BLUETEK COMPUTERS (PTY) LTD

PROTECTION OF PERSONAL INFORMATION-POPI POLICY AND COMPLIANCE

Introduction

BLUETEK COMPUTERS (PTY) LTD is a private body and conducts business as an ITC Sales, services and solutions entity.

The POPI Act requires us to:

1. Sufficiently inform customers/suppliers/employees/job applicants, the purpose for which we will process their personal information;

2. Protect our Information assets from threats, whether internal or external, deliberate or accidental, to ensure business continuation, minimise business damage and maximise business opportunities.

This policy and compliance framework establishes measures and standards for the protection and lawful processing of personal information within our organisation and provides principles regarding the right of individuals to privacy and to reasonable safeguarding of their personal information.

The Information Officer is responsible for:

1. Conducting a preliminary assessment;
2. The development, implementation and monitoring of this policy and compliance framework;
3. Ensuring that this policy is supported by appropriate documentation;
4. Ensuring that documentation is relevant and kept up to date;
5. Ensuring this policy and subsequent updates are communicated to relevant managers, representatives, staff and associates, where applicable.

All employees, subsidiaries, business units, departments and individuals directly associated with us are responsible for adhering to this policy and for reporting any security breaches or incidents to the Information Officer.

Any service provider that provides information technology services, including data storage facilities, to our organisation must adhere the requirements of the POPI Act to ensure adequate protection of personal information held on our behalf. Written confirmation to this effect must be obtained from relevant service providers.

Policy Principles

Principle 1: Accountability

1. We must take reasonable steps to ensure that personal information obtained from customers/suppliers/job applicants/employees is stored safely and securely.
2. This includes: Quotations/Invoices/Other Account information/CV's/References/Qualifications/Integrity Checks and any other personal information that may be obtained for our business purposes.

Principle 2: Processing limitation

1. We will collect personal information directly from customers/suppliers/job applicants/employees.
2. Once in our possession we will only process or release information with their consent, except where we are required to do so by law. In the latter case we will always inform the relevant party.

Principle 3: Specific purpose

1. We collect personal information from customers/suppliers/job applicants/employees to enable us to perform our business activities.

Principle 4: Limitation on further processing

1. Personal information may not be processed further in a way that is incompatible with the purpose for which the information was collected initially. We collect personal information for business purposes only.

Principle 5: Information quality

1. We are responsible for ensuring that customers/suppliers/job applicants/employees information is complete, up to date and accurate before we use it. This means that it may be necessary to request customers/suppliers/job applicants/employees, from time to time, to update their information and confirm that it is still relevant. If we are unable to reach a customer's/suppliers/job applicants/employees for this purpose their information will be deleted from our records.

Principle 6: Transparency/openness

1. Where personal information is collected from a source other than directly from a customer's/suppliers/job applicants/employees (EG Social media, portals) we are responsible for ensuring that the customers/suppliers/job applicants/employees is aware:
    - That their information is being collected;
    - Who is collecting their information by giving them our details;
    - Of the specific reason that you are collecting their information.

Principle 7: Security safeguards

1. We will ensure technical and organisational measures to secure the integrity of personal information, and guard against the risk of loss, damage or destruction thereof. Personal information must also be protected against any unauthorised or unlawful access or processing. We are committed to ensuring that information is only used for legitimate purposes with customers/suppliers/job applicants/employees consent and only by authorised employees of our business.

Principle 8: Participation of individuals

1. Customers/suppliers/job applicants/employees are entitled to know particulars of their personal information held by us, as well as the identity of any authorised employees of our business that had access thereto. They are also entitled to correct any information held by us.

The following records will be considered:

- Accounting records
- Taxation records
- Information Technology
- Personnel Records
- Sales and Marketing
- Statutory Company records
- Client Databases
- Internal Phone lists
- Policies
- Directives
- Minutes of Meetings
- Administrative information

Operational Considerations

Monitoring

The Executive Management and Information Officer are responsible for administering and overseeing the implementation of this policy and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes. All employees, subsidiaries, business units, departments and individuals directly associated with us are to be trained, according to their functions, in the regulatory requirements, policies and guidelines that govern the protection of personal information. We will conduct periodic reviews and audits, where appropriate, to ensure compliance with this policy and guidelines.

Operating controls

We shall establish appropriate standard operating procedures that are consistent with this policy and regulatory requirements. This will include:

1. Allocation of information security responsibilities.
2. Incident reporting and management.
3. Customer/Dealer Code addition or removal.
4. Information security training and education.
5. Data backup.

Policy compliance

Any breaches of this policy may result in disciplinary action and possible termination of employment.

For customers/suppliers/job applicants/employees:

By Submitting your information and application you hereby confirm:

1. That you have read and understood our POPI Policy;

2. That you have no objection to us retaining your personal information in our database for future matching;
3. That the information you have provided to us is true, correct and up to date.

If you have any additional questions about our collection and storage of data procedures, please contact us at:

Form of Request

To facilitate the processing of a request, kindly:

1. Use the prescribed form, available on the website of the SOUTH AFRICAN HUMAN RIGHTS COMMISSION at www.sahrc.org.za;
2. Address your request to the Head of the Company (MD)
3. Provide sufficient details to enable the COMPANY to identify:
   a) The record(s) requested;
   b) The requester (and if an agent is lodging the request, proof of capacity);
   c) The form of access required;
      (i) The postal address or fax number of the requester in the Republic;
      (ii) If the requester wishes to be informed of the decision in any manner (in addition to written) the manner and particulars thereof;
   d) The right which the requester is seeking to exercise or protect with an explanation of the reason the record is required to exercise or protect the right.

Prescribed Fees

The following applies to requests (other than personal requests):

1. A requestor is required to pay the prescribed fees (R50.00) before a request will be processed;
2. If the preparation of the record requested requires more than the prescribed hours (six), a deposit shall be paid (of not more than one third of the access fee which would be payable if the request were granted);
3. A requestor may lodge an application with a court against the tender/payment of the request fee and/or deposit;
4. Records may be withheld until the fees have been paid.
5. The fee structure is available on the website of the SOUTH AFRICAN HUMAN RIGHTS COMMISSION at www.sahrc.org.za.

Availability of Manual

This manual is available for inspection by the general public upon request during office hours and there is no charge for viewing the manual at our offices (where it is available).

It will also be published on www.bluetek.co.za as prescribed by legislation.

Managing Director: Cornelius van der Walt, 0182970164, gov@bluetek.co.za, www.bluetek.co.za