Solution House Software (Pty) Ltd

DATA PRIVACY POLICY STATEMENT of SOLUTION HOUSE SOFTWARE and all its subsidiaries (Hereinafter referred to as SHS)

May 2021

Version: 1.1

1. Introduction and Purpose

SOLUTION HOUSE SOFTWARE (SHS) takes the protection of personal data very seriously. The purpose of this policy statement is to expand upon our Information Security Policy and to describe the way in which we collect, store, use, and protect data that is associated with any Data Subject (natural/juristic person) and/or could be used to identify the Data Subject.

This statement applies to you, if you are:

- A Client or Prospective Client
- A Data Subject who has interacted with one of the SHS Products or Services

2. Definitions

Under the Act, SHS is defined as the Operator, and our client is defined as the Responsible Party:

2.1 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. Called Controllers in other jurisdictions (GDPR)

2.2 Operator means a person who processes personal information on behalf of the responsible party. Called processors in other jurisdictions (GDPR)

2.3 Data Subject is any person, natural or juristic, who can be identified, directly or indirectly, via an identifier such as a name; an ID number; location data; or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

2.4 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
c) Merging, linking, restriction, degradation, erasure or destruction of information.

2.5 Record means any recorded information
a) Regardless of form or medium, including any of the following:
i) Writing of any material
ii) 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
iii) Label, marking or other writing that identifies or describes anything of which it form part, or to which it is attached by any means
iv) Book, map, plan, graph or drawing
v) 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.

2.6 Personal Information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to
a) Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language and birth of the person.
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
e) The personal opinions, views or preferences of the person

f) 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
g) The views or opinions of another individual about the person
h) 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

3. Expanded Definition of Personal Information

3.1 Personal Information that SHS Collects:

a) certain information that is collected by the Responsible Party such as but not limited to Name, surname, ID number, address and location.
b) photographs and facial images
c) certain information collected through manual entries onto SHS products or services by the Responsible Party.

3.2 Personal Information Excludes:

a) Permanently de-identified information that does not relate to, or cannot be traced back to, you specifically
b) Non-personal statistical information collected and compiled by us

4. Information Collection

4.1 Clients of SHS who use services and products are the responsible parties and it is their duty to ensure they have the appropriate legal grounds in place to process personal information of data subjects.

4.2 SHS collects information from the consumer at sites managed/secured/serviced by our clients. Our client, as the defined Responsible Party, is the joint owner of the information collected via SHS services and products, and will have their own Privacy Policies in place to safeguard this information

4.3 Consent to collect information can be express (eg. signing an agreement or accepting an information prompt on software services or products) or implied (by providing guards/employees with access to identification documents or by allowing guards/employees to take photographs).

4.4 POPI 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.

4.5 POPI Section 15(3)(d) provides that further processing of personal information can be deemed compatible if necessary to prevent or mitigate an imminent threat to public health or public safety or to the health and safety of an individual. Public safety and security fall within this provision and further processing of personal information can be deemed compatible with this provision.

4.6 The purpose for which SHS services and products processes the information is to provide a tool to our customers to manage services, requests or incidents relating to crimes and infringements of bylaws happening within their areas and to compile a history of perpetrators to resolve such incidents and manage it pro-actively. This intended use and purpose is specific, explicitly defined and relates to the business of SHS services and products.

4.7 When collecting and sharing personal information for the purpose of investigating and prosecuting infringements and misdemeanours, such processing of information is a reasonable and justifiable limitation of the data subject's constitutional right to privacy.

5. Acceptance and Consent

We will obtain your consent to collect personal data in accordance with POPIA, which states that information may be collected in pursuance of the Responsible Party’s reasonable interests; or in accordance with 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. Purpose, Processing and Retention

SHS products or services capture information including, but not limited to, that which is contained on a driver's license, identity document, name, surname, address and GPS location of incident or as per the purposes set out by the responsible party.

6.1 Information is collected for the purpose of:
- 6.1.1 Safety and Security
- 6.1.2 Public safety and public health
- 6.1.3 Customer Service and service management
- 6.1.4 Site Management
- 6.1.5 Other client specific services or purposes constituting a legitimate interest

6.2 Information may be subject to further processing by SHS for the following purposes: analysis; evaluation; sharing.

6.3 SHS will retain your personal data for as long as it is necessary to fulfil the purposes explicitly set out in this policy, unless:
- 6.3.1 retention of the record is required or authorised by law
- 6.3.2 The data subject has consented to the retention of the record.

7. Disclosure of Information

7.1 In compliance with POPIA and GDPR, SHS will not share consumer data with any third party external to our client contracts and agreements. This includes, but is not limited to: marketing agencies and their affiliates; other clients; employees; the general public

7.2 However, POPIA does require that we share your data with:
- 7.2.1 Our clients (Reseller and Site) pursuant to the SLA we have in place with them, but only in accordance with the principles of the Act and upon confirmation of their own Data Protection Policies.
- 7.2.2 Information Regulators: we may disclose your personal data as required by law or governmental audit
- 7.2.3 Law enforcement: We may disclose personal data if required:
  - by a subpoena or court order;
  - to comply with any law;
  - to protect the safety of any individual or the general public safety and health.

8. Privacy by Design

As SHS develops new/more efficient products, servics or systems which involve the processing of personal data we take the privacy and data protection laws and principles into account in order to build them into the product proactively.

9. Security

9.1 Any information captured on Incident Desk is encrypted and immediately uploaded to secure cloud storage. The information can only be viewed or retrieved on Incident Desk thereafter by authorised personnel of the responsible party or SHS with a username and password for their purposes.

9.2 The information that has been captured can only be accessed by:

- 9.2.1 Authorised personnel of the responsible party for their purposes.
- 9.2.2 Authorised personnel of SHS on request of the responsible party or by an officer of the law; or by the data subject in accordance with the Act.

9.3 In order to ensure the safety of all the information that we gather on behalf of responsible parties:

- 9.3.1 Passwords are required by both the responsible party, as well as by all duly authorized SHS personnel.
- 9.3.2 Only authorized SHS personnel have access to these passwords
- 9.3.3 Each individual staff member is carefully screened before employment

10. Data Breaches

In the event of a breach, we will take all reasonable measures to notify all responsible parties, as well as the relevant supervisory authorities and affected data subjects, as soon as we become aware of such a breach, providing information such as:

10.1 When the breach occurred
10.2 If available, how the breach occurred
10.3 Which information has been breached
10.4 Who may be affected by such breach
10.5 The measures we intend to take to rectify the breach

11. Enquiries

If you have any questions or concerns arising from this privacy policy, please contact us on info@myincidentdesk.com