POPIA Compliance

Sherpa Business Communications (Pty) Ltd supports the right to privacy and will strive to safeguard client and employee personal information. This policy document sets out how we manage privacy.

1. Governance structure

PAIA is managed by CEO Gary Hendrickse (policy, training, legislation) supported by Abby Hendrickse (client data, enquiries), and Justin Zimri (IT framework). Their responsibility is to ensure that private data held by Sherpa is protected, either through technology or best practices.

Other responsibilities include:

- Deal with any requests received regarding POPI
- Cooperate with the Regulator regarding any investigations
- Sustain a compliance structure
- Develop a POPIA manual
- Update policies and terms
- Provide awareness training
- Remain updated on changes to legislation.

Any queries or requests should be directed to gary@sherpa.co.za, abby@sherpa.co.za or justin@sherpa.co.za

2. Prior authorisation

Sherpa only processes unique identifiers for our own purposes, or acts on data received from our clients for their purposes (marketing and communications). We do not share any of this information with any third parties.

For clients, full names, identity numbers and company address details are required for any persons contracting with Sherpa. We also require and use name and (company) contact details for other parties within our client's environment who form part of the working relationship.

For suppliers, full names and identity numbers of the contracting party, along with company details and bank account details (for payment purposes) are required.

Sherpa does not collect or process unique data or information of children.

We do not believe that we require prior authorisation from the Information Regulator.

3. Purpose of holding clients' data

The purpose of storing or noting client data and company information is for the fulfilment of client-originated assignments such as:

- Compiling Marketing and Brand strategies
- Developing CRM frameworks
- Internal communications
- External communications
- Social media management

4. Marketing & Communication

Sherpa will communicate with willing clients to advise of new services, pricing changes, industry trends or case studies to improve their knowledge. All communications will allow recipients to unsubscribe. Sherpa will hold our clients Names, Contact Details (mobile, landline, email), Title and associated Company on record.

In communicating with the clients of our PAIA-compliant clients, Sherpa will subscribe to the same unsubscribe conditions. Data held will be restricted to Company, Name and specified Contact details of our clients. This data is supplied by our client.

The clients (of our clients) data is supplied by Sherpa's clients, also as PAIA compliant companies.

Sensitive data is not collected or stored (e.g. racial group, religious beliefs, health conditions, political affiliations, sexual preferences, cultural orientation).

5. Collection of data

Sherpa may collect and store data under the following conditions:

- Contact is made telephonically, via our website or by e-mail
- A subscription to a newsletter, adding to our mailing list
- Referrals from third parties to whom you've requested an introduction
- Clients who transact regularly with us as their primary supplier.

Sherpa will also receive data of 'clients-clients' from our client collected on the basis of our client being PAIA compliant. In this category, Sherpa is ultra-sensitive to privacy and security.

6. Sharing of data

We will share data under the following circumstances:

- Compliance with judicial proceedings, court or government orders
- Defend ourselves against any legal claims.

In all instances, despite the order provided (which makes for an 'exempt' case), we will consult with our attorneys before disclosing any personal information.

Sherpa will also share data with our client's permission when making a referral to an upstream associate (e.g. hosting company, e-commerce developers, etc.).

7. Digital security

Sherpa takes all reasonable steps to protect the security of data, including:

- Company policy rules regarding IT use, security, and confidentiality.
- User authentication access control on all Cloud services and on-site servers.
- Client data stored on Gmail / Google Drive only accessible using Google Account with 2 step verification.
- Synology NAS shared folders require user authentication and is encrypted.
- External HDD and NAS encrypted.
- Antivirus on both systems.

Should security be breached, Sherpa will advise any affected clients accordingly.

Clients or prospective clients may contact justin@sherpa.co.za for more information, which could include the involvement of our IT support specialist.

8. Policy & procedures

This document is signed by Sherpa's employees, confirming their understanding of the principles of POPIA, the terms (without needing to be an expert) and key behaviour required.

POPIA

Protection of privacy and security of private data.

Personal information

This refers to information relating to an identifiable, living, natural person. Where applicable, an identifiable, existing juristic person.

The Act provides for Sherpa's employees, Sherpa's clients, clients of Sherpa's clients, Sherpa's suppliers, and any individual outside of this realm.

The data requiring protection and privacy includes:

- Full names
- Home and or Business address details
- Contact details
- Unique identifiers such as ID numbers, bank account details.
- Receipt of any communications which is explicitly private and confidential.
- Information accompanying a name which could identify the person.

Policies & procedures

- All personal information to be treated with strict confidentiality by Sherpa employees.
- All documents to be filed securely.
- Any documents not for secure filing to be shredded.
- All company, contact and address details to be stored securely on our system.
- Client information not to be housed on personal platforms (e.g. email) or devices.
- Where personal platforms (e.g. WhatsApp) are preferred, permission should be provided by the client. In the event of the employee leaving Sherpa, such data must be wiped. A Central Log of client details will be maintained.
- Passwords to Sherpa domains to be updated regularly.
- No personal information may be provided to third parties without the permission of the CEO. An example of this is where we refer a client to our hosting associates, or act with a third party on their behalf (i.e. upstream referral).
- Any PAIA 'exempt' judicial or legal requests for data must also be referred to the CEO.
- Where upstream suppliers impact on PAIA terms, either check their compliance prior to referral or advise the client to check for compliance.
- Particularly sensitive information such as Identity Number and Bank Account details to be restricted to area of use within Sherpa.
- Sherpa's IT representative to receive a monthly IT Health confirmation from our IT specialist associate.

The key driver of PAIA is always to protect and secure the privacy of personal information, which should always be top-of-mind. Remember that this privacy extends to your Sherpa colleagues as well, whose privacy must also remain secure.

PAIA in its entirety can be found on popia.co.za, broken into digestible sections. Should you be unsure of any requirements, rather ask before answering or acting.