



INTEGRATED
COMPLIANCE SOLUTIONS

PRIVACY POLICY

Governance | Risk | Compliance | Technology

Privacy governance for compliance architecture,
regulatory operations and controlled information handling.

Version 1.0 | Effective Date: 1 February 2026

Public / Website Legal Document



DOCUMENT CONTROL

Document purpose: This Privacy Policy explains how Integrated Compliance Solutions collects, receives, records, stores, uses, discloses, protects, retains and destroys personal information in line with POPIA and related South African information governance requirements.

Control Item	Detail
Document Name	Privacy Policy
Entity	Integrated Compliance Solutions
Registration Number	2025/830678/07
Version	1.0
Effective Date	1 February 2026
Document Owner	ICS
Approved By	ICS Board
Review Cycle	Annual or as required by legal, regulatory, operational or data processing changes
Classification	Public / Website Legal Document
Website	www.integratedcompliancesolutions.co.za
Contact Person	Compliance Team
Contact Email	info@integratedcompliancesolutions.co.za

ENTITY DETAILS

Item	Detail
Legal Name	Integrated Compliance Solutions
Registration Number	2025/830678/07
Enterprise Type	Private Company
Physical Address	122 Beech Street, Northcliff, Randburg, Gauteng, 2195
Registered Office Address	122 Beech Street, Northcliff, Randburg, Gauteng, 2195
Website	www.integratedcompliancesolutions.co.za
Email	info@integratedcompliancesolutions.co.za
Contact Person	Compliance Team



TABLE OF CONTENTS

DOCUMENT CONTROL	2
ENTITY DETAILS	2
TABLE OF CONTENTS.....	3
1. INTRODUCTION	4
2. SCOPE AND APPLICATION	4
3. RESPONSIBLE PARTY	4
4. DEFINITIONS.....	5
5. WHAT PERSONAL INFORMATION ICS COLLECTS	6
6. SPECIAL PERSONAL INFORMATION AND CHILDREN'S INFORMATION.....	6
7. HOW ICS COLLECTS PERSONAL INFORMATION	6
8. PURPOSE OF PROCESSING	7
9. LEGAL BASIS FOR PROCESSING	8
10. WEBSITE USE, COOKIES AND ONLINE FORMS.....	8
11. DIRECT MARKETING AND COMMUNICATIONS	8
12. SHARING OF PERSONAL INFORMATION	8
13. CROSS-BORDER TRANSFERS	9
14. SECURITY SAFEGUARDS	9
15. DATA BREACH AND SECURITY INCIDENT HANDLING.....	9
16. RETENTION OF PERSONAL INFORMATION.....	9
17. DATA SUBJECT RIGHTS	9
18. ACCURACY OF PERSONAL INFORMATION	10
19. LINKS TO THIRD-PARTY WEBSITES	10
20. CHILDREN'S PRIVACY.....	10
21. CLIENT RESPONSIBILITIES	10
22. OPERATOR AND SERVICE PROVIDER PROCESSING	10
23. COMPLAINTS AND QUERIES	11
24. UPDATES TO THIS PRIVACY POLICY	11
25. CONTACT DETAILS	11



1. INTRODUCTION

- 1.1. Integrated Compliance Solutions respects privacy and is committed to processing personal information lawfully, reasonably and transparently.
- 1.2. This Privacy Policy explains how ICS processes personal information in connection with its website, onboarding, proposals, service engagements, compliance architecture work, regulatory support and ordinary business operations.
- 1.3. This Privacy Policy applies to clients, prospective clients, website users, directors, officers, Key Individuals, representatives, employees or staff members of client entities, consultants, service providers, applicants, contacts, stakeholders and any person whose personal information is processed by ICS in connection with its services.
- 1.4. This Privacy Policy is intended for publication on the ICS website and for inclusion in onboarding packs, service agreements, due diligence packs, compliance documentation and regulatory engagement packs.

2. SCOPE AND APPLICATION

- 2.1. This Privacy Policy applies to personal information processed through or in connection with:
 - the ICS website and any online forms or digital channels made available by ICS;
 - client onboarding, proposals, engagement letters, service level agreements and statements of work;
 - regulatory support engagements, compliance monitoring, reporting, AML/FIC support, POPIA support and governance support;
 - email, telephone calls, online meetings, physical meetings, document submissions, cloud folders, professional correspondence and deliverable review processes;
 - any lawful business, regulatory or operational interaction between ICS and a client, prospective client, service provider, regulator, adviser or stakeholder.
- 2.2. Where a specific agreement, mandate or statement of work contains additional data protection obligations, those obligations apply together with this Privacy Policy, unless there is a direct conflict.

3. RESPONSIBLE PARTY

3.1. Depending on the context, ICS may process personal information as a Responsible Party, an Operator or an independent professional service provider.

Role	How the role may apply
Responsible Party	ICS determines the purpose and means of processing, for example for onboarding, website use, invoicing, internal records, service administration and legal compliance.
Operator	ICS processes personal information on behalf of a client under an agreed mandate, SLA, proposal or service engagement.
Independent professional service provider	ICS processes information to perform compliance, governance, regulatory, AML/FIC, POPIA, evidence-management or operational support services within an agreed scope.

3.2. The exact role depends on the engagement, the source of the information, the relevant processing activity and the legal or regulatory context.



4. DEFINITIONS

Term	Meaning
Personal Information	Information relating to an identifiable natural person and, where applicable, an identifiable existing juristic person, as contemplated in POPIA.
Special Personal Information	Categories of information given additional protection under POPIA, including information relating to health, biometric information, criminal behaviour, religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion or sex life.
Processing	Any operation concerning personal information, including collection, receipt, recording, storage, use, disclosure, transfer, restriction, deletion or destruction.
Responsible Party	A public or private body or other person that determines the purpose and means of processing personal information.
Operator	A person or organisation that processes personal information for a Responsible Party in terms of a contract or mandate without coming under the direct authority of that Responsible Party.
Data Subject	The person to whom personal information relates.
Consent	A voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Client	A person, company, FSP, fintech, group entity, regulated institution, applicant or other organisation that engages with or receives services from ICS.
ICS	Integrated Compliance Solutions, registration number 2025/830678/07.
POPIA	The Protection of Personal Information Act, 4 of 2013, including regulations, codes, guidance and amendments applicable from time to time.
PAIA	The Promotion of Access to Information Act, 2 of 2000.
Information Regulator	The South African Information Regulator established under POPIA.
Regulatory Authority	A regulator, authority, supervisory body, self-regulatory body, ombud, court or public body with jurisdiction over the relevant activity or information.
Services	Compliance, governance, regulatory, AML/FIC, POPIA, evidence, monitoring, reporting, operational control or related advisory services provided by ICS.
Website User	A person who accesses or uses the ICS website or online channels.
Third-Party Service Provider	An external provider used by ICS or a client to support services, systems, records, cloud hosting, professional advice, delivery, communications or administration.



5. WHAT PERSONAL INFORMATION ICS COLLECTS

5.1. ICS collects only the personal information that is reasonably required for its services, business operations, legal obligations, regulatory support functions or legitimate professional purposes.

Category	Examples	Source	Purpose
Identity and contact information	Names, ID or passport details, addresses, email, telephone, job title.	Data subject, client, public records.	Identification, communication, onboarding, service delivery.
Company and registration information	Company name, registration number, tax number, office address, ownership details.	Client, CIPC, public records.	Due diligence, onboarding, regulatory support, records.
Director, shareholder, Key Individual and representative information	Roles, appointments, fit-and-proper data, CPD or competence records, oversight records.	Client, FSCA records, individuals.	Compliance support, governance mapping, licence support.
FSP and licence information	FSP number, licence categories, conditions, profile changes, representative data.	Client, FSCA, regulator records.	Regulatory support, monitoring, submissions.
Regulatory and compliance information	Policies, registers, complaints, incidents, correspondence, governance records, control logs.	Client, regulators, advisers.	Compliance architecture, monitoring, evidence management.
FIC / AML information	FIC registration details, RMCP records, CDD information, risk ratings, escalation records.	Client, accountable persons, FIC-related records.	AML/CFT support, FIC governance, risk controls.
POPIA and information officer details	Information officer details, privacy records, breach logs, PAIA or POPIA packs.	Client, authorised persons.	Information governance and privacy support.
Financial and billing information	Invoices, payment records, VAT information, banking references where applicable.	Client, accounting records, banks.	Billing, accounting, debt management and tax compliance.
Website and technical information	IP address, device data, browser type, pages visited, access time, usage patterns.	Website, cookies, analytics tools.	Website operation, analytics, security and improvement.
Communication records	Emails, meeting notes, call records, instructions, queries, approvals, sign-offs.	Data subject, client, ICS records.	Service delivery, audit trail, dispute management.
Service provider information	Supplier contact details, professional role, service records, billing details.	Service providers, client, ICS records.	Supplier management, service delivery, administration.
Due diligence information	Screening records, conflict checks, regulatory standing, sanctions or risk information where lawful.	Client, public sources, professional advisers.	Risk management, onboarding and legal compliance.
Professional profile information	CV details, qualifications, role history or professional credentials where relevant.	Data subject, client, public profiles.	Competence review, governance support, engagement administration.
Submitted information	Information submitted through forms, emails, document uploads, onboarding packs or client portals.	Website user, client or authorised person.	Responding to requests, providing services and maintaining records.

6. SPECIAL PERSONAL INFORMATION AND CHILDREN'S INFORMATION

6.1. ICS does not intentionally collect special personal information or children's information unless it is necessary for a lawful purpose, regulatory requirement, client instruction, legal obligation, employment-related matter, identity verification, due diligence, investigation or compliance engagement.

6.2. Where special personal information is processed, ICS will do so only where POPIA permits such processing and only to the extent reasonably required for the relevant purpose.

6.3. ICS services are not directed at children. Where children's information is processed, it will be processed only with an appropriate lawful basis or consent where required.

7. HOW ICS COLLECTS PERSONAL INFORMATION

7.1. ICS may collect personal information from the following sources:

- directly from the data subject;
- from client entities, directors, officers, representatives, Key Individuals and authorised persons;
- from public records, regulatory registers and official sources such as CIPC, FSCA, FIC, SARB, PASA, PAIA or other official sources where applicable;
- from third-party professional advisers, banks, payment providers, auditors, accountants, attorneys, compliance officers, consultants or technology platforms;
- through the ICS website, email, calls, meetings, forms, uploads, cloud folders, digital platforms or professional correspondence;
- through regulatory correspondence, due diligence processes, onboarding packs, evidence packs or service delivery records.

7.2. Where a client provides personal information about another person, the client is responsible for ensuring that the information may lawfully be shared with ICS.



8. PURPOSE OF PROCESSING

Purpose	Description
Responding to enquiries	Handling website, email, telephone and other requests from clients, prospective clients and stakeholders.
Client onboarding	Conducting onboarding, account setup, risk assessment, conflict checks and engagement administration.
Preparing proposals, mandates and SLAs	Preparing commercial documents, statements of work, fee schedules, engagement packs and client-specific arrangements.
Providing services	Delivering compliance, governance, regulatory, AML/FIC, POPIA, operating control and evidence-management support.
Regulatory licensing and structuring	Supporting entity, licence, category, role, profile, representative and governance configuration work.
Regulatory engagement support	Supporting FSCA, FIC, SARB, PASA or other regulatory engagement, correspondence, reports or submissions.
AML/CFT and FIC support	Supporting RMCP, CDD, risk rating, monitoring, reporting, escalation and record-keeping controls.
POPIA and information governance support	Supporting privacy governance, information officer responsibilities, breach processes and data handling controls.
Key Individual and representative oversight	Supporting oversight, competence visibility, fit-and-proper records, sign-off and conduct controls.
Preparing deliverables	Preparing reports, registers, policies, evidence packs, submissions, control matrices and review records.
Meeting and communication management	Managing meetings, action logs, instructions, approvals, decisions, review notes and follow-ups.
Invoicing and payment administration	Issuing invoices, tracking payments, accounting records, tax administration and debt management.
Record keeping	Maintaining professional, legal, regulatory, tax, contractual and historical compliance records.
Risk management and internal governance	Managing business risks, conflicts, security, quality control, insurance and governance requirements.
Legal compliance and enforcement	Complying with laws, responding to disputes, regulator queries, complaints, legal processes and enforcing agreements.
Website operation and security	Operating, securing, improving and monitoring website functionality and digital channels.



9. LEGAL BASIS FOR PROCESSING

9.1. ICS may process personal information where one or more lawful grounds apply, including where:

- the data subject has consented to the processing;
- processing is necessary to perform a contract or take steps before entering into a contract;
- processing is necessary to comply with a legal obligation;
- processing protects a legitimate interest of the data subject;
- processing is necessary for the legitimate interests of ICS, a client or a third party;
- processing is necessary for regulatory, compliance, governance, operational or legal purposes;
- processing is required or authorised by law, regulator instruction, court order or other lawful process.

9.2. The applicable legal basis may differ depending on the processing activity, the type of information, the data subject and the engagement context.

10. WEBSITE USE, COOKIES AND ONLINE FORMS

10.1. The ICS website may collect technical information such as IP address, browser type, device information, pages visited, time of access and website usage patterns.

10.2. ICS may use cookies or similar technologies for website functionality, analytics, security and improvement.

10.3. Website users may adjust browser settings to block or manage cookies, but some website functions may not work properly if cookies are disabled.

10.4. Online forms may collect information submitted by the user, including contact details, service enquiries, document requests, onboarding information or other information voluntarily provided.

10.5. Submission of an online form does not automatically create a client engagement unless ICS accepts the engagement in writing.

11. DIRECT MARKETING AND COMMUNICATIONS

11.1. ICS may communicate with clients, prospective clients and stakeholders about services, regulatory updates, compliance information, meetings, documents and related business matters.

11.2. ICS may send direct marketing only where permitted by law.

11.3. Recipients may opt out of marketing communications by using the unsubscribe mechanism provided or by contacting ICS at info@integratedcompliancesolutions.co.za.

11.4. Service-related, legal, regulatory, administrative or operational communications may still be sent where necessary for an engagement, legal obligation or operational purpose.

12. SHARING OF PERSONAL INFORMATION

12.1. ICS may share personal information where reasonably required for lawful business, professional, contractual, legal, regulatory or service delivery purposes. ICS does not sell personal information.

Recipient category	Reason for sharing
ICS personnel	Employees, directors, consultants and contractors who require access for service delivery, governance, administration or support.
Regulatory authorities	FSCA, FIC, SARB, PASA, Prudential Authority or other authorities where relevant to the engagement or required by law.
Financial institutions and payment participants	Banks, sponsor banks, payment providers, processors or financial institutions where relevant to a client mandate or due diligence process.
Professional advisers	Attorneys, auditors, accountants, insurers, consultants and other advisers where required for advice, records, risk management or legal protection.
Technology and cloud providers	Cloud hosting providers, software providers, IT support, digital platforms, communication systems and security providers.
Administrative providers	Couriers, document management providers, office services, billing support or other administration providers.
Client-appointed representatives	Authorised persons, project managers, Key Individuals, directors or nominated contacts of the client.
Third-party providers	Providers involved in the services, including consultants, systems providers, regulatory support providers or service partners.
Public bodies or courts	Courts, law enforcement, regulators, ombuds, public bodies or competent authorities where required or authorised by law.



13. CROSS-BORDER TRANSFERS

- 13.1. Personal information may be stored or processed outside South Africa where cloud platforms, software providers, support services or professional service providers are located outside South Africa.
- 13.2. ICS will take reasonable steps to ensure that cross-border transfers are lawful and subject to appropriate safeguards where required by POPIA.
- 13.3. Where a client has specific cross-border restrictions, the client must notify ICS before providing the relevant information or before instructing ICS to use a particular platform or provider.

14. SECURITY SAFEGUARDS

14.1. ICS applies reasonable technical and organisational safeguards to protect personal information against loss, damage, unauthorised access, unlawful processing, destruction or disclosure.

- access control and appropriate user permissions;
- password protection and secure account management;
- secure cloud storage and platform selection where reasonably available;
- internal confidentiality controls and need-to-know access practices;
- limited access to authorised personnel, consultants and service providers;
- information handling procedures, document control and review disciplines;
- secure disposal, deletion or archiving where appropriate and commercially practical;
- staff awareness, privacy governance practices and reasonable oversight of service providers.

Security limitation: No technology environment is completely risk-free. ICS takes reasonable steps appropriate to the nature of the information, the services and the risks involved, but does not guarantee that unauthorised access or security incidents can never occur.

15. DATA BREACH AND SECURITY INCIDENT HANDLING

- 15.1. Where ICS reasonably believes that personal information under its control has been accessed or acquired by an unauthorised person, ICS will assess the incident and take reasonable steps appropriate to the nature and severity of the incident.
- 15.2. ICS will notify affected parties and/or the Information Regulator where required by POPIA.
- 15.3. Notifications will be made within a reasonable time, taking account of investigation requirements, security considerations, legal obligations and operational constraints.
- 15.4. Clients must notify ICS promptly if they become aware of any security incident involving information shared with ICS, processed by ICS or relevant to an ICS engagement.

16. RETENTION OF PERSONAL INFORMATION

16.1. ICS retains personal information only for as long as reasonably necessary for lawful business, professional, legal, regulatory, contractual or operational purposes.

- service delivery
- legal compliance
- regulatory records
- professional records
- tax and accounting requirements
- dispute management
- insurance purposes
- audit trails
- historical compliance evidence
- legitimate business purposes
- contractual obligations

16.2. Information may be deleted, destroyed, archived, de-identified or returned where appropriate and legally permissible, subject to retention obligations and operational constraints.

17. DATA SUBJECT RIGHTS

17.1. Data subjects have rights under POPIA, subject to the limits and procedures contained in POPIA and other applicable law. These rights include the right to:

- request access to personal information held by ICS;
- request correction or deletion of inaccurate, irrelevant, excessive, outdated, incomplete, misleading or unlawfully obtained personal information;
- object to processing in certain circumstances;
- withdraw consent where processing is based on consent;



- complain to ICS about processing of personal information;
- lodge a complaint with the Information Regulator.

Data subject request contact: Requests may be sent to the Compliance Team at info@integratedcompliancesolutions.co.za or delivered to 122 Beech Street, Northcliff, Randburg, Gauteng, 2195. ICS may request proof of identity and sufficient information to process the request.

18. ACCURACY OF PERSONAL INFORMATION

- 18.1. ICS relies on the information provided by clients, data subjects, authorised persons and third parties.
- 18.2. Clients and data subjects must ensure that information provided to ICS is complete, accurate and up to date.
- 18.3. ICS may request updated information where required for compliance, governance, service delivery, regulatory support, record keeping or risk management.

19. LINKS TO THIRD-PARTY WEBSITES

- 19.1. The ICS website may contain links to third-party websites, platforms or resources for convenience or reference.
- 19.2. ICS is not responsible for the privacy practices, security, terms, availability or content of third-party websites or platforms.
- 19.3. Users should review the privacy policies and terms of third-party websites before providing personal information to those websites.

20. CHILDREN'S PRIVACY

- 20.1. ICS services are not directed at children.
- 20.2. ICS does not knowingly collect children's personal information through the website unless required for a lawful purpose and permitted by POPIA.
- 20.3. Where a child's information is processed in connection with a client instruction, legal obligation, regulatory requirement or professional engagement, ICS will process it only with an appropriate legal basis or consent where required.

21. CLIENT RESPONSIBILITIES

- 21.1. Clients must:
 - ensure that any personal information provided to ICS has been collected lawfully and may lawfully be shared with ICS;
 - notify data subjects where required;
 - obtain consent where consent is required;
 - avoid providing unnecessary or excessive personal information;
 - provide accurate, complete and current information;
 - notify ICS of restrictions, confidentiality obligations, regulator sensitivities or processing limitations that may affect the engagement;
 - promptly inform ICS of any security incident, regulatory concern or data subject request relevant to information shared with ICS.

22. OPERATOR AND SERVICE PROVIDER PROCESSING

- 22.1. Where ICS acts as an Operator for a client, ICS will process personal information according to the client's lawful instructions, the engagement scope and applicable law.
- 22.2. Where ICS determines its own purposes and means of processing, ICS may act as a Responsible Party for that processing activity.
- 22.3. Where ICS appoints its own operators or service providers, ICS will take reasonable steps to ensure appropriate confidentiality and data protection controls are in place, taking account of the service and risk involved.
- 22.4. ICS may use cloud platforms, communication systems, software, consultants, contractors and professional service providers where reasonably required for its services or business operations.



23. COMPLAINTS AND QUERIES

23.1. Privacy queries, POPIA requests or complaints should be sent to info@integratedcompliancesolutions.co.za with the subject line 'Privacy Query' or 'POPIA Request'.

Stage	Process
Step 1	Provide your name, contact details, description of the request or complaint, and proof of identity where required.
Step 2	ICS will acknowledge, assess and respond within a reasonable time, taking account of the nature of the request and applicable law.
Step 3	Where necessary, ICS may request additional information to verify identity, locate records or understand the request.
Information Regulator	Data subjects may also complain to the Information Regulator South Africa. Website: [Insert Information Regulator Website]. Email: [Insert Information Regulator Complaints Email].

24. UPDATES TO THIS PRIVACY POLICY

24.1. ICS may update this Privacy Policy from time to time due to changes in law, regulatory requirements, business operations, systems, services, security practices or information processing activities.

24.2. The latest version should be made available on the ICS website.

24.3. Material changes may be communicated where appropriate, but users and clients are encouraged to review the Privacy Policy periodically.

25. CONTACT DETAILS

Contact Field	Detail
Entity	Integrated Compliance Solutions
Registration Number	2025/830678/07
Contact Person	Compliance Team
Email	info@integratedcompliancesolutions.co.za
Website	www.integratedcompliancesolutions.co.za
Physical Address	122 Beech Street, Northcliff, Randburg, Gauteng, 2195
Document Owner	ICS
Approved By	ICS Board
Effective Date	1 February 2026