PRIVACY POLICY

Contents

Abbreviations

Acronym:	Stands for:
Sybrin	Sybrin Systems (Pty) Ltd and all of 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), Sybrin service providers and Sybrin business associates and partners.
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 and the General Data Protection Regulation.
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, organisation, 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

Statement of Confidentiality and Non-Disclosure

This document contains proprietary and confidential information. All data submitted to RECEIVING PARTY is provided in reliance upon its consent not to use or disclose any information contained herein except in the context of its business dealings with Sybrin. The recipient of this document agrees to inform present and future employees of Sybrin, and the RECEIVING PARTY, who view or have access to its content of its confidential nature.

The recipient agrees to instruct each employee that they must not disclose any information concerning this document to others except to the extent that such matters are generally known to, and are available for use, by the public. The recipient also agrees not to duplicate or distribute, or permit others to duplicate or distribute, any material contained herein without Sybrin's express written consent.

Sybrin retains all title, ownership and intellectual property rights to the material and trademarks contained herein, including all supporting documentation, files, marketing material, and multimedia. This does not extend to any items belonging to our partners and/or clients.

BY ACCEPTANCE OF THIS DOCUMENT, THE RECIPIENT AGREES TO BE BOUND BY THE AFOREMENTIONED STATEMENT.

1. Introduction

1.1. Data protection and privacy through lawful, legitimate, and responsible processing and use of personal data is a fundamental human right under the Constitution. The Sybrin Data Privacy Policy (this Policy) outlines the core principals which Sybrin 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 Sybrin collects and processes personal data.

2. Purpose

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

3. Scope

3.1. This policy applies to Sybrin, 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), Sybrin service providers and Sybrin business associates and partners.

3.2. This policy is intended to assist the directors, officers, employees, and appointed agents of Sybrin in assessing the legal position applicable to a particular decision, behaviour, conduct, act, or omission.

4. Use of information

4.1. This We collect personal information or other information for:

4.1.1 confirming and verifying an individual's identity;
4.1.2 underwriting purposes;
4.1.3 assessing and processing claims;
4.1.4 purposes of claims history;
4.1.5 detecting and preventing fraud and crime;
4.1.6 conducting market or client satisfaction research;
4.1.7 auditing and record keeping;
4.1.8 legal proceedings;
4.1.9 following an individual's instructions;
4.1.10 informing an individual of our services; and/or
4.1.11 making sure our business suits an individual's needs
4.1.12 Employment;
4.1.13 To obtain services and products through tenders and request for quotations;
4.1.14 When there is a legally contractual agreement between the parties;
4.1.15 Send personalised communication;
4.1.16 Build our data base for marketing purposes;
4.1.17 To secure your safety, belongings and the company's facilities;
4.1.18 Respond to inquiries; complaints and requests;
4.1.19 Feedback on our services;
4.1.20 To gain a better understanding of the company's stakeholders;
4.1.21 Process benefits i.e. medical aid and pension (internal employees); and
4.1.22 Security background checks (vetting)

5. Consequences of non-compliance

5.1. Wilful and deliberate non-compliance with this policy can expose Sybrin to significant regulatory sanctions, fines, criminal and/or civil liability. The reputational damage arising from such noncompliance will negatively affect Sybrin's ability to attract and maintain clients.

5.2. 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.

6. Governance and Implementation

6.1. This policy has been approved by the Sybrin Board of Directors.

6.2. This policy must be reviewed every two years or when a significant event occurs, taking into account any changes to regulatory requirements and business operations.

6.3. The Executives and Management of Sybrin are responsible for the successful implementation of the provisions of this policy.

7. Roles and responsibilities

7.1. Assigning roles and responsibilities are necessary to give effect to the requirements of this policy

7.1.1 Policy Owner

- The Sybrin Policy Owner is ultimately accountable for ensuring that Sybrin and its employees comply with the requirements set out in this process.

7.1.2 Policy Custodian

- The Policy Custodian is responsible for overseeing all dispensations, waivers, and breaches to this process.
- The Policy Custodian is responsible for facilitating the review(s) as set out in the policies or standards.

7.1.3 Board of Directors and the Executive Committee

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

7.1.4 Business/Function Head

The business or function head is responsible for the following:

- Ensuring this policy is effectively implemented within their business.
- The Business Head may delegate their responsibility (but not accountability) for implementation of this policy to an appropriate executive within the business.
- Employees

7.1.5 All employees within Sybrin are responsible for complying with this policy.

8. Policy Principles

8.1. **Processing of Data**

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

8.1.1 processed lawfully, fairly and in a transparent manner;
8.1.2 collected only for specified, clear and legitimate purposes;
8.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed;
8.1.4 accurate and kept up to date where applicable;
8.1.5 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
8.1.6 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, Sybrin must ensure that:
8.1.7 Personal information is not transferred to another country without appropriate safeguards being in place; and
8.1.8 Sybrin allows people to exercise their rights in relation to their personal data. Sybrin is responsible for, and must be able to demonstrate compliance with all of the above principles.

8.2. **Lawfulness, Fairness and Transparency**

When collecting and processing personal information for any specific purpose, Sybrin must always have a lawful basis for doing so. Processing personal information is lawful when at least one of the following circumstances is present:

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

Sybrin must document the above lawful reasons relied upon when processing personal information for each specific purpose.

8.3. **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 persons consent must be

8.3.1 specific;

8.3.2 informed (explained in plain and accessible language);

8.3.3 unambiguous;

8.3.4 separate and unbundled from any other terms and conditions provided to the data subject;

8.3.5 freely and genuinely given.

8.4. **Openness**

8.4.1 A person must be able to withdraw their consent without reservation. Once consent has been given, it will need to be updated where Sybrin wishes to process the personal data for a new purpose that is not compatible with the original purpose for which they were collected.

8.4.2 Chapter 6 of POPIA and Chapter 3 Section 1 of GDPR requires Sybrin to ensure that any information provided by Sybrin to people about how their personal data will be processed is concise, easily accessible, easy to understand and written in plain language. (Privacy Notice)

8.4.3 Sybrin 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.

8.4.4 Where Sybrin 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 Sybrin was clearly explained to the person.

9. Data Minimisation

9.1. The personal information that the Sybrin 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

9.2. Personal information must only be processed when necessary for the performance of duties and tasks and not for any other purposes.

9.3. 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.

9.4. When collecting personal information, as required for the performance of duties and tasks, there should not be a request that a person provide more personal information than is strictly necessary for the intended purposes.

9.5. 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.

10. Accuracy

10.1. Personal information that Sybrin collects and processes must be:

10.1.1 accurate and, where required and kept up-to-date; and

10.1.2 corrected and/or deleted, without delay, where an error has been discovered.

10.2. Where appropriate, any inaccurate or expired records should be deleted or destroyed.

11. Storage Limitation

11.1. The personal information that Sybrin 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).

11.2. 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.

11.3. Where appropriate, reasonable steps must be taken to delete or destroy any personal data that Sybrin no longer requires in accordance with Sybrin's Record Management Policies.

11.4. All privacy notices and fair processing notices must inform data subjects of the period for which their personal data will be stored or how such period will be determined.

12. Security of Personal Information

12.1. The personal information that Sybrin collects and processes must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage, and against unauthorised or unlawful processing.
12.2. Sybrin must develop, implement, and maintain appropriate technical and organisational measures for the processing of personal information taking into account the:
12.2.1 nature, scope, context, and purposes for such processing; and
12.2.2 the volume of personal data processed, likelihood and severity of the risks of such processing for the rights of persons.
12.3. Sybrin 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.
12.4. All procedures that Sybrin have put in place to maintain the security of personal information from collection to destruction must be observed and adhered to.
12.5. Confidentiality, integrity, and availability of personal information must be maintained at all times:
12.5.1 Confidentiality means that only people who need to know and are authorised to process any personal information can access it;
12.5.2 Integrity means that personal information must be accurate and suitable for the intended purposes;
12.5.3 Availability means that those who need to access the personal information for authorised purposes are able to do so.
12.6. Sharing personal information with third parties is prohibited unless:
12.6.1 Sybrin has agreed to this in advance; and
12.6.2 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 Sybrin's behalf.

13. Persons' Rights

13.1. Chapter 3(5) of POPIA and Chapter 3 of GDPR provides people with a number of rights in relation to their information. These rights include:
13.1.1 the right to withdraw consent unconditionally;
13.1.2 the right to be informed about how Sybrin collects and processes personal information;
13.1.3 the right to receive a copy of the personal information that Sybrin holds;
13.1.4 the right to have inaccurate personal data corrected or incomplete information completed;
13.1.5 the right to ask Sybrin to delete or destroy personal data if the personal data 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;
13.1.6 the right to restrict processing if there is a reasonable belief that the personal data is inaccurate;
13.1.7 the right to receive or ask Sybrin to transfer personal information to a third party;
13.1.8 The right to be notified of a personal data breach; and
13.1.9 The right to make a complaint to the CRO or another appropriate supervisory authority.

14. Employees

Employees must follow good data protection practices in line with the requirements stated in this policy. Take responsibility for managing and handling personal information and comply to the data principles as laid out within POPIA & GDPR.

14.1. In addition to:
14.1.1 provide adequate disclosure (transparency) on the purpose and intended use of this information
14.1.2 inform the data subject when they are about to collect personal information and obtain consent, inform the data subjects that their data may be shared across the borders and under which circumstances
14.1.3 collecting of this information must be justified, i.e. it must be something they require to fulfil their obligations and/or deliver a service
14.1.4 only share this information with authorised parties both internally and externally

15. Record Retention

15.1. All records pertaining to this policy should be retained in accordance with Sybrin's internal record retention policy.