Data Privacy Policy

by
Pieter Smith

Contents

1 Introduction

The right to privacy is an integral human right recognised and protected in the South African Constitution and in POPIA.

POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner. As a security service provider, BPC is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stake holders. A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

Given the importance of privacy, BPC is committed to effectively manage personal information in accordance with POPIA's provisions.

BPC subscribes to conducting business in accordance to a good code for ethical conduct and in compliance with all applicable privacy laws. The Data Privacy Policy sets out the practice that BPC must adhere to. Business areas may supplement this policy with further requirements specific to their business by way of an addendum which must be approved by the relevant Executive Committee and must serve as an addendum to this policy.

The intent of this policy is to set how BPC approaches data privacy not only pertaining to POPIA, but holistically.

BPC is a responsible party and must from time to time engage with 3rd parties. These 3rd parties will be deemed as operators. BPC will in all circumstances act within the ambit of the law.

1.1 Amendment History

This document is amended by the distribution of new revisions of all or part of the document to the named holders. The history of amendments is recorded below.

Date	Sections Revised	Status	Reason for Change	Authorised
2020/07/07	All	Draft	First Issue	Costa Diavastos

Copies of this document other than those listed above will not be revised; such copies are marked as UNCONTROLLED.

1.2 Scope

The policy applies to BPC and its employees and is applicable to South Africa or is required to act under South African law.

1.3 Accountability

Failing to comply with POPIA could potentially damage BPC's reputation or expose BPC to a civil claim for damages. The protection of personal information is therefore everybody's responsibility. BPC will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, BPC will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

2 Roles and responsibilities

An Information Officer must be formally appointed, and the position must always be occupied. The Information Officer will have a reporting line to the Chief Financial Officer.

Deputy Information Officers may be appointed in each business. The Deputy Information Officers will have a dotted reporting line to the Information Officer. Responsibilities of the Information Officer and the Deputy Information Officers are set out in the next section.

2.1 Information Officer

The BPC POPIA Information Officer is appointed in terms of POPIA and POPIA describes the duties and responsibilities of Information Officer in Section 55 as:

1. An information officer's responsibilities include: -
   a) The encouragement of compliance, by the body, with the conditions for the lawful processing of personal information;
   b) Dealing with requests made to the body pursuant to this Act;
   c) Working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the body;
   d) Otherwise ensuring compliance by the body with the provisions of this Act; and
   e) As may be prescribed.
2. Officers must take up their duties in terms of this Act only after the responsible party has registered them with the Regulator.
3. An information officer must, in addition to the responsibilities referred to in section 55(1) of the Act, ensure that-
   a) a compliance framework is developed, implemented, monitored and maintained
   b) a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
   c) a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);
   d) internal measures are developed together with adequate systems to process requests for information or access thereto; and
   e) internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.
4. The information officer shall upon request by any person, provide copies of the manual to that person upon the payment of a fee to be determined by the Regulator from time to time.

The POPIA information Officer has the power and accountability to appoint Deputy Information Officers (DIO) in unique business units and ensure that the DIO is an employee with decision making authority that embed or manage a business unit.

It will be the duty of the POPIA Information Officer to ensure that the BPC Risk Committee and any other relevant executive team member/management or risk mitigation structure is advised and kept abreast of the relevant data breach incident, the response to the incident and the outcome of the incident.

NOTE: In the absence of, or non-availability of the Information Officer, the relevant DIO or senior member will be responsible to deal with the requirements of this policy and POPIA.

2.2 POPIA Deputy Information Officer (DIO)

The designation and delegation of deputy information officers' duties are defined in POPIA, Section 56. Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of:

a) Such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of this Act; and

b) Any power or duty conferred or imposed on an information officer by this Act to a deputy information officer of that public or private body.

2.3 BPC Head IT Security

The BPC Head of IT Security or alternative will assist the DIO in establishing the criticality of a Data Breach incident and the co-ordination of the investigation.

In respect of a suspected or real Data Breach Incident, the protocols set out as per this policy will be adhered to.

- The Head of IT Security will determine and guide in consultation with the DIO and the relevant Incident Response Team members that will play an active role in the investigation related to a data breach. The identified team(s) will conduct the investigation into the incident to determine the scope, severity and the root cause as well as adequately address on-going or potential risks related to an incident as well as the rectification or mitigation of the existing risk or on-going risk.

- The Head of IT Security in consultation with the DIO will also engage with other stakeholders and support functions as per the roles and responsibilities referred to in this protocol and with reference to the relevant Cyber Incident Response team(s) to establish, **as a priority**, the type of data involved, whether it is personal data relating to clients or employees etc. and if so who are the data subjects and how many are involved. These findings will be reported to the POPIA Information Officer as a priority.

- The Head of IT Security will monitor the progress of the investigation team(s) and report key issues to all relevant stakeholders on a continuous basis as to ensure adherence to the protocols of this Policy.

2.4 Legal Counsel

Appropriate internal legal counsel must be engaged to provide inter alia advice on reporting obligations liability issues etc. or advice on instructing external legal counsel etc., when the circumstances of an incident requires for example escalation.

2.5 Board of directors

BPC's board of directors cannot delegate its accountability and is ultimately answerable for ensuring that BPC meets its legal obligations in terms of POPIA.

The board of directors may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The board of directors are responsible for ensuring that:

- BPC appoints an Information Officer, and where necessary, a Deputy Information Officer.
- All persons responsible for the processing of personal information on behalf of BPC:
    - are appropriately trained and supervised to do so,
    - understand that they are contractually obligated to protect the personal information they come into contact with, and

- are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.

- Data subjects who want to enquire about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which BPC collects, holds, uses, shares, discloses, destroys and processes personal information.

2.6 The Marketing and Communications Dept

Marketing and Communications are responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on BPC's website, including those attached to communications such as emails and electronic newsletters.
- Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with persons acting on behalf of BPC to ensure that any outsourced marketing initiatives comply with POPIA.

2.7 Employees and other Persons acting on behalf of BPC

Employees and other persons acting on behalf of BPC will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

Employees and other persons acting on behalf of BPC are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of BPC may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within BPC or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of BPC must request assistance from their line manager or the POPIA Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of BPC will only process personal information where:

- The data subject consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of BPC or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

- Clearly understands why and for what purpose his, her or its personal information is being collected; and
- Has granted BPC with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of BPC will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, BPC will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- the personal information has been made public, or
- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of BPC will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from BPC's central database or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- Transfer personal information outside of South Africa without the express permission from the Information Officer.

Employees and other persons acting on behalf of BPC are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT department will assist employees and where required, other persons acting on behalf of BPC, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage media such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
- Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.

- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time

Where an employee, or a person acting on behalf of BPC, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the POPIA Information Officer or the Deputy Information Officer.

3 Privacy Impact Risk Assessment

A privacy impact risk assessment must be performed annually with a register of all the identified data privacy risks and mitigating actions. This should include but not limited to:

a) Any processing of personal information.
b) Any transborder transfers of personal information.
c) File transfers to external companies containing personal information.
d) File transfers to internal legal entities (other than the registered entity that originally obtained the data).
e) Audits performed containing personal information.
f) Legal agreements covering data privacy, with expiration dates.
g) Non-disclosure agreements covering data privacy.
h) Expiry of contracts with 3rd parties where data is provided to ensure contracts and data provision simulate corresponding dates.
i) Confirmations from providers on termination of agreements that personal information is destroyed.
j) A central registry where all exceptions and the data privacy impact assessment are stored.

4 Purpose specification

4.1 Declaration of justification for collection and processing of information

All websites as well as terms & conditions for all products and services must state clearly the purpose of obtaining personal information from a client, thus declaring the purpose of the collection. Section 18 of POPIA specifically must be referenced to ensure full compliance.

4.2 Information Quality

All reasonable practical steps must be taken to ensure that the personal information is complete, accurate, not misleading an updated where necessary. The quality of the data must be applied in regard for the purpose the information was collected.

5 Data Security and Information Technology

5.1 Access to personal information and audit trail monitoring

Access to personal information per system must be kept up to date by each business area. Access includes personal information, confidential and secret classified information that appear in (both applicable internally and external to BPC)-

a) Systems

b) Databases

c) Data feeds

d) Data transfers (internal and to external parties)

e) Screens

f) Reports

g) Excel Spreadsheets

h) Data extracts (including text files, csv files and any other file formats that includes the data described above)

All sources that contain data described above, must be access controlled. All access to any of the above must be role based in all systems; with different levels of access applicable.

There must be an active control process in place for access control as well as revoking access.

5.2 Access of laptops/desktops

No individual may access a computer/laptop or any other device without the permission of the individual who is logged on to that device. Nor any other personal information without their permission using their domain logon credentials. No individual may access the computer of another when the computer screen is not locked. Domain and system log-on credentials are private and may not be shared.

5.3 Passwords

- All data must be password protected.
- No password may be shared with anyone.
- When a password is considered compromised, it must be change immediately and reported t the relevant DIO.

5.4 Use of wireless networks

No personal information can be transferred or used over a non-secure or public wireless network. Only trusted and secured wireless networks can be used when working with personal information, or confidential or secret classified data.

5.5 Personal information on your laptop and/or desktop

Personal information is not allowed to be stored on a laptop and/or desktop, unless the device has been encrypted by the BPC approved encryption software. Where the device is not approved encrypted - all personal information must be stored on a BPC identified shared drive, cloud drive or server that is access and IT security protected. If personal information is saved onto a laptop/desktop, the data must be deidentified, regardless if the device is encrypted.

5.6 External and mass and media storage devices

Any external mass or media storage device (external hard drives, USB drives, etc) that is intended to have personal information stored on it, must be encrypted and password protected. The mass or media

storage device is only allowed to be used for a specific purpose and pre-defined period. Once the purpose is no longer valid, the data must be deleted.

5.7 Online mass storage and file sharing

No online mass storage sites may be used for personal information that is not approved by BPC and is not monitored and governed by the required IT Security protocols. These would include as an example, Dropbox, Google Drive etc. No file sharing mechanisms may be used for any data that is not within the approved ambit of the BPC IT Security protocols (These include but are not limited to WeShare etc).

5.8 Privacy Notice on Websites

It is the responsibility of each business responsible for an external website, to ensure that a data privacy notice is provided on the external website. The privacy notice on the various websites must be set out in a clear and easy to understand manner

5.9 Website cookie policy

Where any business makes use of cookies on their external website to identify the user, track access or information about browser activity or that could infer some personal or private information about the individual/user, it is mandatory to have a cookie policy as a pop-up to the user. The cookie policy must be in line with the guidelines set out below:

1) Informed: Why, how and where is the personal data used? It must be clear for the user, what the consent is given to, and it must be possible to opt-in and opt-out of the various types of cookies.

2) Based on a true choice: This means, for example, that the user must have access to the website and its functions even through all, but the strictly necessary cookies have been rejected.

3) Given by means of an affirmation, positive action that cannot be misinterpreted.

4) Given prior to the initial processing of the personal data.

5) Withdrawable. It must be easy for the user to change his or her mind and withdraw the consent.

5.10 Posting of paper documents

All documents in paper format that is posted/couriered must contain a disclaimer on the document.

5.11 De-identification

It is a requirement for personal data to be de-identified. Personal information in all non-production environments must be de-identified, unless special permission is obtained for dispensation by the relevant POPIA IO, DIO. Only individuals with valid reason for access, may have access to personal and information in production environments. A process must be in place and documented to ensure access control is granted, monitored and revoked when required.

5.12 Retention of personal information

Records of personal information may not be retained any longer than is necessary for achieving the purpose for which the information was collected. Records of personal information may be retained for periods in excess of the specified time period for historical, statistical or research purposes if there are appropriate safeguards against the records being used for any other purposes, in which the data must be de-identified.

Any regulation or legislation that has the longest period associated with the retention of the data will take preference (E.g. FAIS, FICAA, Tax legislation etc). Data must be retained for a minimum of 5 years from the last date of transaction, unless otherwise specified in any other policy.

5.13 Data deletion and data shredding or data destruction

Personal information records must be destroyed or deleted or de-identified as soon as reasonably practicable after the data is no longer authorised to be retained. The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form. All physical documents must be destroyed as well.

5.14 Employee data

All employee personal information must be treated in the same manner as client personal information with all of the required safeguards in place.

All systems that contain employee personal information must be accessed controlled with appropriate levels of access granted. All internal reporting (Excel or otherwise); may not be distributed via email or any other mechanism that is not in line with the individuals' access level to the relevant information.

Employees must be informed what information is collected from them, as well as the purpose for the collection. All existing and new employees must consent to this. Where employees do not consent – it must be referred to the Head of HR for resolution.

6 3rd Party participation

6.1 Data privacy compliance by external parties and service providers

Accountability for compliance with POPIA rests with a responsible party. Generally, the responsible party must be a resident of South Africa or the processing should occur within South Africa (subject to certain exclusions in section 3 of POPIA).

An external service provider may/will also be a responsible party unless it acts as an operator for BPC. In the event that an external provider is acting as an operator, the latter must process the information only with the knowledge or authorisation of the responsible party and treat the personal information which comes to their knowledge as confidential and not disclose it, unless required by law or in the course of the proper performance of their duties.

All external providers need to be informed that they need to comply with the requirements of POPIA and of the consequences of non-compliance with the Act, as per the provided clauses and templates provided by BPC Legal.

6.2 Agreements with regards to 3rd parties

No data is allowed to be sent to any third party without having the required documentation and contract in place. The required non-disclosure agreements (NDAs) must be signed by both parties.

In addition, where required, Service Level Agreements (SLAs), Master Services Agreements (MSAs) and Scope of Work (SOW) must be documented and signed by both parties.

Agreements where data including personal information is transferred between parties must have specific data-protection clauses defined in the relevant agreement.

All NDAs must have an expiry date and no data is allowed to be transferred without a valid NDA in place.

7 Email

7.1 Email of personal information

Personal information is not allowed to be mailed in an email, meeting invite or as an attachment (in either an email or meeting invite). Where personal information is being emailed in the body of the email, special attention must be given, and the data must be de-identified. In the event where personal information is included in an attachment, the attachment must be password protected. The password is not allowed to be emailed to the receiver or contained in the same email. The password must be communicated telephonically or via a SMS.

Only BPC approved email (namely the Microsoft Outlook Mail Exchange) software is allowed to be used for all email communication, thus no Gmail, Yahoo or any other email service providers are allowed to be used to email any client or personal information or business-related information, regardless of the size. Should there be size constraints on sending emails, the problem must be raised through the IT ticketing system for alternative approved solutions.

7.2 System generated email of personal information

System generated emails containing personal information are allowed but must be in line with deidentification rules set. Where a system generated email contains an attachment containing personal information; that email attachment must be password protected in a consistent manner.

7.3 Disclaimer on email

All electronic mail must have a disclaimer automatically inserted by the BPC email exchange server.

8 Miscellaneous

8.1 Consent

Consent must be obtained from all clients.

8.2 Compliance training

Compliance training is required on Data Privacy on a **regular basis** and is compulsory for all employees of BPC. Training must be available for permanent employees as well as contractors, consultants and temporary employees. Any changes to this policy must be communicated to all employees of BPC

8.3 Processing of personal information

Personal information may only be processed in accordance to the specific purpose. Individuals with access to personal information may not access the information if it is not to execute on a specific purpose. Personal information of any client or employee may not be accessed randomly.

8.4 Transborder transfer of data

Do note that transborder data transfer (including to neighbouring countries) is stringently regulated; therefore, seek further advice if this is to be done.

8.5 Further processing limitation

If the processing of the data is not in line with the original purposes of the collecting of the data (i.e. for a different, or unrelated purpose) additional consent will be required.

8.6 Prevention or mitigation of serious and imminent threat

Data that may lead to the compromise of public health or public safety, or the life or health of the individual or any other individual may be processed beyond the conditions stipulated to the individual. An example would be should an individual be identified to have a deadly infection (such as Ebola) – BPC has the responsibility to report it accordingly to the authorities.

8.7 Contractual and lawful obligations

Further processing of data, that exceeds the purpose that was set out to the client, must be compatible with the initial collection of the information and be within the realm of the law. The processing must also not contravene the contractual rights between the parties.

8.8 Enriching of data

Data may be enriched post obtaining the data (including personal information), where the necessary documentation is in place. This may include but not limited to data verification.

9 Governance

9.1 Ownership of this policy

Ownership of this policy is vested with the **Chief Executive Officer**.

9.2 Approval

This policy must be approved by the **Chief Executive Officer**.

9.3 Non- Compliance

Non-compliance with this policy, standards, procedures, or the like, is a disciplinary offense and may result in disciplinary action and possible dismissal.

9.4 Implementation

The executive of each business area is accountable for the implementation and adherence to this policy in his/her respective business areas.

9.5 Disciplinary Action

Where a POPIA complaint or a POPIA infringement investigation has been finalised, BPC may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, BPC will undertake to provide further awareness training to the employee.

Any gross negligent or the wilful mismanagement of personal information will be considered a serious form of misconduct for which BPC may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence. Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets in order to limit any prejudice or damages caused.

9.6 Review

This policy must be reviewed on an annual basis or more frequently if deemed necessary.

10 Glossary

BPC	Bidvest Protea Coin and all its subsidiaries and business areas.
Collection for specific purpose	1. Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. 2. Steps must be taken to ensure that the data subject is aware of the purpose of collection of the information.
Client	A juristic or natural person where a relationship has been established or intended. A client has/had a product or received advice where any form of engagement is/has been required. This is applicable to past, existing and potential future transactions.
Cloud	Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive.
Collection for specific purpose	1. Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. 2. Steps must be taken to ensure that the data subject is aware of the purpose of collection of the information.
Consent	Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Cookies	Small text files that are stored by the browser (for example, Internet Explorer, Safari and Chrome) on your computer or mobile phone. Cookies can also be used for authentication or to track web browsing activity.
Data Breach	Intentional or unintentional release of information to an untrusted environments including access by an unauthorised party.
Data Classification	All personal and special personal data must be classified and treated as such throughout the organisations. The section below indicates the different levels of classification. All classification of Personal Information and special personal information must be housed along with the Personal Information Inventory in the group identified Metadata Repository. Secret Confidential Sensitive Private Proprietary Public
Data Subject	Means the natural or juristic person to whom personal information relates.
De-identify	In relation to personal information of a data subject, means to delete any information that: 1. Identifies the data subject; 2. Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or 3. Can be linked by a reasonably foreseeable method to other information that identifies the data subject.
Media Storage Devices	Devices that store application or user information or any device that has the ability to store digital information. Examples are tablets, smart phones etc.
Network	Network is defined as all of its infrastructure which includes but is not limited to hardware and software resources that enable network connectivity, communication, operations and management of the entire network. It provides the communication path and services between users, processes, applications, services and external networks/the internet. This includes all methods of connecting to the network which includes but is not limited to: • VPN • APN • Wired Connection Points

Personal Information	Means information relating to an identifiable, living natural person, and where it is applicable, and identifiable, existing juristic person including, but not limited to: 1. Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person. 2. Information relating to the education or medical, financial, criminal or employment history of the person. 3. Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person. 4. The biometric information of the person. 5. The personal opinions, views or preferences of the person. 6. Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence. 7. The views or opinions of another individual about the person. 8. The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
POPIA	Act No. 4 of 2013: Protection of Personal Information Act, 2013
Private Information Classification	Data should be classified as Private when the unauthorised disclosure, alteration or destruction of that data could result in a **moderate level of risk** to BPC or its subsidiaries. By default, all Institutional Data that is not explicitly classified as Confidential or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data.
Proprietary Information Classification	Proprietary data is data generated internally by BPC in any form and can include technical, analytical, legal or operational data. It can be protected under copyright, patent or trade laws and is safeguarded to protect BPC's competitive edge.
Public Information	Fields and documents classified as public, means that it is available for public consumption and that there is no restriction on the data and/or document. This would typically be information that can be made available on product brochures, websites, social media etc.
Secret Information Classification	Data should be classified as Secret when the unauthorised disclosure, alteration or destruction of the data could cause an **immense level of risk** to BPC or its subsidiaries. Examples of secret data may include data that may lead to insider trading, reputational risk or may have a financial impact to the group. **The highest level of security controls should be applied to Secret data.**
Sensitive Information Classification	Data should be classified as Sensitive when the unauthorised disclosure, alteration or destruction of that data could result in a **moderately high level of risk** to BPC or its subsidiaries. Sensitive data includes but are not limited to medical related information. A reasonable level of security controls should be applied to Private data.