



Privacy Notice

August 2026

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 valuable asset of Sybrin Systems (Pty) Ltd and all of 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 Notice
Document Subtitle:	n/a
Document Identifier	S-POL-PIMS-005
Document Issue Date:	17/10/2025
Business Unit:	IMS
Document Owner:	Jason Darmanovich
Document Classification:	Internal

Approval (Signoff)

Date	First Approver	Business Unit	Signature	Date	Final Approver Name	Business Unit	Signature
	Hannetjie du Toit	Legal			Jason Darmanovich	IT	

Document Change Control

Version	Date	Author	Revision Details
1.0	17/10/2025	Sybrin	First revision.
2.0	20/08/2026	WWISE	Added the process for data subject requests (section 15). Added and considered data privacy laws from the other regions, namely Zambia, Tanzania, and Kenya.

Contents

1.	Purpose, Scope, and Objectives	6
2.	Applicable privacy framework	6
3.	Who is responsible for your personal information?	6
4.	Who does this Notice apply to?	7
5.	What personal information may we process?	7
6.	Where do we obtain personal information?	8
7.	Why do we process personal information?	8
7.1.	Lawful grounds	9
8.	Important external processing activities	9
8.1.	Recruitment and job applicants	9
8.2.	Customers, prospective customers, and client representatives	10
8.3.	KYC and customer due diligence	10
8.4.	Suppliers and KYS.....	10
8.5.	Service delivery and project records	10
8.6.	Surveys, feedback, and NPS.....	10
8.7.	Website enquiries and Contact Us forms	10
8.8.	Events, training, learners, and delegates	11
8.9.	Client references and testimonials	11
8.10.	Direct marketing and business development	11
8.11.	Website analytics, cookies, and similar technologies.....	11
9.	Is providing personal information mandatory?	11
10.	Special, sensitive, and children’s information	11
11.	Who may receive or access personal information?	12
12.	Operators, processors, and service providers	12
13.	Cross-border processing and regional access	12
14.	How long do we keep external personal information?	12
15.	How do we protect personal information?	13
16.	Your privacy rights	14
17.	How to exercise your rights or raise a concern	14
17.1.	Recruitment-specific rights	16
18.	Personal data breaches and security incidents	16
19.	Automated decision-making and profiling	16
20.	Breach and Non-compliance	16
21.	Document Review	16

1. Purpose, Scope, and Objectives

Sybrin respects the privacy of customers, prospective customers, client representatives, suppliers, service providers, contractors, business partners, learners, delegates, facilitators, assessors, moderators, website visitors, event participants, survey respondents, prospective clients, and other external persons whose personal information it processes. This Privacy Notice explains what personal information Sybrin may collect, why it is processed, where it comes from, who may receive it, how long it is retained, how it is protected, and the privacy rights available to data subjects.

This Notice applies to processing undertaken by Sybrin for its own recruitment, business, contractual, regulatory, service delivery, procurement, marketing, website, training, quality, security, and legitimate organisational purposes across South Africa, Kenya, Zambia, and Tanzania. It applies to personal information in electronic, physical, visual, audio, and other forms.

This Notice does not replace collection-specific notices where additional information is required. Sybrin may therefore provide shorter or more specific notices or disclaimers for recruitment applications, KYC, KYS, surveys, website forms, events, training, tenders, testimonials, or other particular processing activities. A recruitment application form may include an acknowledgement that this Privacy Notice has been read; such acknowledgement is evidence of transparency and is not blanket consent to all processing.

2. Applicable privacy framework

The privacy law applicable to your information depends on the employing entity, processing activity, location, and other jurisdictional factors. This policy is designed to support the following four regional privacy regimes:

Region	Primary privacy legislation	Supervisory authority
South Africa	Protection of Personal Information Act 4 of 2013 (POPIA) and applicable Regulations; PAIA applies to certain access-to-records processes.	Information Regulator (South Africa)
Kenya	Data Protection Act No. 24 of 2019 and the Data Protection (General) Regulations, 2021.	Office of the Data Protection Commissioner (ODPC)
Zambia	Data Protection Act No. 3 of 2021 and applicable regulations.	Data Protection Commission (DPC)
Tanzania	Personal Data Protection Act No. 11 of 2022 / Cap. 44 and the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023.	Personal Data Protection Commission (PDPC)

Where another tax, financial, procurement, corporate, training, contractual, regulatory, professional, litigation, or sector-specific requirement applies, Sybrin will process and retain information in accordance with the stricter applicable obligation where required.

3. Who is responsible for your personal information?

Sybrin is the responsible party/data controller in respect of the personal information processing described in this Privacy Notice. This means that Sybrin determines the purposes for which, and the means by which, your personal information is processed.

Region	Primary privacy contact	Name	Contact details
South Africa	Information Officer	Hannetjie Du Toit	Hannetjie.dutoit@sybrin.com
Kenya	Data Protection Officer	Joe Kiragu	Joe.kiragu@sybrin.com
Zambia	Data Protection Officer	Stephen Mulenga	Stephen.mulenga@sybrin.com
Tanzania	Data Protection Officer	Shomari Shija	Shomari.shija@sybrin.com

4. Who does this Notice apply to?

Depending on how you interact with Sybrin, this Notice may apply to you if you are:

- a customer, prospective customer, customer employee, or customer representative;
- a supplier, prospective supplier, service provider, supplier representative, contractor, consultant, or business partner;
- a learner, delegate, facilitator, assessor, moderator, attendee, or other participant in a training, certification, assessment, event, or related service;
- a website visitor, person who submits an inquiry, survey respondent, event registrant, marketing lead, or prospective client;
- a client reference, testimonial provider, or other external person whose professional/contact information is used in legitimate business activities;
- a director, shareholder, authorised representative, beneficial owner, or other person whose information is required for KYC, KYS, contracting, finance, procurement, compliance, or due diligence purposes; or
- another external person whose personal information Sybrin processes in connection with its lawful business activities.

5. What personal information may we process?

The information Sybrin processes depends on the relationship and purpose. It may include:

- Identity and identifying information, including names, surnames, identification or passport details, nationality, date of birth, signatures, registration numbers, and other identifiers where required;
- Contact and professional information, including telephone numbers, email addresses, postal or physical addresses, employer, organisation, job title, role, and business contact details;
- Recruitment and candidate information, including CVs, employment history, qualifications, skills, references, interview notes or assessments, screening or verification information where applicable, preferred role, availability, salary-related expectations where relevant, and recruitment correspondence;
- Customer, supplier, contractual, and commercial information, including agreements, proposals, service records, project information, purchase orders, account information, supplier/customer references, and correspondence;
- Financial, banking, billing, tax, and transaction information where required for invoicing, payments, supplier onboarding, KYC/KYS, financial administration, or legal compliance;

- Due diligence and verification information, including company/director details, beneficial ownership or authorised-representative information, proof of address, verification results, declarations, and supporting documents where relevant;
- Training, learning, assessment, certification, attendance, competence, and professional information where Sybrin provides training or related services;
- Survey, feedback, complaint, inquiry, and service-delivery information, including responses, comments, ratings, contact details, and records of follow-up;
- Website, device, and technical information, including IP address, browser/device details, cookies or similar identifiers, access logs, usage information, and website interaction data where applicable;
- Marketing and event information, including communication preferences, event registrations, lead information, campaign interactions, consent/opt-out records, and approved testimonial information;
- Photographs, audio, video, or other media where relevant to events, training, testimonials, marketing, security, or another appropriately communicated purpose;
- Security, fraud prevention, incident, complaint, investigation, access, or audit information where necessary to protect people, systems, information, assets, or legal rights; and
- Other information reasonably necessary for the specific relationship or processing purpose and communicated where required.

Sybrin does not necessarily collect every category listed above from every person. Personal information must be relevant to the actual purpose and should not be collected merely because it may be useful later.

6. Where do we obtain personal information?

Personal information is commonly obtained directly from you. Where lawful and necessary, it may also be obtained from:

- recruitment platforms, recruitment agencies, referees, screening or verification providers, and professional or public sources where relevant and lawfully used for recruitment;
- your employer, customer, supplier, contracting party, authorised representative, or another person involved in the relevant business relationship;
- public company, professional, regulatory, court, procurement, or other lawful registers and records;
- publicly available websites or professional/business profiles where use is lawful and relevant;
- KYC/KYS, fraud prevention, screening, verification, banking, payment, or other authorised service providers;
- government bodies, regulators, courts, law-enforcement authorities, professional bodies, certification/accreditation bodies, or other lawful sources;
- Sybrin systems, websites, service-delivery platforms, survey tools, event tools, CRM systems, project records, financial systems, logs, or communications; and
- operators/service providers processing information on Sybrin's behalf.

7. Why do we process personal information?

Sybrin processes external personal information only for specific, legitimate, and lawful purposes. These may include:

- receiving and managing job applications, assessing candidate suitability, arranging interviews, verifying qualifications or references where appropriate, communicating with candidates, making recruitment decisions, onboarding successful candidates, and maintaining limited recruitment records;
- responding to enquiries and communicating with customers, prospective customers, suppliers, partners, website users, and other stakeholders;

- establishing, administering, performing, and managing customer, supplier, service, project, procurement, and other contractual relationships;
- conducting KYC, KYS, supplier/customer verification, due diligence, fraud prevention, conflict of interest checks, and other governance or compliance activities;
- delivering consulting, project, training, assessment, certification, service delivery, customer support, and related services;
- processing invoices, payments, purchase orders, supplier/customer accounts, reimbursements, and other financial records;
- monitoring service delivery, project performance, customer satisfaction, quality, complaints, corrective action, and continual improvement;
- conducting surveys, obtaining feedback, analysing responses, and improving services, with identifiable information limited to what is necessary;
- organising events, training, webinars, meetings, workshops, and related communications;
- preparing proposals, bids, tenders, client references, and commercial submissions where the relevant information is necessary and lawfully available;
- maintaining websites, online services, security, analytics, technical support, logging, and system integrity;
- carrying out appropriately authorised marketing and business-development activities and maintaining opt-out / suppression records;
- meeting legal, regulatory, tax, audit, contractual, accreditation, certification, reporting, record-keeping, and dispute-resolution obligations;
- protecting the rights, safety, property, confidential information, systems, assets, and legitimate interests of Sybrin, its clients, personnel, and others; and
- establishing, exercising, or defending legal claims and responding to regulators, courts, law-enforcement authorities, or other lawful requests.

7.1. Lawful grounds

The lawful ground depends on the jurisdiction and purpose. Sybrin may process personal information where processing is necessary to take steps at your request before entering into a contract or to enter into or perform a contract, comply with a legal or regulatory obligation, protect the legitimate interests or rights of a data subject, pursue Sybrin's or a third party's legitimate interests where permitted and appropriately assessed, or where valid consent is relied upon for a specific optional purpose. For recruitment, Sybrin does not rely on a mandatory consent checkbox merely to receive and assess an application. Where legitimate interests are used, the interest, necessity, impact on the individual, reasonable expectations, and safeguards are assessed and documented. Consent may be used for a genuinely optional purpose, such as retaining an unsuccessful candidate's details for future opportunities where that is the selected lawful basis.

8. Important external processing activities

8.1. Recruitment and job applicants

When you apply for a vacancy or are considered for an employment opportunity, Sybrin may process information necessary to administer the recruitment process and assess your suitability. This may include your identity and contact details, CV, employment history, qualifications, skills, references, interview or assessment information, recruitment correspondence, and screening or verification information where relevant. Information may be collected directly from you through the recruitment platform or application process and, where lawful and necessary, from referees, recruitment agencies, screening or verification providers, professional registers, or other appropriately verified sources.

Processing for a current vacancy may be based on steps taken at your request in connection with a prospective employment relationship, applicable legal obligations, and/or other lawful grounds available in the relevant jurisdiction.

Where Sybrin relies on legitimate interests for a specific recruitment purpose, the interest and balancing assessment will be documented internally. A privacy acknowledgement checkbox is used to evidence that you have been informed; it does not constitute blanket consent.

If your application is unsuccessful, Sybrin currently retains the recruitment record for 12 months from the date of application, subject to any longer mandatory legal, regulatory, dispute, investigation, or legal-hold requirement applicable in the relevant region. If you are successful, relevant recruitment records may become part of your employee record and will thereafter be handled under the Employee Privacy Notice and the approved employee retention schedule. The recruitment system and any provider supporting it are subject to privacy and security assessment, operator/processor controls, and cross-border assessment where applicable. Materially higher-risk features such as AI ranking, automated rejection, biometric checks, or expanded sensitive data processing require additional privacy assessment before implementation.

8.2. Customers, prospective customers, and client representatives

Sybrin may process business contact details, contractual information, correspondence, service records, project information, billing information, and other limited personal information necessary to establish and manage customer relationships, deliver services, administer contracts, manage projects, provide support, invoice, report, and maintain appropriate business and quality records. Access is limited to authorised personnel with a legitimate business need.

8.3. KYC and customer due diligence

Where customer verification or due diligence is required, Sybrin may process identity, business, director/representative, address, financial, verification, and related information necessary to verify the customer or authorised representatives, manage risk, prevent fraud, and comply with legal, contractual, governance, or onboarding requirements. A collection-specific KYC privacy disclaimer may be provided with the relevant form or process.

8.4. Suppliers and KYS

For supplier onboarding and administration, Sybrin may process supplier representative details, verification and due-diligence information, banking/payment information, company/director information, contractual records, declarations, and other information required to assess, onboard, pay, monitor, and manage suppliers. A collection-specific KYS privacy disclaimer may be provided with the relevant form or process.

8.5. Service delivery and project records

Client representative names, contact details, roles, approvals, change requests, service forms, project records, performance records, and related correspondence may be processed to deliver services, manage changes, monitor performance, evidence contractual performance, and support quality management. Where Sybrin receives personal information from a client solely to perform services under that client's instructions, Sybrin may act as an operator / processor for that information.

8.6. Surveys, feedback, and NPS

Where surveys or feedback activities collect identifiable information, Sybrin processes that information for feedback, research, service improvement, analysis, and any necessary follow-up. Identification will be limited to what is necessary for the stated purpose. Where historical analytics remain useful after identification is no longer required, Sybrin may de-identify or aggregate results rather than retain unnecessary identifiable information.

8.7. Website enquiries and Contact Us forms

Information provided through website enquiry or Contact Us forms is processed to respond to and manage the enquiry, perform requested follow-up, maintain appropriate correspondence records, and improve service where relevant. A short collection-specific privacy disclaimer may appear directly on the form.

8.8. Events, training, learners, and delegates

Where Sybrin provides training, events, webinars, workshops, assessments, or related services, it may process registration, attendance, contact, organisation, learning, assessment, certificate, feedback, and communication information to administer and evidence the service, issue certificates where applicable, communicate with participants, and meet customer, accreditation, contractual, or quality requirements.

8.9. Client references and testimonials

Where a client representative provides or authorises a reference, reference letter, testimonial, or similar professional statement, Sybrin may use the approved information for the agreed business-development, proposal, website, or marketing purpose. Reusable references and testimonials should remain current, accurate, relevant, and authorised, and should be removed or updated where the authority or relationship ends or the information becomes inaccurate.

8.10. Direct marketing and business development

Sybrin may use business contact information for direct marketing and business-development activities only where permitted under the applicable regional law. Where consent is required, it will be obtained in an appropriate manner. Where another lawful basis is permitted, Sybrin will apply the relevant conditions. Marketing communications will provide an appropriate method to object or opt out, and Sybrin will maintain minimal suppression records necessary to honour those choices.

8.11. Website analytics, cookies, and similar technologies

Sybrin websites may use essential technologies required for website operation and, where implemented, analytics or similar technologies to understand website use, improve functionality, protect the site, and support legitimate digital activities. Where applicable law requires notice or consent for non-essential technologies, appropriate cookie or tracking controls will be used. Further detail may be provided in a separate Cookie Policy.

9. Is providing personal information mandatory?

Some information is voluntary, while other information is necessary to apply for and be considered for a vacancy, enter into or perform a contract, deliver a requested service, verify a customer or supplier, process a payment, meet a legal or regulatory obligation, protect security, or administer another legitimate relationship. For recruitment, Sybrin will identify information that is required to assess or administer the application and will not treat a mandatory privacy acknowledgement as consent. If required information is not provided, Sybrin may be unable to assess or progress the application. Any genuinely optional recruitment processing will be identified separately.

10. Special, sensitive, and children's information

Certain activities may involve information that is treated as special, sensitive, or specially regulated under one or more of the applicable regional laws. Examples may include identity information, financial information, health information, criminal or background screening information, biometric information, or other sensitive categories. Such information will only be processed where necessary, lawfully authorised, proportionate to the purpose, and subject to appropriate safeguards. In recruitment, special or sensitive information will not be collected merely because it may be useful; it will only be requested or verified where there is a genuine role, legal, security, or other lawful requirement.

Sybrin services are not generally directed at children unless the particular service, training, event, survey, project, or customer arrangement expressly involves children or minors. Where children's information is processed, Sybrin will apply the specific legal requirements relevant to the jurisdiction, including appropriate consent/authorisation, transparency, minimality, security, and impact assessment measures where required.

11. Who may receive or access personal information?

Depending on the processing activity and only where necessary and lawful, recipients may include:

- authorised Sybrin departments and personnel involved in the relevant recruitment/HR, customer, supplier, project, finance, legal, service-delivery, training, commercial, marketing, IT, quality, or compliance process;
- banks, payment providers, insurers, auditors, professional advisers, certification/accreditation bodies, and other service providers where relevant;
- technology, hosting, cloud, recruitment, screening or verification, CRM, survey, event, communications, training, financial, or other operators/processors acting on Sybrin's instructions;
- customers, suppliers, business partners, tendering entities, project parties, or other counterparties where disclosure is necessary for the relevant relationship or transaction;
- government bodies, tax authorities, regulators, courts, law-enforcement bodies, or other public authorities where disclosure is required or permitted by law;
- professional, public, or regulatory bodies where required for verification, certification, accreditation, or compliance; and
- other recipients where the disclosure is lawfully justified and appropriately communicated.

Sybrin does not sell personal information.

12. Operators, processors, and service providers

Sybrin may appoint authorised third-party service providers to process personal information on its behalf. These providers may support recruitment platforms, candidate screening or verification, technology, hosting, communications, payments, surveys, events, training, customer/supplier administration, document management, security, or other services. Where a provider acts as an operator/processor, Sybrin requires appropriate confidentiality, security, processing, incident notification, retention/deletion, sub-processor, and other contractual controls proportionate to the service and applicable law.

Where Sybrin acts as an operator / processor for a client, Sybrin processes personal information in accordance with the client's documented instructions and the relevant agreement, subject to any independent legal obligations that apply to Sybrin.

13. Cross-border processing and regional access

Sybrin operates across South Africa, Kenya, Zambia, and Tanzania and may use shared or cloud-based technology. This does not mean that every category of personal information is transferred between all four countries. Cross-border hosting, access, support, or disclosure is assessed for the specific processing activity and must be reflected in the ROPA where applicable.

Where personal information is transferred, hosted, supported, or accessed outside the country in which it was collected, Sybrin will apply the applicable legal transfer conditions and safeguards. Depending on the jurisdiction, this may include contractual safeguards, approved transfer mechanisms, adequate protection, data subject consent where appropriate, regulator approval/authorisation, or a cross-border permit. In particular, Sybrin will apply any applicable requirements under POPIA section 72, the Kenyan Data Protection framework, Zambia's cross-border transfer requirements, and Tanzania's PDPC permit framework.

14. How long do we keep external personal information?

Sybrin retains personal information only for as long as necessary for the relevant purpose or for a longer period where required or permitted by applicable law, contract, audit, investigation, dispute, legal hold, or other lawful requirement. Approved periods and triggers are maintained in the ROPA.

External record / activity	Current retention approach	Trigger	Important qualification
Unsuccessful candidate applications / recruitment records	12 months	Date of application	A longer mandatory regional, dispute, investigation or legal-hold requirement prevails. Successful candidate records transition to the employee record.
Supplier onboarding / KYS and supplier financial records	7 years	Applicable financial, tax, supplier, or statutory trigger	A longer mandatory regional or contractual period prevails.
Customer invoicing / accounts records	7 years	Applicable transaction, financial, or statutory trigger	A longer mandatory regional or contractual period prevails.
Executed contracts and related legal records	7 years	End/termination of contract	Legal hold, dispute, limitation, or other legal requirement may extend the period.
Project-delivery and contract-performance records	5 years	Project completion / close-out	Longer customer, contractual, legal, or evidentiary requirements prevail.
Client references / reusable reference information	While current and authorised	End of relevant client relationship / authority / revalidation	Tender evidence copies may follow a separate tender or contract period.
Testimonials	While approved, accurate, relevant, and in use	Withdrawal, relationship change, campaign end, or review outcome	Remove from publication/reusable use when authority ends or information becomes inaccurate.
Surveys, website enquiries, event leads, and marketing information	Only for the approved purpose and follow-up period	End of the stated purpose / objection / approved follow-up	Where analytics remain useful, de-identify or aggregate rather than retain unnecessary identifiable information.

At the end of the approved retention period, records are securely deleted, destroyed, or de-identified in accordance with Sybrin's Data and Records Retention, Protection, and Deletion Policy and disposal controls, subject to any applicable legal hold or regional override.

15. How do we protect personal information?

Sybrin applies technical and organisational safeguards appropriate to the nature and sensitivity of the information. These may include:

- role-based and need-to-know access restrictions;
- authentication and multifactor authentication where appropriate;
- encryption and secure transfer mechanisms;
- controlled systems, repositories, and approved cloud services;
- logging, monitoring, access reviews, and privileged-access controls;
- confidentiality obligations and privacy/information-security awareness;

- backup, recovery, vulnerability management, secure configuration, and endpoint protection;
- physical security and access controls;
- incident-management and personal-data breach procedures;
- operator due diligence and contractual security requirements; and
- retention, deletion, masking, de-identification, and secure disposal controls.

No security measure eliminates all risk. Sybrin therefore reviews controls, incidents, privacy risks, PIAs, audit findings, processing changes, and legal requirements through its IMS/PIMS and updates safeguards where necessary.

16. Your privacy rights

Your specific rights depend on the law applicable to the processing. Subject to applicable legal conditions and exceptions, you may have rights to:

- be informed about how your personal information is processed;
- request confirmation of whether Sybrin holds personal information about you and request access to it;
- request correction or rectification of inaccurate, incomplete, misleading, or outdated information;
- request deletion, erasure, or destruction where the information is no longer lawfully required;
- object to certain processing, including direct marketing where applicable;
- request restriction or limitation of processing where recognised by the applicable law;
- withdraw consent where a particular processing activity is based on consent, without affecting lawful processing already undertaken;
- request data portability where that right applies in the relevant jurisdiction;
- exercise rights relating to solely automated decisions or profiling where applicable; and
- raise a privacy complaint with Sybrin and, if necessary, with the competent supervisory authority.

These rights are not absolute. Sybrin may be required to retain or continue processing certain information for contractual, tax, regulatory, legal claim, audit, investigation, security, or other lawful purposes.

17. How to exercise your rights or raise a concern

You may exercise the privacy rights available to you under the law applicable to the relevant processing by contacting the applicable regional privacy contact or the central PIMS/privacy contact listed in section 3. The table below explains how the main rights can be exercised in practice.

Right / request	How to exercise it
Access / confirmation	Ask whether Sybrin holds personal information about you and request access to the relevant information. Identify the record, system, process or period concerned so that the request can be located efficiently.
Correction / update	Identify the information that is inaccurate, incomplete, misleading or outdated, state the correction required and, where reasonably necessary, provide supporting information showing the correct details.
Deletion / destruction / erasure	Identify the information you want deleted or destroyed and explain the basis for the request. Sybrin will assess whether it is still legally, contractually or operationally authorised or required to retain the information before deleting it.

Right / request	How to exercise it
Objection / restriction of processing	Identify the processing activity you object to or want restricted and explain the relevant circumstances. Where the applicable law permits an objection without reasons, including certain direct-marketing objections, no additional justification will be required.
Withdrawal of consent	Where a specific activity is based on your consent, state that you withdraw that consent and identify the activity concerned. Withdrawal applies going forward and does not affect processing already lawfully undertaken or processing that Sybrin may continue on another lawful basis.
Direct-marketing opt-out	Use the unsubscribe or opt-out method in the communication, where provided, or contact the privacy team and identify the marketing channel or contact details concerned. Sybrin will retain only the minimum suppression information necessary to honour the opt-out where appropriate.
Cookie / tracking consent withdrawal, where applicable	Use the website cookie-preference tool where available, or contact the privacy team. Withdrawal will apply to non-essential tracking going forward and does not affect processing lawfully undertaken before the preference was changed.
Data portability, where applicable	Identify the personal information concerned and, where relevant, the preferred recipient or format. This right will be applied only where it exists under the law applicable to the processing.
Automated decision / profiling rights, where applicable	Identify the decision or process concerned and request the applicable explanation, review, representation or human intervention available under the relevant law.
Privacy complaint	Describe the privacy concern, the processing activity involved and the outcome you are seeking. Include any relevant dates or references that will help Sybrin investigate the matter.

How to submit a formal request: Send the request to the applicable regional privacy contact or the central PIMS/privacy contact listed in section 3. The request should, where possible, include your full name, the relevant Sybrin entity or region, the right you are exercising, the information or processing concerned, and sufficient detail for the request to be understood and located. Do not send passwords or unnecessary identity documents by ordinary email.

Identity and authority checks: Sybrin may request proportionate information to verify your identity or, where another person acts for you, their authority. Verification information will be limited to what is reasonably necessary to prevent unauthorised access, alteration or deletion.

Forms and assistance: You do not need to use an internal Sybrin template if the substance of your request is clear, unless the applicable law requires a prescribed form. In South Africa, objections under POPIA section 11(3)(a) may be submitted on Form 1, and requests for correction or deletion/destruction under section 24 may be submitted on Form 2. Sybrin will provide reasonable assistance where required.

Response and outcome: Requests will be recorded and handled within the timeframe required by the law applicable to the processing. If a request cannot be fully granted, Sybrin will explain the applicable reason where required and will identify any available internal complaint or supervisory-authority route.

You may also lodge a complaint with the competent supervisory authority where you believe your personal information has been processed unlawfully or your rights have not been appropriately addressed.

Region	Authority	Contact / complaint route	Website
South Africa	Information Regulator	enquiries@inforegulator.org.za 010 023 5200	inforegulator.org.za
Kenya	Office of the Data Protection Commissioner (ODPC)	info@odpc.go.ke 020 780 1800	odpc.go.ke
Zambia	Data Protection Commission (DPC)	(+260) 750 799 801 use current DPC contact/complaint route	dataprotection.gov.zm
Tanzania	Personal Data Protection Commission (PDPC)	helpdesk@pdpc.go.tz use current PDPC complaint route	pdpc.go.tz

17.1. Recruitment-specific rights

If you are a job applicant, you may contact the privacy contact in section 3 to request access to or correction of recruitment information, withdraw an application, object to processing based on legitimate interests where the applicable law permits, withdraw a genuinely optional consent, or request deletion where Sybrin is no longer authorised or required to retain the information. A request to withdraw from the recruitment process does not automatically require immediate deletion of every record where Sybrin must retain limited information for legal, regulatory, dispute, audit, or evidentiary purposes. You may also ask how automated or profiling tools have been used where such tools apply and the relevant law provides that right.

18. Personal data breaches and security incidents

If personal information is affected by an actual or suspected security compromise, Sybrin will manage the incident under its Information Incident Management and PII / Personal Data Breach procedures. Sybrin will investigate, contain, assess, document, remediate, and make regulator, client, or data-subject notifications where required by the law applicable to the incident.

19. Automated decision-making and profiling

Sybrin does not intend to make decisions about external data subjects that produce legal or similarly significant effects solely through automated processing unless the activity is specifically assessed, lawfully permitted, appropriately communicated, and subject to any safeguards required by the applicable law. Where AI, profiling, scoring, or automated decision-making is introduced, Sybrin will assess the activity through its PIIA process where required.

20. Breach and Non-compliance

Any non-compliance or breach of any part of this Policy by any user of this document may be subject to disciplinary action, in line with Sybrin's Disciplinary Code, which may include the termination of the user's contract or employment.

21. Document Review

This Notice 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.