BDV PLATINUM

CHARTERED ACCOUNTANTS (SA)

DATA PRIVACY POLICY

At BDV Platinum we are committed to protecting your privacy and to ensure that your personal information is collected properly, lawfully and transparently. Without this personal information, we would not be able to function effectively. It is therefore crucial that we protect your personal information in accordance with the guidelines set out in the Protection of Personal Information Act 4 of 2013. This Policy sets out how we achieve that.

TABLE OF CONTENTS:

1. Definitions

For the purpose of this Privacy Policy -

“Company” (referred to as either “we”, or “our” in this Policy) means BDV Platinum Audit Services Incorporated and BDV Platinum Professional Services Incorporated, 49 Bell Crescent, Westlake Business Park, Westlake 7945.

“**Data subjects”** (referred to as “you” in this Policy) means the person or organisation to whom personal information Incident relates and includes -

(a) prospective clients;

(b) clients;

(c) staff members and job applicants;

(d) service providers, contractors, and suppliers;

(e) shareholders and directors; and

(f) members of the public and visitors.

“**Incident”** means -

(a) non-compliance with this policy and any procedures relating to it;

(b) contraventions of any data protection legislation such as the POPIA; and

(c) Security incidents such as breaches of confidentiality, failure of integrity, or interruptions to the availability of personal information

“Processing” means any activity or operation that achieve a specific result during which personal information is created, collected, used, shared, transformed, stored, or destroyed.

A processing activity is important if we could experience critical or high levels of risk if the process or activity is disrupted or could no longer continue.

“Personal information” means any information relating to an identifiable individual (living or deceased) or an existing organisation (a company, public body, etc.). This includes the personal information of all customers, staff members, job applicants, shareholders, board members, service providers, contractors, suppliers, members of the public, and visitors.

Examples include:

(a) identifiers, such as a name, identity number, staff number, account number, customer number, company registration number, tax number, photos, videos, or any other unique information that can be used to identify a person;

(b) demographic information, such as race, gender, sex, pregnancy, marital status, national or ethnic or social origin, colour, sexual orientation, age, religion, conscience, belief, culture, language, and birth;

(c) information relating to physical or mental health, wellbeing, or disability;

(d) background information, such as education, financial, employment, medical, criminal or credit history;

(e) contact details, such as physical and postal address, email address, telephone number, online identifier (e.g. a person's twitter handle) or location information;

(f) biometric information: this refers to techniques of identification that are based on physical, physiological, or behavioural characterisation, such as blood-typing, fingerprinting, DNA analysis, retinal scanning, facial recognition, and voice recognition;

(g) someone's opinions, views, and preferences;

(h) private or confidential correspondence and any further correspondence that would reveal the contents of the original correspondence;

(i) views or opinions about a person, such as interview notes and trade references; and

(j) the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject.

"POPIA" means The Protection of Personal Information Act 4 of 2013 and its regulations.

"The POPIA Programme" is our ongoing efforts to comply with the provisions of the POPIA and includes:

(a) stakeholder consultation;

(b) defining roles and responsibilities;

(c) policy development;

(d) policy implementation;

(e) monitoring and audit; and

(f) continual improvement.

“Third parties” means any person (including companies, partnerships, legal entities, governmental authorities, and agencies) who are not party to the agreement, i.e., someone who is not you or us;

2. Purpose of this Policy

We have this Policy to help guide our actions so that we keep our client, employee and service provider data safe, protect our reputation and comply with all the relevant data protection regulations, including the Protection of Personal Information Act (POPIA).

3. Scope of this Policy

This Policy applies to:

(a) Any activity where we produce or use personal information;

(b) Anybody involved in processing activities where we produce or use personal information; and

(c) All employees, service providers, contractors and other individuals who have access to personal information

4. Our Policy

While all personal information should be protected, we take a risk-based approach to compliance. We prioritise the protection of personal information that is used in our important business activities, and in activities that could have a substantial impact on a data subject’s right to privacy.

It is our Policy to:
(4.1) follow the principles of privacy protection that are set out in the POPIA; and

(4.2) conduct data protection impact assessments.

4.1 We follow the principles of data privacy

THE PRINCIPLE	WHAT WE DO
Classify personal information	We identify and classify the personal information that we use and produce
Document processing activities	We document all processing activities to ensure that we can respond to requests from the Information Regulator and requests for information by data subjects or third parties.
Specify the purpose for processing	We specify and document the purposes for which we process personal information.
Provide legal basis for processing activities	We ensure that: (a) all processing activities have a legal basis; and (b) We document the specific legal basis for processing personal information for each activity

THE PRINCIPLE	WHAT WE DO
Keep processing to a minimum	We ensure that: (a) we process information that is adequate, relevant, and not excessive, considering the purpose of the activity; and (b) we de-identify personal information before we start the activity where possible. Where de-identification is not possible, we must consider masking the personal information.
Obtain personal information from lawful sources	We obtain personal information from lawful sources only. Lawful sources of personal information include: (a) the data subject; (b) information that the data subject made public deliberately; (c) public records; and (d) a source that the data subject consented to. (e) Other sources may be lawful in special circumstances. If you are unsure, speak to the Deputy Information Officer.
Process transparently	We disclose all processing activities to data subjects in our privacy notices.
Ensure personal information quality	We take reasonable steps to ensure that personal information is complete, accurate, not misleading, and updated when necessary.

THE PRINCIPLE	WHAT WE DO
Limit Sharing	We only share personal information if it is legal to do so and ethically justifiable. We: (a) identify all instances when personal information is shared with external organisations or individuals (third parties); (b) ensure that sharing personal information complies with data protection legislation and the Information Sharing Procedure; (c) enter into appropriate contracts and take additional steps that may be necessary to reduce the risk created by sharing personal information; (d) conduct an information sharing assessment to determine who is responsible to ensure that contracts are concluded, who must review the contracts, and whether we must take additional steps to reduce the risks created by sharing; (e) keep record of personal information sharing activities, including the outcome of assessments, a record of additional steps taken, what personal information was shared and when, and the method we used to share the personal information.

THE PRINCIPLE	WHAT WE DO
Keep personal information secure	We protect all personal information that we use and produce against breaches of confidentiality, failures of integrity, or interruptions to the availability of that information. All personal information processing must comply with our Information Security Management Policy.
Manage personal information incidents	All employees must report incidents in accordance with our Information Security Management Policy and Incident Management Procedure. An incident includes: (a) non-compliance with this Policy and any procedures that relate to it; (b) contraventions of any data protection legislation such as the POPIA; and (c) security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availability of personal information. Employees must immediately report: (a) any known or suspected incidents; or (b) any circumstances that increase the risk of an incident occurring. Reports must be sent to mark@bdvplatinum.com

THE PRINCIPLE	WHAT WE DO
Manage retention periods	We ensure that all records: (a) are managed appropriately and in accordance with any operational or legal rules that may apply; and (b) comply with our Records Management Policy.
Respect data subjects' rights	We respect the rights of data subjects to: (a) access their records; (b) know who their information was shared with; (c) correct or delete inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or illegally obtained information; (d) withdraw consent; and (e) object to the processing of their information when it is not necessary for the conclusion or performance of a contract or to comply with an obligation imposed by law. All data subject requests must go through the Data Subject Request Procedure.

4.2 We conduct personal information impact assessments

Senior Management must ensure that a personal information impact assessment is done before we start a new processing activity. The data protection impact assessment must include a risk analysis of the activity.

We must conduct a personal information impact assessment before we:

(a) continue to process personal information as part of an activity that has not undergone a data protection impact assessment before;

(b) change an existing processing activity;

(c) launch a new product or service;

(d) expand into other countries;

(e) use new systems or software for processing personal information; or

(f) share personal information with third parties.

A personal information impact assessment has three phases:

(1) Identify activities in which personal information is processed.

(2) Complete the data protection impact assessment questionnaire to document the activity, classify information, and perform a risk-rating for the activity.

(3) Complete a further investigation and assessment with assistance from the Deputy Information Officer if the activity had a risk rating of high or critical after the data protection impact assessment questionnaire was completed.
All activities that are rated as critical or high risk during the data protection impact assessment must undergo an assessment every three years.

5 Non- Compliance with this Policy

5.1 If the company does not comply

Our reputation is our biggest asset. Without our reputation, our relationships with key stakeholders and investors would suffer. In addition, we could face substantial fines.

5.2 If you do not comply

This Company only works when we all do our part, and all of us want to see the organisation succeed. If you do not comply with this policy, or if you discover that we are not complying with the policy and you do not tell us about it, you could face disciplinary action.

6. How to contact us

If you have questions about this policy or believe we have not adhered to it, or need further information about our privacy practices or wish to give or withdraw consent, exercise preferences or access or correct your personal information, please feel free to contact us:

49 Bell Crescent

Westlake Business Park

Westlake

T: (021) 701 7620

E: mark@bdvplatinum.com

7. Changes to this Policy

You may request a copy of this privacy policy from us using the contact details set out above. We may modify or update this privacy policy from time to time. These changes will be effective from the date on which they are posted.

Please review this privacy policy from time to time to check whether we have made any changes to the way in which we use your personal information.

8. Document Metadata

Document number			
Document version			
Document approval authority			
Document Approval date			
Document Owner			
Document author(s)			
Last updated			
Visibility			