Nimble Group Data Protection

Dated: Sept. 2022

Definitions

POPIA	means Protection of Personal Information Act.
Subsidiaries	These include, Norman Bissett and Associates (Namibia, Botswana), Nimble Collection Services, Nimble Risk Services, Nimble Group Kenya
Information Office	means: Andre Booysen Nimble Group 35 brickfield Road Saltriver Cape Town 021 830 0700
Register of Systems	Means a register of all systems or contexts in which personal data is processed by Nimble Group.
Nimble	Means: Nimble Group and all subsidiaries operating under the name "Nimble Group"

1. Policy Statement:

Data Privacy, and how we securely use your Personal Information, is very important to us, we understand your concern about how we use your personal data. Nimble Group and its Subsidiaries collect and process your personal information in accordance with the privacy principles set out below.

The principles we employ to protect Personal Information are in line with the POPI Act, Our Company Code of Ethics and other applicable Laws, rules, and Standards.

Data protection principles

1. Nimble Group and all its Subsidiaries that operate within the Nimble Group are committed to protecting personal Information and we freely promote such behaviour.

2. We provide ongoing training to all our staff and continuously improve on how we maintain data privacy and security, and where needed, we also assist our third-party service providers to do the same.

3. We promote a culture of "Whistle Blowing"

4. We will be transparent when Customers apply via the PAIA process to have access to their personal information. The PAIA process can be found on our Company Website: WWW.NimbleGroup.co.za

5. We will process your Information in a Lawful and responsible manner that would not infringe your data privacy.

6. We may collect your personal information for the purpose that it is intended for, it must be relevant to the purpose of processing, and it may not be collected excessively.

7. Reasonable measures will be implemented to ensure the quality and accuracy of your personal information.

8. We would update all personal information if something changed, when you inform us of these changes.

9. Any queries or complaints from Customers around data protection and privacy will be dealt with swiftly as we respect your rights under the various laws applicable to data protection and Privacy.

10. Nimble Group complies with Data protection and Privacy laws in the countries where we operate.

11. All our third-party suppliers must have appropriate Data Protection and Security measures in place that will comply with our Privacy Statements and rules if we choose to outsource any services.

12. Where it becomes necessary to transfer data to other countries to ensure an ongoing service to our customers; we will ensure that all appropriate measures are in place to comply with Data Privacy and Security laws applicable to that Country, ensuring the safeguarding of your personal data.

13. If we process the personal Information of minors, we will only do so with the consent of parents, legal guardians or as allowed by law.

2. General provisions

a. This policy applies to all personal Information processed by Nimble Group and its subsidiaries.
b. The Responsible Person shall take responsibility for the Nimble' s ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. Nimble will register with the Information Regulators Office as an organisation that processes personal data.
e. The Information Officer will register with the Information Regulators office as the officer that ensures compliance with the rules as stipulated in The Protection of Personal Information Act.

3. Lawful, fair, and transparent processing

a. To ensure its processing of data is lawful, fair, and transparent, Nimble shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to Nimble shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by Nimble must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests
b. Nimble shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in Nimble' s systems.

5. Data minimisation

a. Nimble shall ensure that personal data are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. The Charity shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, Nimble shall have in place a Data Retention policy where personal data is processed and may review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. Nimble shall ensure that personal data is stored securely using modern software that is kept-up to date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted, this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration,
unauthorised disclosure of, or access to, personal data, Nimble shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Company Information Officer.