil proceedings.(Sec 99)

5. The Information Regulator

5.1 Data Subjects have right of recourse with the Information Regulator, in the event that their Personal Information is compromised.

5.1.1 The Regulator has jurisdiction throughout the Republic, is independent and subject only to the Constitution and accountable to the National Assembly

5.1.2 Minor Offences imposed by the Regulator can be a fine and/or imprisonment up to 12 months

5.1.3 Major Offences imposed by the Regulator can be a fine and/or imprisonment up to 10 years.

6. The SHS Commitment to Safeguarding Client and Consumer Information.

It is a requirement of POPIA to adequately protect the Personal Information we hold and to avoid unauthorized access and use of said Personal information.

We will continuously review our security controls and processes to ensure that all Personal Information we hold is secure. The following procedures are in place in order to protect the Data Subjects' Personal Information

6.1 Policies and Procedures

6.1.1 Privacy Agreement
6.1.2 Privacy Statement
6.1.3 Incident Response Policy and plan
6.1.4 Terms of Service
6.1.5 Staff Training
6.1.6 Incident Register
6.1.7 Non-Disclosure Agreements (Staff)
6.1.8 End User Agreement
6.1.9 Password Policy

6.2 Physical Security

6.2.1 Physical Computer Hardware refers to, but is not limited to:
Desk Tops; Laptops; Tablets; Cell phones; Memory Sticks, USB Ports, all other Mobile Devices; Printers and Shredders.

6.2.2 SHS has a Password Policy regarding all hardware, ensuring the following:

6.2.2.1 All Devices and Computers are Password Protected

6.2.2.2 No staff member may leave their device/computer unattended without first ensuring it is properly locked and password protected

6.2.2.3 All Passwords are carefully selected to ensure maximum security

6.2.2.4 Passwords are changed on a regular basis

6.2.2.5 No passwords are stored physically or electronically in a manner which could be vulnerable to unauthorized acces

6.2.2.6 No devices are permitted to be left in vehicles or public spaces where they would be vulnerable to unathourised access

6.2.2.7 Staff found to be in contravention of this policy will be subject to immediate disciplinary action

6.2.3 Access to the SHS premises is limited with physical security measures deemed reasonable and in accordance with standard practice within South Africa. This may include:

6.2.3.1 Alarm System

6.2.3.2 Premises Secured with walls, gates and electric fencing

6.3 Employees:

6.3.1 All employees have signed Non-Disclosure Agreements preventing them from sharing any of the information to which they have access through the normal execution of their duties

6.3.2 All employees have received training regarding POPIA and the Internal Procedures for ensuring compliance

6.3.3 Non-compliance with SHS's procedures is grounds for disciplinary action and/or dismissal and this is stated in all employment contracts

6.4 All consumer information is stored off site by a Third party Service Provider, with whom SHS has a Service Level Agreement in place, and whose Privacy Policies are known to SHS and, to the best of our knowledge, believed to be strictly enforced.

6.5 All electronic files or data are backed up by the IT Service Provider who is also responsible for system security which protects third party access and physical threats.

6.6 Consent to process consumer information is obtained from consumers through information exchange with the security guards, field workers or client staff.

6.6.1 Consent is tacit, and is achieved through the Data Subject exchanging information with client security guards, field workers or client staff and allowing their photo to be taken.

6.6.2 Consumers are entitled to refuse consent: the operational response to this is risk dependant and entirely at the discretion of the site

owner/manager. SHS cannot and does not recommend any specific course of action in this regard.

6.7 Where consent to process consumer information cannot be obtained from consumers, Section 11(1)(f) provides that a responsible party may process personal information if such processing is necessary for a legitimate interest pursued by the responsible party. Public safety, security and rendering municipal services fall within the parameters of constituting a legitimate interest.

6.8 The SHS Privacy Policy and other relevant documentation is available in full upon request, should you wish to view it

7. The Obligations of the Responsible Party and Co-Operator

7.1 As stated in 1.1 of this document:

7.1.1 If you are the End User Customer, you are the RESPONSIBLE PARTY under the Act.

7.2 Responsible Party

The significant burden of compliance rests with the Responsible Party
The Responsible Party is obligated regarding the following, details as per section 4 above:

7.2.1 Appointing an Information Officer whose responsibility it is to ensure compliance and to enforce it within the organization

7.2.2 Determining the specific purpose for data collection and/or processing, and ensuring that the conditions set out in the Act are complied with:

7.2.2.1 The purpose must be explicit, lawful and explained to the data subject

7.2.3 Knowing the processing limitations:

7.2.3.1 Data subjects must consent
7.2.3.2 Must process to protect the legitimate interest of data subject
7.2.3.3 Must pursue a legitimate interest
7.2.3.4 Data subject may withdraw consent or object on reasonable grounds.

7.2.4 Understanding Record Retention

7.2.4.1 Data must not be retained any longer than necessary
7.2.4.2 Personal Information must be destroyed, deleted or de-identified as soon as is reasonably practical.

7.2.5 Limiting Collection and Further Processing

7.2.5.1 Must be in accordance or compatible with the purpose for which it was collected.

7.2.5.2 Information will not be collected indiscriminately, but by fair and lawful means, and be limited to what is necessary to ensure security and/or management of their site

7.2.6 Openness, ensuring the Data Subject is aware of:

7.2.6.1 The information being collected

7.2.6.2 The name and address of the Responsible Party and the Operator

7.2.6.3 The purpose for which the information is being collected

7.2.6.4 Whether or not the supply of the information is voluntary or mandatory

7.2.6.5 The consequences of failure to provide the information

7.2.6.6 The right of access to and the right to rectify the information collected

7.2.6.7 The right to object to the processing of the information

7.2.7 Security Safeguards

7.2.7.1 The Responsible Party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical organisational measures.

7.2.8 The Data Subject may request responsible party to:

7.2.8.1 Correct or delete information which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully

7.2.8.2 Delete or destroy information that the responsible party is no longer authorised to retain

7.2.9 The Information Officer shall ensure that:

7.2.9.1 All employees and volunteers know the importance of keeping personal information confidential

7.2.9.2 Care is taken when personal information is disposed of or destroyed to prevent unauthorized parties from gaining access to it

7.2.10 The Responsible party should notify data subject and Regulator of any breach of data.

7.3 Operator

As Operator you are responsible for ensuring that your handling of any and all data is in accordance with the Act. Whilst absolved of the responsibility of

determining the reasons and data to be collected, you are nonetheless obligated regarding the following:

7.3.1 Appointing an Information Officer whose responsibility it is to ensure compliance and to enforce it within the organization

7.3.2 Knowing the processing limitations:
- 7.3.2.1 Data subjects must consent
- 7.3.2.2 Must process to protect the legitimate interest of data subject
- 7.3.2.3 Must pursue a legitimate interest
- 7.3.2.4 Data subject may withdraw consent or object on reasonable grounds.

7.3.3 Understanding Record Retention
- 7.3.3.1 Data must not be retained any longer than necessary
- 7.3.3.2 Personal Information must be destroyed, deleted or de-identified as soon as is reasonably practical.

7.3.4 Limiting Collection and Further Processing
- 7.3.4.1 Must be in accordance or compatible with the purpose for which it was collected.
- 7.3.4.2 Information will not be collected indiscriminately, but by fair and lawful means, and be limited to what is necessary to ensure security and/or management of their site

7.3.5 Openness, ensuring the Data Subject is aware of:
- 7.3.5.1 The information being collected
- 7.3.5.2 The name and address of the Responsible Party and the Operator
- 7.3.5.3 The purpose for which the information is being collected
- 7.3.5.4 Whether or not the supply of the information is voluntary or mandatory
- 7.3.5.5 The consequences of failure to provide the information
- 7.3.5.6 The right of access to and the right to rectify the information collected
- 7.3.5.7 The right to object to the processing of the information

7.3.6 Security Safeguards
- 7.3.6.1 The Operator must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical organisational measures.

7.3.7 The Data Subject may request responsible party to:

7.3.7.1 Correct or delete information which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully

7.3.7.2 Delete or destroy information that the responsible party is no longer authorised to retain

7.3.8 The Information Officer shall ensure that:

7.3.8.1 All employees and volunteers know the importance of keeping personal information confidential

7.3.8.2 Care is taken when personal information is disposed of or destroyed to prevent unauthorized parties from gaining access to it

7.3.9 The Operator, together with the Responsible Party, should notify data subject and Regulator of any breach of data.

8. Practical Applications of Obligations

8.1 This is merely intended as a guideline and is in no way exhaustive. The onus is upon the Responsible Party and Co-Operator, where applicable, to ensure their full compliance with POPIA and other relevant legislation

8.2 The parties should ensure that an adequate risk assessment is completed and that the following policies and procedures, at an absolute minimum, are in place:

8.2.1 Privacy Policy
8.2.2 Incident Response Policy and plan
8.2.3 Complaints Policy
8.2.4 Incident Register
8.2.5 Staff Non-Disclosure Agreements
8.2.6 Password Policy

8.3 Physical Security

8.3.1 Physical Computer Hardware refers to, but is not limited to:
Desk Tops; Laptops; Tablets; Cell phones; Memory Sticks, USB Ports, all other Mobile Devices; Printers and Shredders.

8.3.1.1 All Devices and Computers must be adequately password protected

8.3.1.2 No staff member should leave their device/computer unattended without first ensuring it is properly locked and password protected

8.3.1.3 Passwords must be changed on a regular basis

8.3.1.4 No passwords should be stored physically or electronically in a manner which could be vulnerable to unauthorized access

8.4 Employees

8.4.1 All employees dealing with the Personal Information of the Data Subject should receive adequate training on POPIA and its implications

8.4.2 All employees should sign Non-Disclosure Agreements preventing them from sharing any of the information to which they have access through the normal execution of their duties

8.4.3 No employee should be entitled to hold, for any length of time, the identity documents of a Data Subject, under any circumstances whatsoever. Once the document has been scanned there is no reasonable purpose for such, and is considered a serious breach of POPIA

8.4.4 Only duly authorized employees should be given access to the SHS backend, dashboards and reports, and the passwords and login details for the SHS site should be carefully guarded by the Operations/Site/Security/Facilities Manager

8.5 Data Feedback Reports

8.5.1 All Data Feedback reports must be sent to the absolute minimum number of people: those with the need to see information in order to make decisions on the operational response (TransUnion reports for example)

8.5.2 Information shared must be shared only with the individual concerned and never shared via Whatsapp groups or other applications

8.5.3 Whatsapp is considered, under the Act, to be a secure means of sharing sensitive information provided the sender and rescipient have the adequate password protection on their individual devices.

8.6 Data Subject Consent

8.6.1 The site manager should ensure that:

8.6.1.1 Guards, fiieldworkers and employees have been adequately trained in asking politely for personal details and images and are equipped to respond appropriately if asked for reasons

8.6.1.2 Guards, fiieldworkers and employees are familiar with the contents of the POPI act and are equipped to respond appropriately if asked for information.

8.6.2 The site/security manager shall have in place an operational procedure for dealing with consumers who refuse consent.

8.6.2.1 Under the Act, consumers are entitled to refuse consent for collection of their data, but the site, being private property and with a legitimate purpose for collection, is entitled to refuse entry depending on its risk profile and preferences

The scope of this aspect of the policy is written in support of the provisions of the POPI Act (Ch 5, Part B)

9. Review.

The SHS Information Officer is responsible for an annual review to be completed prior to our Privacy Policy anniversary date. Any ammendments to this Policy will result in ammendments to other supporting documentation, including this Agreement as well as others named within it

The Information Officer will ensure relevant stakeholders are consulted as part of the annual review to be completed prior to the policy anniversary date.

ACKNOWLEDGEMENT

Name: _____ Name:_____

Designation:_____ Place:_____

Date:_____ Date:_____

_____ _____

For and on behalf of the Customer For and on behalf of SHS