# Privacy Statement

## How Lighthouse Risk Consulting handles personal information

| | |
|---|---|
| **Responsible party** | Lighthouse Risk Consulting (Pty) Ltd |
| **Effective date** | 15 September 2026 |
| **Document owner** | Information Officer |
| **Applies to** | Website visitors, business clients, representatives, delegates, suppliers and persons whose records are lawfully reviewed |
| **Review trigger** | At least annually and whenever processing, platforms or applicable law materially changes |

## 1. Privacy at a glance

Lighthouse Risk Consulting (Pty) Ltd (Lighthouse, we, us or our) is a South African regulatory compliance, governance, risk, training and business-support consultancy serving financial services businesses. We process personal information only when it is reasonably necessary for a specific, lawful business or regulatory purpose and we limit access to people and service providers who need it.

Our compliance work focuses principally on information about Financial Services Providers (FSPs), key individuals, representatives, personnel, contractors and service providers. When we perform compliance monitoring activities (e.g. inspection of an FSP client file0, the underlying client or policyholder information is reviewed only to assess whether the FSP has reasonably met applicable FAIS, General Code of Conduct and related compliance requirements. Ongoing compliance evaluation and monitoring shall further include policies, processes, procedures and any related artifacts to assess compliance assurance, and ultimately provided reporting back to the FSP, and its leadership.

Information is not collected to build a Lighthouse marketing database, provide financial advice to that client, or take over the FSP's client relationship. This Statement gives notice under the Protection of Personal Information Act 4 of 2013 (POPIA). It should be read with our PAIA Manual and any engagement-specific privacy notice, mandate, operator agreement or platform terms that apply to a particular service.

## 2. Who is covered and the roles we perform

For clarity, this Statement uses the following practical descriptions:

- Business client means the FSP, employer, product supplier, professional body or other organisation that engages Lighthouse, on a frequent and ongoing basis.
- Representative includes representatives, key individuals, supervised representatives and other personnel whose competency, conduct or compliance records are assessed or administered.
- Inspected client means the individual or organisation whose file is held by a business client and selected for a compliance inspection.
- Data subject has the meaning given in POPIA and may be a natural or juristic person.

Lighthouse is the responsible party when it determines why and how personal information is processed for its own client administration, contracting, invoicing, communications, website, training-provider, governance and legal-compliance purposes.

Where Lighthouse accesses or handles an FSP's underlying client information solely on that FSP's documented instructions for a file inspection, Lighthouse ordinarily acts as an operator and the FSP remains the responsible party. The role is determined by the actual processing arrangement, not merely by the name of a platform or contract.

## 3. Information we may process

### 3.1. Business clients and contacts

We may process names, job titles, identity and registration details where necessary, business and contact details, mandates, correspondence, contracts, billing and payment records, regulatory status, complaints, service history, meeting notes and access credentials allocated to authorised users.

### 3.2. FSPs, key individuals and representatives

Depending on the agreed service, information may include FSCA, FIC, CMS identifiers (and where applicable NCR), roles and authorisations, dates of first appointment, product subcategories, qualifications, regulatory examinations, class of business and product-specific training, experience, supervision, continuous professional development, professional memberships, employment history, honesty and integrity declarations, competency evidence, monitoring findings, remedial actions and audit trails. This shall at all times include any and all related information for compliance and lawful purposes.

### 3.3. Inspected client files

A sampled file may incidentally contain identifying and contact details, financial product information, needs-analysis and advice records, disclosures, replacement or conflict records, instructions, communications, complaints, transaction evidence and, where relevant to the product and lawfully held by the FSP, limited financial or health-related information. Lighthouse reviews only what is reasonably necessary for the stated monitoring purpose. Findings should use the least identifying detail reasonably needed to evidence the compliance conclusion.

### 3.4. Suppliers, prospective contractors and other persons

We may process business contact details, qualifications, references, declarations, screening results, bank and tax details, contracts, invoices, communications and service-performance records. Special personal information or criminal-behaviour information is processed only where POPIA permits it and, where required, with consent or another applicable statutory authorisation.

### 3.5. Website and electronic communications

We may process information voluntarily submitted through a website contact form or email and limited technical information generated by normal hosting and security operations, such as IP, device, browser and security-log data. Lighthouse does not use or collect cookie information through its website. This Statement will be updated before any cookie-based technology may be introduced.

## 4. Why we process information

- To assess, accept, scope, deliver and administer consulting, compliance, training, monitoring, assurance and related services in order to help business clients and their people understand, evidence and uphold lawful obligations in the South African financial services industry.
- To inspect sampled client files and report whether applicable FAIS, General Code of Conduct and related standards appear to have been reasonably met.
- To maintain competency, CPD, supervision, training, appointment, declaration and compliance records where included in the mandate.
- To manage access, platform accounts, service support, security, business continuity and audit trails.
- To contract, invoice, account, recover lawful debts and meet tax, company, professional and regulatory duties.
- To respond to enquiries, complaints, data-subject requests, PAIA requests, litigation, regulatory inspections and lawful directions.
- To prevent or investigate misuse, fraud, security incidents, conflicts, misconduct and material regulatory risk; and to communicate relevant services or regulatory developments in a lawful and proportionate manner, with an effective opt-out where required.

Personal information will not be used for a new purpose that is incompatible with the purpose for which it was collected unless POPIA permits the further processing. Lighthouse takes reasonably practicable steps to keep information complete, accurate, not misleading and updated where this is necessary for its intended use, taking account of the source and purpose of the information.

## 5. Lawful grounds

Consent is not the only, or necessarily the primary, ground for processing. Depending on the context, Lighthouse relies on one or more grounds as may be permitted in POPIA as follows:

- Performance of or steps toward a contract;
- Compliance with an obligation imposed by law;
- Protection of a legitimate interest of the data subject; and
- Processing necessary to pursue the legitimate interests of Lighthouse, a business client or another authorised third party.

Consent is used where it is the appropriate legal ground, including where a special-information rule, screening process or direct-marketing rule requires it.

Our legitimate interests include delivering competent compliance support, maintaining reliable regulatory evidence, protecting systems and confidential information, administering client relationships and helping regulated businesses manage legal and conduct risk.

Before relying on legitimate interests, we consider necessity, proportionality, reasonable expectations, safeguards and the potential effect on the data subject. A data subject may object on reasonable grounds relating to their particular situation where relevant, unless legislation requires the processing.

The underlying financial-services obligations may arise, depending on the client and service, from the Financial Advisory and Intermediary Services Act 37 of 2002, its subordinate instruments including the General Code of Conduct and Fit and Proper Requirements, the Financial Intelligence Centre Act 38 of 2001, the Financial Sector Regulation Act 9 of 2017, applicable medical-schemes requirements and other binding sectoral rules.

Listing a law does not mean every law or provision applies to every engagement.

## 6. How information is obtained

Information may be obtained directly from the data subject; from the business client or an authorised person; from an employer, product supplier, training provider, professional body or regulator; from public registers and deliberately public sources; from service providers carrying out authorised verification; from the platforms used to deliver the service; and from website or system interactions.

Indirect collection is used only when permitted by in POPIA and appropriate to the purpose.

Supplying information may be mandatory where a law, regulatory requirement, contract or verification process requires it. If necessary information is not supplied, Lighthouse or the business client may be unable to complete an assessment, verify compliance, grant access, issue evidence, perform the service or meet a legal duty.

We will not treat optional website marketing information as mandatory for receiving an unrelated service.

## 7. Platforms and service providers

Lighthouse uses carefully selected platforms and providers to support controlled delivery. Current material platforms and or providers may include:

| Provider or Platform | Business purpose | Privacy position |
|---|---|---|
| FSPHub | Compliance practice management, workflow, records and reporting relevant to the agreed service. | Access is limited to authorised users and the information reasonably needed for the configured service. |
| ACDevelop | Training, product-specific training, CPD, competency records, assessments and regulatory reporting. | Information is used to administer learning and evidence completion, competency or participation. |
| DotsAfrica | Authorised identity, qualification, background or related due-diligence verification when required for the engagement. | Screening is initiated only where lawful, relevant and appropriately authorised; results are restricted. |
| Viljieco IT | Managed IT services supporting the security and resilience of Lighthouse's IT infrastructure. | Access is limited to operational need and subject to confidentiality, security and appropriate operator controls. |

These providers, and any hosting, communications, accounting, security, professional or support providers, may act as operators or as separate responsible parties for defined processing.

Lighthouse requires appropriate confidentiality, security and processing commitments where POPIA's operator provisions apply. A provider's own privacy notice may also apply when a person directly creates or controls an account with that provider.

A named provider is not authorised to use inspected client information for unrelated advertising or to determine an FSP client's, or other Business client's regulatory or employment outcome. Platform-generated flags, scores or workflow prompts support human review and do not by themselves replace the responsible decision-maker.

## 8. Sharing and disclosure

Personal information may be supplied, only where appropriate to the purpose, to the engaging business client and its authorised personnel; product suppliers, professional bodies and training or verification providers i.e. FSPHub, ACDevelop and DotsAfrica, as well as Viljieco IT, Lighthouse's appointed managed service provider; secure technology, hosting, backup and communications providers; accountants, insurers, attorneys and other professional advisers; banks and payment providers; regulators, ombuds, statutory bodies, courts and

law-enforcement authorities; and prospective parties to a lawful business reorganisation subject to confidentiality and due diligence.

Lighthouse does not sell personal information. We do not disclose information to another competing business client. Where PAIA, litigation or a regulator requires disclosure, privacy, confidentiality, privilege and third-party rights remain subject to the applicable law.

## 9. Cross-border processing

Some cloud, communications, support or backup services may process or permit support access to information outside South Africa. A transfer will be made only where POPIA permits it, including where the recipient is subject to a law, binding corporate rules or an agreement that provides an adequate level of protection. The location and safeguards of material platforms should be confirmed in the relevant supplier register and contract before publication of any country-specific representation.

## 10. Security and incident response

Lighthouse applies reasonable, risk-based technical and organisational safeguards having regard to the nature of the information, foreseeable risks, available technology and the cost of implementation. Measures may include role-based and least-privilege access, strong authentication, secure configuration, encryption in transit and where appropriate at rest, endpoint protection, backups, logging, confidentiality undertakings, secure transfer methods, supplier due diligence, restricted screening results, retention controls, staff or contractor awareness and incident-response procedures.

Lighthouse has appointed Viljieco IT as its managed service provider to support IT infrastructure security. Lighthouse retains its POPIA accountability and supplier oversight; Viljieco IT must limit any access and processing to authorised support under appropriate confidentiality, security and operator controls.

No method of storage or transmission is completely risk-free. If there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, Lighthouse will investigate, contain and document the event and will notify the responsible party, Information Regulator and affected data subjects where and in the manner evisaged in POPIA. Where Lighthouse acts as operator, it will notify the responsible party immediately in accordance with the relevant regulatory sections.

## 11. Retention and disposal

We keep personal information only for as long as it is authorised and reasonably needed for the original purpose, a compatible purpose, a contract, the establishment or defence of legal claims, or an applicable recordkeeping duty. The applicable period varies by record and may be affected by FAIS, FICA, tax, company, professional-body, contractual, complaint, litigation-hold or regulatory requirements.

For client-file compliance monitoring, the preferred approach is controlled access to the business client's source record and retention of a proportionate finding or working-paper reference rather than an unnecessary duplicate of the full client file. Any working copy must be returned, securely destroyed, deleted, de-identified or restricted when the authorised purpose and retention basis end. Destruction or deletion shall prevent reconstruction in an intelligible form.

## 12. Your rights and how to use them

Subject to POPIA, PAIA and other applicable law, a data subject may ask whether Lighthouse holds personal information about them; request access; request correction or deletion of information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained; request destruction or deletion of a record Lighthouse is no longer authorised to retain; object on reasonable grounds to processing; object to direct marketing; withdraw consent where consent is relied on; and complain to the Information Regulator.

Confirmation of whether Lighthouse holds personal information about the requester is free of charge. To request confirmation of whether Lighthouse holds your personal information, or to request access to that information please complete the prescribed PAIA Form 2 contained in Lighthouse's PAIA Manual. A personal requester is not charged the PAIA request fee, although prescribed access, reproduction, search, preparation or transfer fees may apply where permitted. Adequate certified proof of identity will be required.

## 13. Data subject access and request forms

| Request | Legal route | Form or channel |
|---|---|---|
| Confirm whether Lighthouse holds personal information | POPIA sections 23(1)(a) and 25 | Prescribed **PAIA Form 2**. Confirmation is free of charge. |
| Obtain a record or description of personal information | POPIA sections 23(1)(b) and 25; PAIA section 53 | Prescribed **PAIA Form 2** |
| Object to lawful-interest or direct-marketing processing | POPIA section 11(3) | **POPIA Form 1**, or a substantially similar permitted submission. |
| Correct or delete information, or destroy or delete a record | POPIA section 24 | **POPIA Form 2**, or a substantially similar permitted submission. |
| Complain about interference with personal-information protection | POPIA sections 73 to 75 | **POPIA Form 5** or the Information Regulator's eServices channel. |

An objection may be submitted free of charge in a form substantially similar to current POPIA Form 1. A correction, deletion or destruction request may be submitted free of charge in a form substantially similar to current POPIA Form 2. The amended Regulations permit accessible submission channels, including hand delivery, post, email, SMS, WhatsApp or another expedient manner; a telephonic request or objection must be recorded and made available to the data subject on request. Use only a verified Lighthouse contact channel.

Lighthouse will notify the data subject in writing of the action taken on a correction, deletion or destruction request within 30 days after receipt. Depending on the facts, Lighthouse may correct, destroy or delete the information, provide credible supporting evidence, or, where agreement cannot be reached and the data subject asks, attach an indication that correction was requested but not made. Where a change affects a decision about the data subject, Lighthouse will, if reasonably practicable, inform relevant recipients to whom the information was disclosed.

A request must identify the person, information or processing concerned and provide enough detail to verify identity or authority safely. Lighthouse may refuse or limit a request where the law requires or permits this, including to protect another person’s privacy, confidential commercial information, privilege, security or a lawful retention duty. Lighthouse will assess an objection and stop the affected processing where POPIA requires. A complaint alleging interference with personal information may be submitted to the Information Regulator using current POPIA Form 5 or the Regulator’s online process.

## 14. Direct marketing and website cookies

Lighthouse may send relevant business-to-business regulatory or service communications where lawful. Unsolicited electronic direct marketing will comply with POPIA and the applicable Regulations. Where prior consent is required, Lighthouse will request it once from a non-client through a permitted accessible method.

A telephonic or automated-call consent request must be recorded; an opt-out does not constitute consent. Existing-client marketing will be limited to Lighthouse's own similar services and will provide an opportunity to object at collection and in every communication. A recipient may opt out at any time without charge.

Lighthouse does not use or collect cookie information through its website, including for analytics, preferences, profiling, advertising or direct marketing. This Statement and any required transparency or consent controls will be implemented before cookie information is collected or used.

## 15. Children and special personal information

Lighthouse's services are directed to businesses and financial-services professionals, not children. Personal information of a child, health information, criminal-behaviour information, biometrics and other special personal information will be processed only when relevant and authorised under POPIA. If such information appears incidentally in an inspected activity, access is restricted to the lawful inspection purpose and it must not be repurposed. A competent person's consent or another applicable statutory authorisation must exist where POPIA requires it.

Where proposed processing falls within the parameters of "prior authorisation" in terms of POPIA, including qualifying processing of criminal-behaviour information on behalf of third parties, Lighthouse will obtain prior authorisation or confirm that the responsible party has done so before the processing begins, unless a lawful exemption applies. Health information will also be handled in accordance with the Regulations relating to the Processing of Data Subjects' Health Information by Certain Responsible Parties, 2026, where those Regulations apply to the responsible party or processing concerned.

## 16. Complaints and the Information Regulator

Please raise a concern with the Information Officer first so that Lighthouse can investigate and respond. This does not remove the right to complain to the Information Regulator.

The Regulator's current published details are:

Woodmead North Office Park,
54 Maxwell Drive,
Woodmead,
Johannesburg,
2191

Telephone: 010 023 5200 | Toll-free: 0800 017 160 | Email: enquiries@inforegulator.org.za;
POPIA complaints: POPIAComplaints@inforegulator.org.za | https://eservices.inforegulator.org.za.

## 17. Changes to this Statement

We will update this Statement when material processing, platforms, safeguards or legal requirements change. The current version and effective date will be displayed on the website. Material changes will be communicated through a proportionate channel where required.

## VERSION CONTROL AND DOCUMENT MANAGEMENT SHEET

| DOCUMENT IDENTIFICATION | |
|---|---|
| **REQUIRMENT** | **DETAILS** |
| Policy Title | **COMPLAINTS MANAGEMENT FRAMEWORK** |
| Policy ID | PS_GOV_2026_1.0 |
| Document Type | Privacy Statement |
| Policy Category | Governance |
| Applies To | Company Representatives and Staff (as applicable) |
| Document Owner | Jaco ("JP") Moolman |
| Approval Authority | |
| Approval Date | 2026/09/15 |
| Policy Status | Active |
| Next Review Date | 2027/09/15 |

| Version History | | | |
|---|---|---|---|
| **Version** | **Date** | **Description of Change** | **Approval by** |
| 1.0 | 2026/09/15 | First issue of Privacy Statement | Managing Director |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| DISTRIBUTION & AWARENESS | |
|---|---|
| **DESCRIPTION** | **DETAILS** |
| Communication to | **Staff, Clients** |
| Method of Communication | Website |
| Acknowledgement Required | Yes |
| Record Location | FSPHub: Lighthouse Compliance: Governance |
| | |

**CONTROL STATEMENT**

This is a controlled notification document. Only the version indicated above is valid and enforceable. Unauthorised changes are prohibited. Superseded versions must be clearly marked and archived.

If a notification cannot be clearly identified, versioned, and owned, it is not under control.

**Authoritative references:**

**Protection of Personal Information Act 4 of 2013:** https://www.justice.gov.za/legislation/acts/2013-004.pdf

**Promotion of Access to Information Act 2 of 2000:** https://www.justice.gov.za/legislation/acts/2000-002.pdf

**Department of Justice PAIA legislation and notices:** https://www.justice.gov.za/paia/paia.htm - includes the 2021 PAIA Regulations and the 2025 POPIA Regulations amendment

**POPIA health-information regulations 2026:** https://www.gov.za/sites/default/files/gcis_document/202603/54268gon7198.pdf - GG 54268, GoN 7198 of 6 March 2026

**Information Regulator POPIA forms:** https://inforegulator.org.za/popia-forms/

**Information Regulator contact and complaints:** https://inforegulator.org.za/contact-us/