

Privacy Policy and Data Protection Policy of

Debella Finance (Pty) Ltd

Registration No 2016/415041/07

Authorised Financial Services Provider No 34111

["Debella Finance"]

May 2019



Table of Contents

1. Personal information.....	3
2. Purpose for collection	3
3. Consent to collection	3
4. Sharing	4
5. Law enforcement and disclosure.....	4
6. No selling.....	4
7. Retention	4
8. Transfer to another country	5
9. Introduction	5
10. Legislative Environment.....	5
11. Application.....	5
12. Protection.....	5
13. General rules relating to Personal Data.....	6
14. Responsible Parties.....	6
15. The Risk and Compliance Manager.....	6
16. The IT Manager	7
17. General Data Protection Rules.....	7
18. Data Storage Paper	8
19. Electronic data	8
20. Data Use	8
21. Data Accuracy	9
22. Data Subject Access Requests.....	9
23. Providing Information.....	9
24. Disciplinary Code and Employee’s Employment Contract	9

Privacy Policy

1. PERSONAL INFORMATION

Personal information **includes**:

- certain information that we collect automatically when you visit our website or application;
- certain information collected on registration;
- certain information collected when processing invoices for any insurance policy applied for by you or on your behalf;
- certain information collected on submission; and
- optional information that you provide to us voluntarily (see below);

but **excludes**:

- information that has been made anonymous so that it does not identify a specific person;
- permanently de-identified information that does not relate or cannot be traced back to you specifically;
- non-personal statistical information collected and compiled by us; and
- information that you have provided voluntarily in an open, public environment or forum including any blog, chat room, community, classifieds, or discussion board (because the information has been disclosed in a public forum, it is no longer confidential and does not constitute personal information subject to protection under this policy).

2. PURPOSE FOR COLLECTION

We may use or process any services information, or optional information that any party has provided to us for the purposes indicated when it was agreed to provide it to us. Processing includes gathering relevant personal information, disclosing it, and combining it with other personal information. We generally collect and process any personal information for various purposes, including:

- services purposes – to enable us to provide our services;
- marketing purposes – such as pursuing lawful related marketing activities;
- business purposes – such as internal audit, accounting, business planning, and joint ventures, disposals of business, or other proposed and actual transactions; and
- legal purposes – such as legislative and regulatory compliance or pursuing good governance.

We may use any personal information that that has been provided to us for the purposes indicated when it was agreed to provide it to us.

3. CONSENT TO COLLECTION

We will obtain the applicable party's consent to collect personal information:

- in accordance with applicable law;
- when it is provided to us with any registration information or optional information.

We will obtain the appropriate party's consent to collect personal information in accordance with applicable law when it is provided to us.

4. SHARING

We may share a party's personal information with:

- all product suppliers that are relevant to the services we have rendered or intend rendering to such party;
- our service providers under contract who help provide certain services or help with parts of our business operations, including fraud prevention, bill collection, marketing, technology services;
- other third parties who provide us with relevant services where appropriate.

We may share any personal information with third parties for the purposes of fulfilling our obligations to the respective party among other purposes.

We may disclose the respective party's personal information as required by law or governmental audit.

5. LAW ENFORCEMENT AND DISCLOSURE

We may disclose personal information if required:

- by a subpoena or court order;
- to comply with any law;
- to protect the safety of any individual or the general public; and
- to prevent violation of our customer relationship terms.

We may disclose personal information to third parties if required for legal reasons.

6. NO SELLING

We will not, under any circumstances, sell any personal information. No personal information will be disclosed to anyone except as provided in this privacy policy or as permitted by the current and applicable law.

7. RETENTION

We will only retain any personal information for as long as it is necessary to fulfil the purposes explicitly set out in this policy unless:

- retention of the record is required or authorised by law; or
- the party concerned has consented to the retention of the record.

During the period of retention, we will continue to abide by our non-disclosure obligations and will not share or sell any personal information.

8. TRANSFER TO ANOTHER COUNTRY

We do not transmit or transfer personal information outside of South Africa to any foreign country nor do we process any personal information in any country other than South Africa.

Should it ever be required, Debella Finance will not transfer any personal information to a foreign country without the permission of the party concerned or if required to do so in terms of any applicable legislation or in terms of an order of a court of law.

Data Protection Policy

9. INTRODUCTION

This Data Protection Policy seeks to ensure that Debella Finance:

- Complies with international legal standards and best practice for the receipt, importing, processing, handling and storing of personal data of individuals (“data subjects”), both as received from its clients, and as held in respect of its own employees;
- Protects the rights of its own employees, as well as that of its clients and third parties in respect of individuals’ data;
- Transparently renders how it process, handles and stores individuals’ data;
- Protects itself from the risks of a data breach.

10. LEGISLATIVE ENVIRONMENT

This policy seeks to align best practice in Debella Finance with legal standards governing its clients, including the Protection of Personal Information Act (“POPI”) anticipated to be enacted into law in South Africa in the foreseeable future.

In doing so, it is acknowledged that Debella Finance does not collect or gather data from any party but receives and/or imports data from relevant parties to enable Debella Finance to provide services. Debella Finance does however, collect or gather data from its own employees for various purposes related to human resources and employment benefit administration.

11. APPLICATION

This policy applies to all employees of Debella Finance in respect of all personal data accessed in the provision of services by Debella Finance to any party to whom or on whose behalf any service is rendered, as well as the management of its employment relationships with its own employees.

12. PROTECTION

This policy is intended to protect Debella Finance from various very real data security risks including breaches of confidentiality through data breaches, hacking risks, and the risks of liability in relation to all relevant parties, third parties’ data acquired from such relevant parties and all its own employees.

The rules and standards set out in this policy apply regardless of –

- whether personal data relates to any party including an employee of Debella Finance, and/or
- is stored electronically, digitally, on paper, or on other materials, or through other methods.

13. GENERAL RULES RELATING TO PERSONAL DATA

Personal data shall at all times be:

- processed fairly and lawfully, in accordance with legal standards applicable to such data or data categories;
- obtained only for specific lawful purposes;
- adequate, relevant and not excessive;
- accurate, and kept up to date;
- held for no longer than necessary for the purpose it was obtained for;
- processed in accordance with the rights of data subjects;
- be protected in appropriate ways, methodologies and procedures and according to suitable methods, both organisationally and technologically;
- not be disclosed or transferred or exported illegally, or in breach of any agreement with a client.

14. RESPONSIBLE PARTIES

All employees shall continually be responsible for ensuring the safeguarding, protection and avoidance of any unauthorised disclosure or breach of data personal data in the execution of employment duties and services to Debella Finance, or otherwise in the course of rendering services or being associated with the company.

15. THE RISK AND COMPLIANCE MANAGER

The Risk and Compliance Manager shall –

- in time, be registered as the responsible officer under POPI, once enacted in South Africa;
- execute, and bear responsibility for reporting to executive management about compliance with all technological and operational data protection standards and protocols and advise of any risk of breach at the earliest opportunity with a view to avoiding any risk or breach, or limiting any damage resulting from it. To ensure compliance with this provision, a Breach Notification Form must be completed by any employee of Debella Finance who becomes aware of any breach /or possible breach;
- ensure that all operational and technological data protection standards are complied with;
- arrange data protection training and provide advice and guidance to all employees;
- be entitled and have authorisation to initiate disciplinary proceedings against any employee who at any time breaches any technological and/or organisational and/or

operational data protection standard, rule, custom, instruction, policy, practice and/or protocol (verbal, in writing or otherwise) (“rule”) applicable in any department or area of the operations of the company;

- review and approve any contracts or agreements with third parties to the extent that they may handle or process data subject information;
- attend to requests from individuals to access data Debella Finance holds about them “data subject requests”).

16. THE IT MANAGER

The IT Manager shall –

- ensure that all systems services and equipment used for processing and/or storing data adhere to internationally acceptable standards of security and data safeguarding, and is regularly updated to continue to comply with such standards;
- issue appropriate, clear, regular rules and directives, whether for the organisation as a whole or a particular part of it, department, person or level of person in relation to any aspect of the company’s work, including password protocols, data access protocols, levels of persons who enjoy access to certain data sign-on procedures, password safeguarding protocols, sign-on and sign-off procedures, log-on and log-off procedures; the description of accessories, applications and equipment that will or may be used, and/or that may not be used under any circumstances, and the like.
- evaluate any third-party services the company is considering or may acquire to process or store data, e.g. cloud computing services.

17. GENERAL DATA PROTECTION RULES

All personal data shall be deemed confidential information and be handled as such.

The only person/s entitled to access data covered by this policy, will be those who need to access it for the execution of their direct work services or required outputs.

Under no circumstances will data or personal information be shared outside the scope of required work outputs, or informally. In the event of any doubt, an employee shall be entitled to access confidential information only after obtaining authorisation from their line manager or a senior manager, where any work output requiring access is unusual or out of the ordinary.

Employees will receive induction and on-the-job training in relation to all security standards applicable to such employee’s service delivery and work outputs involving personal information of data subjects.

Employees shall keep all data secure by taking sensible practical precautions and complying with all rules, practices and protocols. In particular, strong passwords shall be used at all times. Passwords shall not be shared under any circumstances;

18. DATA STORAGE PAPER

Where data is stored on paper, it will always be kept in a secure place to which any unauthorised person has no access. This also applies to data stored electronically which has been printed out for any reason.

Employees must ensure that paper and print outs are not left in places where unauthorised persons can see them, e.g. on a printer, and all unwanted paper must be shredded.

19. ELECTRONIC DATA

Where data is stored electronically, it must be protected from unauthorised access, accidental deletion or any risk of exposure to malicious hacking attempts.

Data must be protected by strong passwords that are changed regularly and never shared between employees.

All data may only be stored on designated drives and servers and may only be uploaded to approved cloud computing services.

All servers containing personal data must be located in secure protected locations away from general office space.

Data must be backed up frequently in accordance with backup protocols. Such backups must be tested regularly in line with the company's standard backup procedures and protocols under the direction of the IT Manager. The Risk and Compliance Manager is responsible to schedule a minimum of two random tests each year.

Data may not be saved directly to laptops or other mobile or removable devices such as tablets or smart phones or sticks or data sticks.

All servers and computers containing data must be protected by approved security software, and one or more firewalls under the direction of the IT Manager.

20. DATA USE

It is acknowledged that personal data is at the greatest risk of loss, breach of confidentiality, corruption, hacking or theft when it is accessed or used. Therefore, when working with personal data, employees must ensure that screens of their computers are always locked when left unattended.

Personal data must not be shared informally, and in particular it must never be sent by email or without protection with appropriate passwords, where required to be sent by email.

Data must be encrypted before being transferred electronically. The IT manager together with the Risk Manager must develop and maintain protocols for data transfer to ensure it is sent in protected form to authorised external contacts only, and to avoid it being sent to any unauthorised external or internal parties.

Personal data must never be transferred or sent to any entity not authorised directly to receive it. Employees are prohibited from saving copies of personal data to their own computers.

Employees will at all times access and update only the central, official copy of any data or

work output document, such as payroll.

21. DATA ACCURACY

Employees must take reasonable steps to comply with company rules and work practices to ensure data is kept accurate and up-to-date. The more important the accuracy of any component of personal data is, the greater the effort and measures must be to ensure its accuracy.

Data must always be held in as few places as necessary to ensure efficient service delivery and risk avoidance. Employees are not permitted to create any unnecessary additional data sets. Employees shall at all times remain knowledgeable and informed about all data updating practices and work protocols used by Debella Finance, such as updating via official, acknowledged websites and platforms used by clients.

22. DATA SUBJECT ACCESS REQUESTS

Where an employee or individual who is entitled to it contacts the company requesting any personal information, such request is referred to as a "subject access request".

Employees and individuals who are the subject of personal data held by Debella Finance are entitled to:

- enquire what information is held about them and the purpose for holding it;
- enquire how to gain access to their own personal data;
- be informed of any special measures the company uses to keep such data up to date.

Subject Access Requests shall be made by e-mail and addressed to the Risk and Compliance Manager, who shall address it in consultation with management. The identity of a person making a data subject request will always be verified before handing over any information requested.

23. PROVIDING INFORMATION

In certain circumstances, South African legislation will allow that personal data be disclosed to law enforcement or other agencies without the consent of the data subject. In such circumstance, Debella Finance may be obliged to disclose the requested data but will first ensure that the request is legitimate and will seek assistance beforehand from its legal advisers or other experts. Only the Risk and Compliance Officer will be authorised to furnish the requested data to the enquiring party.

24. DISCIPLINARY CODE AND EMPLOYEE'S EMPLOYMENT CONTRACT

This data protection policy governs every employee of Debella Finance, both during the course of his/her services to it, and to the extent applicable, after termination of services. To the extent that this policy sets out workplace rules (as defined) governing the employee in the course of his/her work and services to the company, it shall form part of the company's Disciplinary Code and Procedure and is hereby also incorporated into it.

A breach of any rule in relation to the protection of personal data set out in this policy shall, in the event of breach thereof, form the basis of disciplinary action. In appropriate circumstances a breach hereof proven in a disciplinary enquiry may lead to dismissal.

The imposition of any disciplinary sanction or dismissal shall not preclude the company from instituting civil proceedings against an employee who acted in breach of this policy where such breach has resulted in liability, loss, reputational damage and/or other damages to the company in the course of pursuing its commercial operations.
