Privacy and Data Protection Policy

October 2025

Statement of Confidentiality & Non-Disclosure

This document contains proprietary and confidential information. The Receiving Party acknowledges and agrees that the information contained herein is a special and asset of Sybrin Systems (Pty) Ltd and all its affiliates and group companies ("Sybrin"). The Receiving Party acknowledges and agrees to treat all information as strictly confidential, and with the highest level of integrity. Without detracting from the foregoing, the Receiving Party will not use, share, handle, process, store, and/or reproduce the information, either directly or indirectly, for its own benefit and/or the benefit of any other person unless explicitly authorised to do so in writing by Sybrin, which may withhold such consent in its sole and absolute discretion. The Receiving Party will not disclose any information contained herein to any person other than the Receiving Party's employees involved in carrying out the purpose and then only on a strictly necessary basis. Before disclosing any information provided, the Receiving Party will ensure that all employees are made aware of the confidential nature thereof and that all employees have signed an undertaking with no less onerous obligations of confidentiality. The Receiving Party will ensure that their employees will continue to comply with these obligations. The Receiving Party will initiate internal security procedures to prevent unauthorised disclosure of any information contained herein and use the same standard and duty of care (which will not be less than a reasonable standard of care) in protecting Sybrin's information as it uses to protect its own information. Sybrin retains, not limited to, all title, ownership, and intellectual property rights to the material and trademarks contained herein, including all supporting documentation, files, marketing material, and multimedia. The Receiving Party's obligations regarding the information herein will continue for the duration of any Agreement and continue for a period of 1 (one) year following the termination of any Agreement between Sybrin and the Receiving Party, notwithstanding all other obligations between the Parties thereof.

Document Control

Details

Document Title:	Privacy and Data Protection Policy
Document Identifier	S-POL-PIMS-005
Document Issue Date:	17/10/2025
Business Unit:	Legal
Document Owner:	Hannetjie du Toit
Document Classification:	Confidential

Approval (Signoff)

Date	First Approver	Business Unit	Signature	Date	Final Approver Name	Business Unit	Signature
	Hannetjie du Toit	Legal			Ryan Barlow	EXCO	Ryan Barlow

20/10/2025 JM du Toit 20/10/2025

Document Change Control

Version	Date	Author	Revision Details
1.0	17/10/2025	WWISE	First revision.

Contents

1. Purpose

1.1. Purpose

In its everyday business operations Sybrin makes use of a variety of personally identifiable information (PII), including data about:

- Current, past and prospective employees
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Sybrin is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Sybrin's systems.

2. References and Associated Documents

Details

ISO/IEC 27701:2019	Clause 5.1, 5.2, 5.4, 6.1, 6.2, 6.3, 7.4, 7.5, 8.3, 8.4, 8.5 Annexure A and Annexure B
Privacy Impact Assessment Process	S-FT-PIMS-026 Privacy Impact Assessment Process
PII Analysis Procedure	S-PRO-PIMS-007 PII Analysis Procedure
Legitimate Interest Assessment Procedure	S-PRO-PIMS-006 Legitimate Interest Assessment Procedure
Records Retention and Protection Policy	S-POL-PIMS-003 Records Retention and Protection Policy

3. Abbreviations and Definitions

Details

Consent	Freely given, specific, informed, and unambiguous indication of the data subject's agreement to the processing of their PII.
Cross-border Transfer	Transfer of PII from one country to another, often subject to regulatory safeguards.
Data Subject	The individual whose PII is being collected, held, or processed.
Data Transfer	The act of moving or transmitting PII from one system, organisation, or geographic location to another.

DPA	Data Protection Act (Kenya)
EPOCA (TZ)	Electronic and Postal Communications Act (Tanzania)
GDPR	General Data Protection Regulation (EU)
ISO	International Organisation for Standardization
Personally Identifiable Information (PII)	Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal. Any information that can be used to identify an individual either directly or indirectly (e.g., name, ID number, email, IP address).
PII Controller	Privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes.
PII principal	Natural person (and/or any organisation operating in South Africa) to whom the personally identifiable information (PII) relates.
PII Processor	Privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller.
PIMS	Privacy Information Management System
POPIA	Protection of Personal Information Act (South Africa)
Processing of PII	Operation or set of operations performed upon personally identifiable information (PII).
Receiving Party	The individual or entity who obtains and is responsible for protecting sensitive information disclosed by Sybrin.
Third Party	Any entity (other than the data subject, controller, or processor) involved in handling or processing PII.

4. Privacy and Data Protection Policy

4.1. Applicable Privacy Legislation

The table below shows the main items of privacy legislation that apply to the countries (or groups of countries) and states within which Sybrin operates.

BLOC/COUNTRY/STATE	APPLICABLE LEGISLATION
South Africa	Protection of Personal Information Act, 2013 (POPIA)
Kenya	Data Protection Act, No. 24 of 2019 (DPA)
Zambia	Data Protection Act, No. 3 of 2021
Tanzania	Personal Data Protection Act, 2022
United Kingdom	UK General Data Protection Regulation (UK GDPR) Data Protection Act, 2018

Table 1: Applicable privacy legislation

Sybrin has a legal obligation to always comply with the provisions of this legislation. Whilst there will be variations in these provisions, this policy establishes the key principles that are commonly required to be observed in such legislation.

Significant fines may be applicable if a breach is deemed to have occurred under the relevant privacy legislation, which is designed to protect the PII of citizens of the country (or state, region or countries) involved. It is Sybrin's policy to ensure that our compliance with applicable legislation is always clear and demonstrable.

4.2. Principles relating to processing of PII

There are several fundamental principles upon which most privacy legislation is based. These are summarised as follows:

1. **Lawfulness, fairness and transparency** - PII shall be processed lawfully, fairly and in a transparent manner in relation to the PII principal
2. **Purpose limitation** – PII shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. **Data minimization** – the PII collected and stored shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. **Accuracy** – PII shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that PII that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
5. **Storage limitation** – PII shall be kept in a form which permits identification of PII principals for no longer than is necessary for the purposes for which the PII is processed
6. **Integrity and confidentiality** – PII shall be processed in a manner that ensures appropriate security of the PII, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Sybrin will ensure that it complies with all these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

4.3. Rights of the individual

The PII principal also has rights regarding their PII. These will generally consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights are supported by appropriate procedures within Sybrin that allow the required action to be taken within the timescales stated in the applicable privacy legislation.

PII PRINCIPAL REQUEST	TIMESCALE
The right to be informed	When data is collected (if supplied by PII principal) or within one month (if not supplied by PII principal)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month

PII PRINCIPAL REQUEST	TIMESCALE
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

Table 2: Timescales for PII principal requests

4.4. Lawfulness of processing

Depending on the legislation involved, there may be several alternative ways in which the lawfulness of a specific case of processing of PII may be established. It is Sybrin's policy to identify the appropriate basis for processing and to document it, in accordance with the applicable legislation. The main options are described in brief in the following sections.

4.4.1 Consent

Where appropriate, Sybrin will obtain consent from a PII principal to collect and process their data. In case of children below the age specified in applicable legislation parental consent will be obtained. Transparent information about our usage of their PII will be provided to PII principals at the time that consent is obtained and their rights regarding their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.

If the PII is not obtained directly from the PII principal, then this information will be provided to the PII principal within a reasonable period after the data is obtained and within one month.

4.4.2 Performance of a contract

Where the PII collected and processed is required to fulfil a contract with the PII principal, consent is not required. This will often be the case where the contract cannot be completed without the PII in question, for example, a delivery cannot be made without an address.

4.4.3 Legal obligation

If the PII is required to be collected and processed in order to comply with applicable law, then consent is not required. This may be the case for some data related to employment and taxation for example, and for many areas addressed by the public sector.

4.4.4 Vital interests of the PII principal

In a case where the PII is required to protect the vital interests of the PII principal or of another natural person, then this may be used as the lawful basis of the processing. Sybrin will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of PII. As an example, this may be used in aspects of social care, particularly in the public sector.

4.4.5 Task carried out in the public interest

Where Sybrin needs to perform a task that it believes is in the public interest or as part of an official duty then the PII principal's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

4.4.6 Legitimate interests

If the processing of specific PII is in the legitimate interests of Sybrin and is judged not to affect the rights and freedoms of the PII principal in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

4.5. Privacy by design

Sybrin has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process PII will be subject to due consideration of privacy issues, including the completion of one or more privacy impact assessments.

The privacy impact assessment will include:

- Consideration of how PII will be processed and for what purposes
- Assessment of whether the proposed processing of PII is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the PII
- What controls are necessary to address the identified risks and demonstrate compliance with applicable legislation.

Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate, including at the end of processing, and the mechanisms used to achieve them will be documented.

4.6. Contracts involving the processing of PII

Sybrin will ensure that all relationships it enters that involve the processing of PII are subject to a documented contract that includes the specific information and terms required by the applicable legislation. For more information, see the *PII Controller-Processor Agreement Policy*.

4.7. International transfers of PII

Transfers of PII between countries will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the applicable legislation. This depends partly on the relevant authority's judgement (for example in the case of the GDPR, the European Commission) as to the adequacy of the safeguards for PII applicable in the receiving country and this may change over time.

Where an adequacy decision (or similar statement) does not exist for a destination country, an appropriate safeguard such as standard contractual clauses will be used, or a relevant exception identified as permitted under the applicable legislation.

4.8. Breach notification

It is Sybrin's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of PII. In line with the applicable legislation, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, where required the relevant supervisory authority will be informed within the specified timeframe (for example, for the GDPR within 72 hours). This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

~~Under privacy legislation the relevant authority may have the right to impose a range of fines, often based on a percentage of annual worldwide turnover or a specific amount, for infringements of the regulations.~~

4.9. Addressing compliance to applicable privacy legislation

The following actions are undertaken to ensure that Sybrin always complies with the accountability principle of privacy legislation within the countries in which it operates:

- The legal basis for processing PII is clear and unambiguous
- A Data Protection Officer is appointed with specific responsibility for data protection in the organisation (if required)

- All staff involved in handling PII understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to PII principals wishing to exercise their rights regarding PII and such enquiries are handled effectively
- Regular reviews of procedures involving PII are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
    - Organisation name and relevant details
    - Purposes of the PII processing
    - Categories of individuals and PII processed
    - Categories of PII recipients
    - Agreements and mechanisms for transfers of PII to other countries including details of controls in place
    - PII retention schedules
    - Relevant technical and organisational controls in place

These actions are reviewed on a regular basis as part of the management process concerned with privacy and data protection.

5. Document Review

This Policy forms part of the Integrated Management System (IMS) and must be reviewed at least annually, or when changes occur. All changes must be signed off by the document owner and the appropriate level of authority, as defined in S-ISLP-004 Control of Documents and Records Procedure before it is communicated to the users of this document. All changes must be accurately recorded in S-IMS-MI-001-Sybrin Document Change Request (Master Index), on Sybrin's IMS SharePoint site. (https://sybrincloud.sharepoint.com/sites/IMS/SitePages/CollabHome.aspx). The revised document must be stored appropriately according to S-ISLP-004 Control of Documents and Records Procedure. All users of the document must be notified of any changes, and the amended document must be provided to all appropriate users.

Signed with Impression - Chain of Custody

Signature Request			
Signature Request ID:	7af662d6-240a-4c9f-a612-18c584d35a9d	Timestamp:	2025-10-20 09:28:49 GMT
Signee Name:	Hannetjie Du Toit	Sender Name:	Sharon Wilken
Request Type:	WebSigning	Request Status:	WEBVIEWER SIGNED
Original Document			
Document Name:	SPOLPIMS005 Privacy and Data Protection Policy.pdf	Document Size:	315.9 KB
Email Evidence			
Signee Email:	hannetjie.dutoit@sybrin.com	Email Subject:	A document from Sharon Wilken is ready for signature
Email Sent Timestamp:	2025-10-17T06:18:00.621375	Email Opened Timestamp:	Not available in Silent Mode
Web Evidence			
Signee IP Address:	41.13.78.194	Request Timestamp:	2025-10-20 09:23:54 GMT
Signee GPS (if shared):	ZA: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36 Edg/141.0.0.0	Terms Accepted Timestamp:	2025-10-20 09:26:00 GMT
Annotations and Modifications			
Signature Count:	1	Form Fields Filled Count:	1
Text Annotation Count:	0	Initial All Pages Count:	0
Single Initial Count:	0		
Signing Evidence			
Signee Mobile:	+27000000000	Sign Type:	WebSigning
Security Challenge:	NONE	Part of Workflow:	fdc66efe-28f5-47c7-b35f-95aa26b1421e
Chain Of Custody Generation			
Attached Document Name:	20251020T092848.885201Z SPOLPIMS005 Privacy and Data Protection Policy.pdf	Attached Timestamp:	2025-10-20 09:28:49 GMT

Signed with Impression - Chain of Custody

Signature Request			
Signature Request ID:	8506274a-f9ea-4b44-9090-42018217c957	Timestamp:	2025-10-20 11:42:11 GMT
Signee Name:	Ryan Barlow	Sender Name:	Sharon Wilken
Request Type:	WebSigning	Request Status:	WEBVIEWER SIGNED
Original Document			
Document Name:	SPOLPIMS005 Privacy and Data Protection Policy.pdf	Document Size:	322.5 KB
Email Evidence			
Signee Email:	ryan.barlow@sybrin.com	Email Subject:	A document from Sharon Wilken is ready for signature
Email Sent Timestamp:	2025-10-20T09:28:57.023468	Email Opened Timestamp:	Not available in Silent Mode
Web Evidence			
Signee IP Address:	105.233.97.203	Request Timestamp:	2025-10-20 11:41:33 GMT
Signee GPS (if shared):	ZA: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36 Edg/141.0.0.0	Terms Accepted Timestamp:	2025-10-20 11:41:38 GMT
Annotations and Modifications			
Signature Count:	1	Form Fields Filled Count:	1
Text Annotation Count:	0	Initial All Pages Count:	0
Single Initial Count:	0		
Signing Evidence			
Signee Mobile:	+27000000000	Sign Type:	WebSigning
Security Challenge:	NONE	Part of Workflow:	fdc66efe-28f5-47c7-b35f-95aa26b1421e
Chain Of Custody Generation			
Attached Document Name:	20251020T114210.982471Z SPOLPIMS005 Privacy and Data Protection Policy.pdf	Attached Timestamp:	2025-10-20 11:42:11 GMT