

Protection of Personal Information (POPI) Policy

Policy Owner: PoPI SteerCo	Policy Number: TBC Revision Number: 1.	Date: 01 st November 2015
----------------------------	---	--------------------------------------

1. INTRODUCTION

Business Connexion Group and its subsidiaries are committed to protecting Personal Information of its Employees, Clients and Suppliers. The purpose of this Protection of Personal Information (POPI) Policy (this Policy) is to demonstrate this commitment and to inform employees of the principles to be applied in processing of Personal Information.

2. POLICY STATEMENT

Business Connexion Group Limited (hereinafter referred to as "Business Connexion Group") is required to comply with the provisions of the Protection of Personal Information Act No. 4 of 2013 (hereafter referred to as "POPI") by virtue of the nature of its business. Although the commencement date has not been proclaimed, once it is businesses are expected to have one year to comply.

POPI promotes transparency with regard to what information is collected and how it is to be processed. POPI is South Africa's first piece of comprehensive data protection legislation that seeks to regulate the processing of Personal Information during commercial activities.

Data security and privacy are key. POPI seeks to empower the customer, insofar as rights are concerned and insofar as the protection of Personal Information and data security is concerned.

3. PROCESSING OF PERSONAL INFORMATION

Processing of Personal Information means broadly anything done with Personal Information, including the:

- collection (receipt, recording, organisation, collation or retrieval);
- use (updating, alteration, modification, consultation, restriction, merging or linking);
- storage (electronic and physical storage);
- distribution (transmission or the making available); and
- destruction (erasure)

of Personal Information.

According to POPI, "Personal Information" means information relating to an identifiable natural person and juristic person. Personal information includes, but is not limited to:

- contact details: email, telephone, address;
- demographic information: age, sex, race, birth date, ethnicity;
- history: employment, financial, educational, criminal, medical history;
- biometric information: blood type;

- opinions of and about the person; and
- private correspondence.

4. POPI INFORMATION OFFICER RESPONSIBILITIES

The POPI Information Officer plays an important role within the Business Connexion Group. The BCX Group Chief Risk Officer has been appointed as the POPI Information Officer and is responsible for:

- developing, publishing and maintaining a POPI Policy which addresses all relevant provisions of POPI;
- encouraging and ensuring Business Connexion Group's compliance with POPI;
- ensuring that POPI induction training takes place for all staff and ensuring periodic communication awareness on the requirements of POPI takes place;
- ensuring that appropriate policies and controls are in place for ensuring compliance with POPI;
- ensuring that data subjects have access to their Personal Information held by Business Connexion Group and handling data subject access requests;
- handling all aspects of the relationship with the Regulator and dealing with any request from the Information Regulator (hereafter referred to as "Regulator"); and
- ensuring that Business Connexion Group responds to breaches in Personal Information security in accordance with the notification requirements set out in POPI.

4.1 Information Protection Principles

Business Connexion Group, in processing Personal Information, must comply with the below-mentioned eight information protection principles as stipulated in POPI. It is important to understand that these principles do not stand in isolation. They constitute a combination of principles which interact with one another, sometimes overlapping and complementing one another, which need to be applied holistically.

(i) Accountability

Chapter 3, Section 8 of POPI deals with the principle of accountability and provides that Business Connexion Group must ensure that the eight information protection principles and all the measures that give effect to these principles are complied with. This is applicable at the time of the determination of the purpose, the means of processing and during the processing itself. The POPI Information Officer whose role is outlined in detail in Section 5 of this Policy, is accountable for ensuring compliance by Business Connexion Group.

(ii) Processing Limitation

Chapter 3, Sections 9 to 12 of POPI provides for the limitation of processing Personal Information. Since Business Connexion Group processes large volumes of Personal Information across all the business units, the following important considerations should be adhered to:

- personal Information must be processed lawfully in a manner that does not infringe the privacy of the data subject

- Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive
- consent from the individual will be required before any Personal Information may be processed
- such information must consistently be updated to ensure its accuracy and completeness
- processing of Personal Information for the purposes of direct-marketing is expressly prohibited unless those seeking to process the information as such obtains the individuals consent
- an individual's Personal Information may only be sent beyond the boundaries of South Africa if its purpose is to fulfil a contract between the individual and the company concerned, is required by law or proper consent has been obtained
- individuals have the right to request the confirmation if their Personal Information is being accessed from Business Connexion Group and may in addition to this make corrections to this Personal Information.

(iii) Purpose Specification

Chapter 3, Sections 13 and 14 of POPI, provides for the principle of purpose specification, which states that Personal Information must be collected for a specific purpose, explicitly defined and legitimate reasons related to a function or activity of Business Connexion Group. Business Connexion Group must take steps to ensure that the data subject is aware of the purpose for which his/her information is being collected. Further, records must not be kept for longer than necessary to achieve the purpose for which it was obtained. However, there are exceptions.

Personal information may be held longer for historical, statistical or research purposes if it has established adequate safeguards against these records being used for other purposes. Further, Business Connexion Group can retain information if longer than necessary if retention is required by law, if it requires the record for lawful purposes related to its function or activities, if the retention is required by a contract or if the data subject has consented to retention.

(iv) Further Processing Limitation

Chapter 3, Section 15 of POPI provides for the principle relating to the limitation on further processing. This is where Personal Information is received from a third party and passed on to Business Connexion Group for further processing. In these circumstances, the further processing must be compatible with the purpose for which it was collected, for example, if the data subject has consented to the processing, if the information is available in a public record, or if further processing is needed for legal reasons, national security, national health or tax collection or if the information is used for historical, statistical or research purposes.

(v) Information Quality

Chapter 3, Section 16 of POPI provides for the quality of information and states that Business Connexion Group must take reasonably practical steps and regularly review its procedures for ensuring that the Personal Information is complete, reliable, accurate, not misleading and up-to-date. In taking these steps Business Connexion Group must have regard to the purpose for which the Personal Information is collected or further processed. Upon request, individuals (employees and Clients) as well as companies must be able to

access Personal Information about themselves and request that inaccurate or incomplete information be corrected or amended.

(v) Openness

Chapter 3, Sections 17 and 18 of POPI provides for the principle of openness, which requires Business Connexion Group to give two separate notifications to both the Regulator as well as the data subject.

The first notification to the Regulator must occur before the information is processed, but only one general notification is required. The notification must set out the purpose of the processing, descriptions of the categories of data subjects and information to be processed, the recipients or categories of recipients to whom the information may be supplied as well as any planned trans-border flows of information and details of the security measures.

The second is a notification to the data subject. If Business Connexion Group is collecting information it must take reasonably practical steps to ensure that data subjects are aware that Personal Information about them is being collected, the purpose of the collection, the nature of the information, the identities of those who will receive the information and the fact that the data subject has the right to access the information.

However Business Connexion Group does not need to comply with this notification requirement if compliance is not reasonably practicable in the circumstances of the case.

(vi) Security Safeguards

Chapter 3, Sections 19 to 22 of POPI sets out the principle of security safeguards as follows:

- Business Connexion Group as a responsible party, is required to ensure the integrity of Personal Information in its possession by taking reasonable measures to prevent loss, damage, unauthorised destruction and unlawful access. This measures include password protections for online information systems and restricted access to Personal Information, in respect of both Business Connexion Group employees and Clients (wholesale and/or retail)
- where there are reasonable grounds to believe that the Personal Information of an individual has been acquired by a person lacking the necessary authority, Business Connexion Group must notify the Regulator and the individual as soon as reasonably possible after the discovery of the compromise
- this notification may only be delayed if the South African Police Service, the National Intelligence Agency or the Regulator determines that such notice will serve as a hindrance to its criminal investigation
- the notice must be in writing and can be provided to the individual via post, electronic mail, placed on Business Connexion Group's website, published in the media or as may be directed by the Regulator
- this notice must contain sufficient information to allow the individual to take the necessary protective measures.

If a third party is used to process the information, that party must also treat the information as confidential and it must have security measures in place.

All requests from outside Business Connexion Group concerning Personal Information of employees (current and previous) must be referred to the Chief of Human Resources. All requests relating to the Personal Information of Clients must be referred to the BCX Group Chief Risk Officer.

(vii) Data Subject Participation

In terms of Chapter 3, Sections 23 to 25 of POPI, a data subject has the right to request Business Connexion Group to confirm, free of charge, whether or not it holds Personal Information about them, a description of the Personal Information held, including information about the identity of all third parties, who have, or who have had access to the information. In addition, a data subject may request Business Connexion Group to correct or delete Personal Information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, misleading or obtained unlawfully or destroy or delete a record of Personal Information about the data subject that Business Connexion Group is no longer authorised to retain.

4.2 Other PoPI Requirements

(i) Direct Marketing

In terms of Chapter 8, Sections 69 to 71 of POPI, the processing of Personal Information for direct marketing by email, text, voice or image for the purpose of offering to supply any goods or services to a data subject is prohibited unless those seeking to process the information as such obtains the individuals consent. Whenever data is first collected which might be used for any marketing purpose, this purpose must be made clear and the data subject must actively indicate to Business Connexion Group an interest to be part of the offerings and must be given a clear and reasonable opportunity to object to the processing of his or her Personal Information (opt in). Should the data subject object, any further processing of the information is in breach of POPI.

(ii) Trans-border information flows

Chapter 9, Section 72 of POPI makes provision for trans-border information flows. An individual's Personal Information may only be sent beyond the boundaries of South Africa if its purpose is to fulfil a contract between the individual and the company or between the individual and a third party (that is a supplier) acting as an agent for Business Connexion Group, by law or proper consent has been obtained. Business Connexion Group commits to ensure the conditions regarding trans-border flow of information is fully complied with through the use of the necessary contractual commitments from the relevant third parties.

Further, before the information is processed, the notification to the Regulator must set out amongst others, the recipients or categories of recipients to whom the information may be supplied as well as any planned trans-border flows of information and details of the security measures.

(iii) Third Party Contracts

Chapter 3, Sections 20, 21 of POPI specifically requires that Business Connexion Group ensures, in terms of a written contract, that a third party which processes Personal Information for Business Connexion Group, establishes and maintains the security safeguards set out in POPI.

Business Connexion Group employees may transfer information to a third party acting as an agent for Business Connexion Group. However prior to any such transfer, Business Connexion Group employees must ensure that the third party provides a written agreement to provide the same level of protection required by the principles of POPI. In addition, the contracts which Business Connexion Group concludes with third parties must ensure, amongst other, that the requirements relating to consent, purpose specification, direct marketing and notification of the Clients' rights under POPI, is catered for in the contract

(viii) Retention of records

Section 14 of POPI provides for the retention of records. In terms of the purpose specification principle it is important that Business Connexion Group records are not retained for any longer than is necessary for achieving the purpose for which the information was collected or processed. Once the purpose is fulfilled, Business Connexion Group is obliged to destroy or delete a record of Personal Information. Business Connexion Group must establish retention periods for staff, Clients and suppliers. The retention periods must be the minimum as required by current legislation.

However, there are exceptions. Personal information may be held longer for historical, statistical or research purposes if it has established adequate safeguards against these records being used for other purposes. Further, Business Connexion Group can retain information if longer than necessary if the retention is justified by the POPI Information Officer, if Business Connexion Group requires the record for lawful purposes related to its function or activities, if the retention is required by a contract or if the data subject has consented to retention.

5. APPLICABILITY

This Policy is applicable to all employees of Business Connexion Group. The consistent application of this Policy will promote fair and equitable Human Resource practices within Business Connexion Group.

5.1 Effective Date

The effective date of this Policy is 1st November 2015.

This policy will be reviewed as and when required, in order to comply with changes in POPI or Business Connexion Group administrative rules and/or to enhance its effectiveness. Furthermore, ad-hoc changes and improvements will be made as and when they are identified

5.2 Associated / Related Legislation and Regulations

This Policy is guided by the following relevant legislation and associated regulations:

- (i) Protection of Personal Information Act, 2013
- (ii) Electronic Communications and Transactions Act, 2002

5.3 Associated / Related Policies and adopted Standards

This Policy is guided by the following Business Connexion policies and adopted standards:

- (i) Security Policy;
- (ii) Code of Employment Policy; and
- (iii) Control of Records Policy.

5.4 Policy Authority

Any changes to this Policy must be approved by the PoPI Steering Committee.

All Business Connexion Group employees and management shall comply with POPI. Failure and or refusal to abide by the rules detailed in this Policy may be deemed as misconduct and Business Connexion Group may initiate the appropriate investigation and disciplinary action against employees, which may lead to a dismissal and or civil action. A claim of ignorance as to the existence and or application of this Policy shall not be grounds for justification of non-compliance

6. GLOSSARY OF TERMS

Definition	Description
Customer	Refers to both retail and wholesale Clients.
Consent	Means a voluntary, specific and informed expression of will in terms of which a data subject agrees to the processing of Personal Information relating to him or her.
Data Subject	Any person who's information is processed (employees, retail and/ or wholesale Client).
Juristic Persons	Refers to companies.
Natural Persons	Refers to individuals.
Non-compliance	An act or omission whereby Business Connexion Group has not met its compliance requirements.
Personal Information	Information relating to a natural person or juristic person.
Processing of Personal Information	The collection, use, storage, distribution, modification or destruction of Personal Information.
Responsible Party	Public/Private bodies who process information.
Third party	Otherwise known as a supplier.

7. REVISION HISTORY

Policy Number	Policy Title	Creation Date	Revision Number	Author
Version 1	Protection of Personal Information (POPI) Policy	01 November 2015	Version 1	Group Information Officer

7.1 Changes since last version

Applicable changes to the document since least published version			
Change requested by:		Date of Request:	
Summary of changes			
Version Number	Paragraph	Description of change	Effective Date
Version 1	Complete Document	New Policy	01 November 2015