

PRIVACY POLICY

Intercyte Consulting CC / SafeCyte

Document number	WIPP01	Issue date	September 2026
Document type	Policy	Revision	1
Approving Officer	Emile van Zyl	Designation	Managing Director
Original issue	June 2021	Last reviewed	September 2026

1. Objective and scope

This Privacy Policy explains how Intercyte Consulting CC, trading through the SafeCyte compliance management platform and related services ("SafeCyte", "we", "us" or "our"), collects, uses, stores, shares and protects personal information. It also explains the rights available to data subjects under South African privacy law.

This policy applies to personal information processed through our website, software platform, mobile or web-based services, customer support, business communications and related services. It is intended to support compliance with the Protection of Personal Information Act 4 of 2013 (POPIA) and other applicable South African law.

2. Key definitions

- Account: a user account created to access the Service or parts of the Service.
- Company / Responsible Party: Intercyte Consulting CC where it determines the purpose and means of processing personal information.
- Operator: a third party that processes personal information for or on behalf of a responsible party under a mandate or contract.
- Personal information: information relating to an identifiable, living natural person and, where applicable under POPIA, an identifiable existing juristic person.
- Processing: any operation or activity concerning personal information, including collection, receipt, recording, organisation, storage, updating, retrieval, use, dissemination, merging, restriction, erasure or destruction.
- Service: the SafeCyte platform, website and related Intercyte Consulting CC services.
- Special personal information: categories of information afforded additional protection under POPIA.
- Usage Data: technical and diagnostic information generated through use of the Service.
- Website: www.safecyte.co.za.
- You / data subject: the person or entity to whom personal information relates, as applicable.

3. Personal information we may collect

3.1 Information you provide

- Name, surname, job title and organisation.
- Email address, telephone number and business contact details.
- Account credentials and profile information.
- Address, city, province and postal code where relevant.
- Information submitted through forms, enquiries, demonstrations, support requests or contractual interactions.
- Information uploaded to or recorded within the SafeCyte platform by authorised customer users.

3.2 Information collected automatically

When you use our website or Service, we may collect technical information such as IP address, browser type and version, device type, operating system, pages or features accessed, dates and times of access, unique device identifiers, log information and diagnostic data.

3.3 Customer-controlled information

SafeCyte customers may use the platform to process compliance-related information about their employees, contractors, suppliers or other data subjects. In these circumstances, the customer may be the responsible party and Intercyte Consulting CC may act as an operator. Customers remain responsible for ensuring that they have an appropriate lawful basis and authority for the information they place in the platform.

4. Cookies and similar technologies

We may use cookies and similar technologies that are necessary for website or platform functionality, security, authentication, preferences, analytics and service improvement. Where required, users will be given appropriate choices regarding non-essential cookies.

- Essential cookies support authentication, security and core functionality.
- Preference or functionality cookies remember settings selected by users.
- Analytics technologies may help us understand how the website or Service is used and improve performance.

Browser settings may allow you to block or delete cookies. Blocking essential cookies may affect the operation of parts of the Service.

5. Why we process personal information

We process personal information only where there is an appropriate purpose and lawful justification. Depending on the circumstances, this may include consent, performance of a contract, compliance with a legal obligation, protection of a legitimate interest, or another basis permitted by POPIA.

- To provide, operate, secure and maintain the SafeCyte Service.
- To create and administer user accounts and authorised access.
- To perform contracts and provide purchased or requested services.
- To provide implementation, support, training and customer service.
- To communicate service, operational, security and account information.
- To respond to enquiries, requests and complaints.
- To maintain business, compliance, audit and security records.
- To analyse usage, troubleshoot problems and improve our services.
- To protect our rights, systems, customers and users and to prevent misuse or fraud.
- To send marketing or business communications where permitted by law and subject to applicable opt-out or consent requirements.

6. Direct marketing

Where we send electronic direct marketing communications, we will do so in accordance with applicable requirements under POPIA and other relevant South African law. Where consent is required, we will seek it before sending such communications. Recipients may opt out or object to direct marketing using the mechanism provided in the communication or by contacting us.

7. Sharing personal information

We do not sell personal information. We may disclose or provide access to personal information where reasonably necessary for the purposes described in this policy, including:

- Service providers and operators that provide hosting, infrastructure, communications, analytics, security, support or other services to us.
- Professional advisers, auditors or insurers where reasonably necessary.

- Affiliates or business partners where lawful and appropriate.
- A purchaser, successor or other relevant party in connection with a genuine merger, restructuring, financing or sale of all or part of the business.
- Public authorities, regulators, courts or law-enforcement bodies where required or permitted by law.
- Other parties where the data subject has consented or directed us to disclose the information.

Operators processing personal information on our behalf are expected to process it only under appropriate instructions and to apply suitable confidentiality and security safeguards.

8. Retention and deletion

We retain personal information only for as long as reasonably necessary for the purpose for which it was collected or subsequently processed, and for any period required or permitted by applicable law, contract, dispute-resolution, audit or legitimate record-keeping requirements. When personal information is no longer required, it will be deleted, destroyed or de-identified as appropriate.

9. Cross-border transfers

Our services and service providers may involve processing or storage outside South Africa. Where personal information is transferred to a third party in a foreign country, we will take reasonable steps to ensure that the transfer is permitted under section 72 of POPIA, including through an adequate level of protection, appropriate binding arrangements, consent, contractual necessity or another lawful basis recognised by POPIA.

10. Security of personal information

We use appropriate, reasonable technical and organisational measures designed to protect personal information against loss, damage, unauthorised destruction, unlawful access or unlawful processing. Measures are reviewed in light of the nature of the information, foreseeable risks and available safeguards.

No method of electronic transmission or storage can be guaranteed to be completely secure. Users are also responsible for protecting their account credentials and promptly notifying us of suspected unauthorised access.

11. Security compromises

Where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, we will assess the incident and, where required by POPIA, notify the Information Regulator and affected data subjects as soon as reasonably possible, subject to lawful restrictions or directions.

12. Your rights

Subject to POPIA and applicable limitations, data subjects may have the right to:

- Be informed when personal information is collected and about the purpose of processing.
- Request confirmation of whether we hold personal information about them and request access to it.
- Request correction or deletion of personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained.
- Object, on reasonable grounds where applicable, to certain processing.
- Object to direct marketing and withdraw consent where processing is based on consent.
- Request deletion or destruction where permitted by law.
- Lodge a complaint with the Information Regulator.

We may need to verify identity before acting on a request. Certain information may need to be retained where required or permitted by law.

13. Special personal information and children's information

Where the Service is used to process special personal information or personal information relating to children, such processing must have an appropriate legal basis and must comply with the additional requirements of POPIA.

Customers using SafeCyte are responsible for ensuring that information they submit to the platform is collected and processed lawfully.

14. Third-party websites and services

Our website or Service may contain links to third-party websites or services. We do not control those third parties and are not responsible for their privacy practices. Users should review the applicable privacy notices before providing personal information to third parties.

15. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes to our services, processing activities, technology, legal requirements or regulatory guidance. The current version will be published on our website with the applicable review or update date. Where a change is material, we may provide additional notice where appropriate.

16. Contact us

Questions, privacy requests or concerns regarding this Privacy Policy may be directed to:

- Email: emile@intercyte.co.za
- Email: helia@intercyte.co.za
- Website: www.safecyte.co.za

Data subjects may also lodge complaints with the Information Regulator (South Africa) using the Regulator's official channels.

17. Revision history

Section / paragraph	Rev. No.	Amendments	Date	Name
Entire document	1	Reviewed and updated for 2026; modernised terminology, POPIA rights, direct marketing, security compromises, operators, retention and cross-border processing.	September 2026	Emile van Zyl