

National Debt Connection (Pty) Ltd (“NDC”)

Privacy Policy in terms of the requirements of the Protection of Personal Information Act 4 of 2013

- 1) Personal Information is treated as strictly confidential in accordance with the provisions of the Act.
- 2) Personal Information is processed in accordance with Applicable Laws, and in accordance with any lawful instructions, requirements or specific directions of our clients.
- 3) Personal Information is not disclosed or made available to any third party (including NDC personnel) other than authorised personnel who require access to such Personal Information, strictly in order for NDC to carry out our obligations.
- 4) Personnel and any other persons having access to the Personal Information are bound by appropriate and legally binding confidentiality and non-use obligations in relation to the Personal Information.
- 5) Internal network user rights (persons having access) are defined by Windows Active Directory running on our domain directory and are thus highly secure and restrictive. Call Center Agents have no access to secured files or folders, no USB or CD-ROM access and limited web access.
- 6) Personnel are monitored 24 hours via live video stream recorded to hard drive for 30-day increments. Furthermore, physical access is granted via a RFID tag and monitored 24/7 via Custom software with reporting capability.
- 7) NDC takes appropriate, reasonable technical and organisational measures to ensure that the integrity of the Personal Information in our possession or under our control is secure and that such Personal Information is protected, against unauthorised or unlawful processing, accidental loss, destruction or damage, alteration, disclosure or access by having regard to:

7.1 any requirement set forth in Applicable Law; stipulated in industry rules or in codes of conduct or by a professional body; and/or

7.2 industry accepted information security practices and procedures.

- 8) Investigations (using generally accepted auditing methodologies) are done to identify all reasonably foreseeable internal and external risks to Personal Information in our possession or under our control at least once in every 12 (twelve) months.
- 9) Appropriate safeguards have been implemented and are maintained against the risks identified.
- 10) Processing of the Personal Information of Data Subjects provided by clients are done for a specific, lawful purpose strictly in accordance with our client's instructions.
- 11) Information collected from Data Subjects are done in a manner as to not infringe the privacy of the Data Subject, in accordance with any Applicable Law governing the collection of Personal Information from the Data Subject.
- 12) The POPI act stipulates that personal information may only be retained for a period necessary to achieve the objective for which it was collected (intended purpose), unless one of the exceptions apply.
- 13) The Minimum Data Retention Period is governed by general legislation and where more than one legislation is impacted, the legislation with the maximum duration is applied.
- 14) NDC is required to comply with the data retention and destruction guidelines as prescribed by their relevant governing bodies.
- 15) Data is retained in electronic format and will be retained for as long as we are required to do so by law or have a legitimate purpose/need for the data.
- 16) NDC deletes all personal information (with the exclusion of voice recordings) once it no longer has a legitimate purpose for retaining or processing such information.
- 17) Deletion (destruction) means to a point that the information cannot be reconstructed or retrieved. It includes all copies and or back-up data on either front end and/or backend data bases.
- 18) NDC ensures that all Personal Information communicated (including any digital communication or any Personal Information stored in digital form) is secured against being

accessed or read by unauthorized parties by (i) using appropriate security safeguards; and (ii) having due regard to generally accepted information security practices and procedures which may apply to it generally or which may be required in terms of specific industry or professional rules and regulations.