



LEGAL & POLICY

POPIA Policy

MyOwn ISP's compliance framework under the Protection of Personal Information Act

Applies to: myownisp.co.za and the MyOwn ISP Client Portal

1. Purpose and scope

This POPI Policy sets out how MyOwn ISP, a division of ATEC Systems & Technologies (Pty) Ltd ("MyOwn ISP", "we", "us", "our") complies with the Protection of Personal Information Act 4 of 2013 ("POPIA") when processing the personal information of clients, prospective clients, website and Client Portal users, employees, suppliers and other third parties.

This Policy applies to all personal information processed by MyOwn ISP, whether collected through our website, the Client Portal, our sales and support channels, or via our network partner FibreNetworks and other Fibre Network Operators ("FNOs"). It should be read together with our Privacy Policy, which explains in customer-facing terms what information we collect and why, and our Refund & Cancellation Policy.

2. Definitions

- **Personal information:** information relating to an identifiable, living natural person or existing juristic person, as defined in section 1 of POPIA.
- **Processing:** any operation performed on personal information, including collection, storage, use, dissemination or destruction.
- **Data subject:** the person to whom personal information relates (e.g. a client, portal user, or employee).
- **Operator:** a third party that processes personal information on our behalf under contract (e.g. a payment gateway or hosting provider).
- **Information Regulator:** the statutory body established under section 39 of POPIA to oversee compliance.

3. Our Information Officer

Information Officer	Marijke van Zyl
Email	marijke@atec.co.za
Telephone	082 370 2519
Deputy Information Officer(s)	None appointed

The Information Officer is responsible for encouraging compliance with POPIA within MyOwn ISP, dealing with requests made to the company in terms of POPIA, working with the Information Regulator, and ensuring internal compliance measures are developed, implemented, monitored and maintained, including this Policy, our PAIA Manual, and our internal record of processing activities.

4. The eight conditions for lawful processing

MyOwn ISP processes personal information in accordance with the eight conditions for lawful processing set out in Chapter 3 of POPIA:

4.1 Accountability (section 8)

MyOwn ISP is responsible for ensuring that the conditions for lawful processing, and all measures giving effect to them, are complied with at the time personal information is collected and throughout processing.

4.2 Processing limitation (sections 9–12)

We only process personal information lawfully and in a manner that does not infringe the privacy of the data subject. Processing is minimal and limited to what is adequate, relevant and not excessive, and takes place only where a lawful justification applies — for example, the data subject's consent, performance of a contract (such as our service agreement), compliance with a legal obligation (such as RICA or ICASA regulations), or MyOwn ISP's legitimate interest in operating and securing its network. Where required, we collect personal information directly from the data subject.

4.3 Purpose specification (sections 13–14)

Personal information is collected for a specific, explicitly defined and lawful purpose connected to providing fibre connectivity, billing, support and related Services, and is not kept for longer than is necessary to achieve that purpose, subject to legal, contractual and regulatory retention requirements (see our Privacy Policy, clause 7).

4.4 Further processing limitation (section 15)

Further processing of personal information must be compatible with the purpose for which it was originally collected. Before processing personal information for a new purpose, we assess compatibility with the original purpose, the nature of the information, the consequences for the data subject, and how the information was collected.

4.5 Information quality (section 16)

We take reasonably practicable steps to ensure personal information is complete, accurate, not misleading, and updated where necessary, including giving clients the ability to update their details through the Client Portal.

4.6 Openness (sections 17–18)

We maintain documentation of processing operations, and, unless an exclusion under section 18(4) of POPIA applies, we take reasonably practicable steps to ensure data subjects are aware of what information is being collected, from what source, the purpose of collection, whether the supply is voluntary or mandatory, and the consequences of not providing the information. This is given effect primarily through our Privacy Policy and consent notices at the point of collection.

4.7 Security safeguards (sections 19–22)

We take appropriate, reasonable technical and organisational measures to prevent loss, damage, or unauthorised destruction of personal information, and unlawful access to or processing of personal information, including:

- Encryption of data in transit and role-based access controls for internal systems;
- Written agreements with operators (including our payment gateways and hosting providers) requiring them to maintain equivalent security measures and confidentiality;
- Use of PCI DSS-compliant payment gateways (PayFast, Ozow, Netcash, Zapper, and card/wallet processing for Visa, Apple Pay and Samsung Pay) so that MyOwn ISP does not store full payment card or wallet credentials;
- A documented data breach response procedure (clause 6 below);
- Regular staff awareness training on information security and confidentiality obligations.

4.8 Data subject participation (sections 23–25)

Data subjects may request confirmation of whether MyOwn ISP holds their personal information, request access to it, and request correction or deletion of personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or unlawfully obtained. Requests are handled as described in clause 5 below.

5. Handling data subject requests

A data subject (or a person duly authorised by the data subject) may submit a request to access, correct, or delete personal information, or to object to processing, by contacting our Information Officer using the details in clause 3. We will:

1. Acknowledge receipt of the request and verify the identity of the requester;
2. Where the request is made under the Promotion of Access to Information Act 2 of 2000 (“PAIA”), process it in accordance with our published PAIA Manual and the prescribed forms and fees;
3. Respond within the timeframes prescribed by POPIA and/or PAIA;
4. Where a request is refused, provide written reasons and inform the data subject of their right to lodge a complaint with the Information Regulator.

6. Data breach response

Where MyOwn ISP has reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, we will:

1. Contain and investigate the incident as soon as reasonably possible;
2. Assess the nature and extent of the compromise and the personal information affected;
3. Notify the Information Regulator in writing as soon as reasonably possible after discovery, as required by section 22 of POPIA;
4. Notify affected data subjects as soon as reasonably possible, in sufficient detail to allow them to take protective measures, unless a lawful reason exists to delay notification (e.g. a request from law enforcement);
5. Record the incident, our response, and any corrective action taken, in our internal incident register.

7. Operators and third-party processing

Where a third party processes personal information on our behalf as an operator (for example, our payment gateway providers, Client Portal hosting provider, SMS/email notification provider, or debt collection agency), we conclude a written agreement requiring the operator to:

- Process personal information only for the purposes we authorise and in accordance with our instructions;
- Treat personal information as confidential and not disclose it, unless required by law;
- Implement and maintain appropriate security safeguards, and notify us immediately of any security compromise.

FibreNetworks and other FNOs receive only the minimum personal information necessary to provision, activate, maintain and repair the physical fibre connection to a client's premises (such as the installation address and a fault or order reference), under the terms of our wholesale network access agreements.

8. Cross-border transfers

Where personal information is transferred to a third party outside South Africa (for example, cloud infrastructure or payment processing located abroad), we ensure the transfer complies with section 72 of POPIA — that is, the recipient is subject to a law, binding corporate rules, or agreement providing an adequate level of protection, the data subject has consented, or the transfer is necessary for performance of a contract.

9. Record of processing activities

MyOwn ISP maintains an internal record of the categories of personal information it processes, the purpose of processing, the categories of recipients, retention periods, and the security measures applied. This record is reviewed at least annually and whenever a new system, product or third-party processor is introduced.

10. Training and awareness

All MyOwn ISP staff and contractors who have access to personal information receive POPIA awareness training on induction and periodically thereafter, covering their obligations under this Policy, confidentiality, and how to recognise and report a suspected data breach.

11. Complaints

A data subject who believes MyOwn ISP has processed their personal information unlawfully may lodge a complaint with our Information Officer in the first instance, or directly with the Information Regulator:

Website	www.inforegulator.org.za
Email (general enquiries)	inforeg@justice.gov.za
Email (POPIA complaints)	POPIAComplaints@inforegulator.org.za
Physical address	JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

12. Review of this Policy

This Policy is reviewed at least annually, and whenever there is a material change in our processing activities, our Services, or applicable law. The current version is available on our website and the Client Portal.